APPLICAZIONI DELLA TECNOLOGIA BLOCKCHAIN

VOLUME 3 - 2023

a cura di Danilo Bazzanella e Andrea Gangemi

Autori

Davide Andriano, Anna Lisa Belardo, Andrea Deluca, Luca Tamburo, E. Abate, C. Bertolini, M. Bosio, N. Gallo, Giorgia Appolloni, Valerio Gallo, Simran Singh, Gianluca Turco, Alessio Attanasi, Giorgia Buccelli, MariaCannistrà, RachidEl Amrani, Gianluca Cappiello, Matilde Carnevale, Nadia Giolito, Salvatore Scorsone, Mahdi Beji, Martina Bonelli, Riccardo Kiefer, Sara Papapietro, Cardellino Cecilia, D'Amico Lorenzo, Ferraro Luca, Gelsi Alessandro, Cristian Brunetto, Melissa Cannas, Stefano Leto, Sonia Vittone, Giorgia delle Grazie, Jacopo Taramasso, Daniele Miola, Gabriele Canova, Francesco Pio Barletta, Valerio Donnini, Alessandro Zamponi, Alex Carluccio, Samuele Longo, Veronica Orciuoli, Lorenzo Spinardi, Enrico Bonsignorio, Daniele Di Marco, Ilaria Palumbo, Rachele Pierri, Michele Masiello, Abdelouahab Moubane, Elisa Salvadori, Filippo Scaramozzino, Francesca Portadibasso, Ilaria Panuccio, Giulio Maselli, Iacopo Romano, Simona Di Battista, Davide Prestifilippo, Ilaria Zerbini

DIPARTIMENTO DI SCIENZE MATEMATICHE
POLITECNICO DI TORINO

INDICE

LE NUOVE VESTI DELL'EURO
Davide Andriano, Anna Lisa Belardo, Andrea Deluca, Luca Tamburo

NOSTR: UN SOCIAL NETWORK DECENTRALIZZATO
E. Abate, C. Bertolini, M. Bosio, N. Gallo

SOMNIUM SPACE
Giorgia Appolloni, Valerio Gallo, Simran Singh, Gianluca Turco

CHAINLINK: PROPAGAZIONE DELL'INFORMAZIONE
Alessio Attanasi, Giorgia Buccelli, MariaCannistrà, RachidEl Amrani

INTRODUZIONE E FUNZIONAMENTO DI RGB
Gianluca Cappiello, Matilde Carnevale, Nadia Giolito, Salvatore Scorsone

CORDA: UNA PIATTAFORMA BLOCKCHAIN PER I SERVIZI FINANZIARI
Mahdi Beji, Martina Bonelli, Riccardo Kiefer, Sara Papapietro

RIPPLE: UNA PANORAMICA SULLA TECNOLOGIA E SUL SUO POTENZIALE
Cardellino Cecilia, D'Amico Lorenzo, Ferraro Luca, Gelsi Alessandro

I SERVIZI DELLA BLOCKCHAIN TON
Cristian Brunetto, Melissa Cannas, Stefano Leto, Sonia Vittone

SPATIAL
Giorgia delle Grazie, Jacopo Taramasso, Daniele Miola, Gabriele Canova

HYPERLDEGER
Francesco Pio Barletta, Valerio Donnini, Alessandro Zamponi

WELCOME TO DECENTRALAND
Alex Carluccio, Samuele Longo, Veronica Orciuoli, Lorenzo Spinardi

CBDC: UN'INNOVAZIONE NEI PAGAMENTI DIGITALI
Enrico Bonsignorio, Daniele Di Marco, Ilaria Palumbo, Rachele Pierri

SOLANA
Michele Masiello, Abdelouahab Moubane, Elisa Salvadori, Filippo Scaramozzino

POLYGON E LA POLITICA 110% GREEN
Francesca Portadibasso, Ilaria Panuccio, Giulio Maselli, Iacopo Romano

I CONSUMI ENERGETICI DI BITCOIN
Simona Di Battista, Davide Prestifilippo, Ilaria Zerbini

LE NUOVE VESTI DELL'EURO

Alessio Attanasi, Giorgia Buccelli, MariaCannistrà, RachidEl Amrani

Politecnico di Torino

Corso di Laurea in Ingegneria Informatica
A.A. 2022/2023

BLOCKCHAIN E CRIPTOECONOMIA

CryptoFuture e le nuove vesti dell'euro

Prof. Danilo Bazzanella

Prof. Andrea Gangemi

Andriano Davide s302094

Belardo Anna Lisa s302056

Deluca Andrea s303906

Tamburo Luca s303907

Indice

Capitolo 1: Introduzione 3

Capitolo 2: Tipologie e usi della CBDC 5

2.1: Retail e Wholesale a confronto 5

2.3: Account based e Token based a confronto 8

2.3: Modelli di implementazione 9

Capitolo 3: Ipotesi di un euro digitale 16

3.1: Progetto della banca centrale europea 16

Capitolo 4: Metodi implementativi della CBDC 23

4.1: Caratteristiche tecnologiche di una valuta digitale 23

4.2: Framework basato su blockchain 26

4.3: Pagamento transfrontaliero tramite CBDC 35

4.4: Meccanismi di sicurezza 37

Capitolo 5: CryptoFuture 43

5.1: Sviluppo della CBDC nel mondo 44

Conclusioni 50

Sitografia 51

Capitolo 1
Introduzione

Definizione di CBDC

Le banche centrali sono state per molti anni la fonte di denaro più affidabile per il pubblico, in conformità con i loro obiettivi di politica pubblica. Tuttavia, il mondo sta cambiando notevolmente e il settore della finanza non è nuovo alle possibilità di cambiamento. Da un punto di vista commerciale, i pagamenti digitali sono diventati più veloci e convenienti, soprattutto con volumi e diversità crescenti.

La CBDC (*Central Bank Digital Currency*) è un nuovo tipo di moneta digitale emessa dalle banche centrali. Si tratta di una valuta innovativa attualmente in fase di discussione: le banche centrali di molti paesi hanno mostrato interesse per la sua emissione. Una CBDC sarebbe implementata tramite la tecnologia blockchain e svolgerebbe le stesse funzioni della moneta fiat: presenterebbe le stesse caratteristiche del denaro contante ma assumendo una forma digitale.

Secondo Bech e Garratt (settembre 2017), le valute digitali che potrebbero essere emesse dalle autorità monetarie erano inizialmente chiamate "*Central Bank Crypto Currency*" (CBCC). In dettaglio, le hanno definite come:

"una forma elettronica di denaro emesso dalla banca centrale che può essere scambiata in modo decentralizzato noto come peer-to-peer, il che

significa che le transazioni avvengono direttamente tra l'emittente e il destinatario senza la necessità di un intermediario centrale".

Successivamente, Bjerg ha aggiunto una nuova caratteristica alla precedente definizione di CBCC. L'accessibilità universale è stata integrata nel concetto precedente, sottolineando che CBCC può essere facilmente ottenuta e utilizzata per effettuare pagamenti.

Nel 2018, la Banca dei Regolamenti Internazionali (BRI) ha iniziato a utilizzare il termine "*Central Bank Digital Currency*" invece di "*Central Bank Crypto Currency*", accentuando che le CBDC sono un credito sulla banca centrale come il contante o le riserve. Infatti, secondo la BRI:

"una CBDC è una forma digitale di moneta emessa dalla Banca Centrale che è diversa dai saldi nei conti di riserva o di regolamento tradizionali [...], è uno strumento di pagamento digitale, denominato nell'unità di conto nazionale, che è un'immediata responsabilità della Banca Centrale".

Capitolo 2

Tipologie e usi della CBDC

Esistono due tipologie di CBDC che presentano diversi potenziali vantaggi in termini di inclusione finanziaria, sicurezza ed efficienza delle transazioni nel contesto economico e finanziario.

Retail e Wholesale a confronto

La CBDC *retail* è rivolta al pubblico generale e mira a fornire una valuta digitale sicura e conveniente per transazioni quotidiane, mentre la CBDC *wholesale* è destinata alle istituzioni finanziarie per facilitare transazioni di grandi dimensioni e migliorare l'efficienza delle operazioni finanziarie.

La CBDC *retail* è progettata per essere utilizzata dal pubblico generale, compresi individui, famiglie e piccole imprese. È una forma di valuta digitale emessa direttamente dalla banca centrale e accessibile al pubblico a livello individuale. Mira a fornire un'alternativa digitale sicura e affidabile al contante e alle forme di pagamento tradizionali. Gli individui possono detenere CBDC *retail* in portafogli digitali, dispositivi mobili o smart card, consentendo loro di effettuare pagamenti online e offline. Con tale tipologia di valuta digitale, le persone possono eseguire transazioni quotidiane come pagare beni e servizi presso i rivenditori che la accettano, inviare e ricevere denaro da altri individui o pagare bollette e tasse direttamente al governo. La CBDC *retail* può facilitare pagamenti immediati,

trasferimenti di denaro sicuri e tracciabili e una maggiore inclusione finanziaria per le persone che potrebbero non avere accesso ai servizi bancari tradizionali.

La CBDC *wholesale* è progettata per essere utilizzata dalle istituzioni finanziarie, come banche di compensazione, banche commerciali e investitori istituzionali. A differenza della variante *retail*, quella *wholesale* mira a facilitare transazioni di grandi dimensioni tra entità finanziarie. Questo tipo di CBDC è principalmente utilizzato per scopi di liquidità interbancaria, compensazione di transazioni finanziarie, gestione di rischi e negoziazione di titoli, garantendo una maggiore efficienza e sicurezza. Inoltre, offre una forma di liquidità digitale immediata e garantisce la finalità e l'irrevocabilità delle transazioni, migliorando l'operativa del sistema finanziario.

Si possono distinguere due tipi di CBDC *wholesale* a seconda delle loro implementazioni: (1) pagamenti nazionali, (2) pagamenti transfrontalieri.

Nel contesto dei pagamenti nazionali, la maggior parte delle transazioni *wholesale* nel periodo attuale è associata a un valore elevato, a tempi di regolamento più brevi e a partecipanti istituzionali. Le transazioni *wholesale* possono essere instradate generalmente attraverso le banche centrali che operano su sistemi di regolamento lordo in tempo reale (RTGS) responsabili dell'esecuzione di questi pagamenti. L'esempio di due sistemi di pagamento di grande valore in Europa, come EURO1 e TARGET2, illustra l'uso di CBDC di tipo *wholesale*. EURO1 è un sistema di pagamento ad alto valore utilizzato per le transazioni all'interno dell'area dell'euro, il quale consente la liquidazione istantanea e definitiva delle transazioni in euro tra le banche aderenti, facilitando pagamenti di grossi importi o operazioni di

mercato interbancario. TARGET2, invece, è un sistema di regolamento lordo in tempo reale utilizzato per i pagamenti transfrontalieri e nazionali nell'area dell'euro che, gestito dall'Eurosistema, permette alle banche di effettuare pagamenti tra di loro in modo rapido e sicuro, garantendo il trasferimento dei fondi tra i conti bancari. I pagamenti nazionali in TARGET2 iniziano generalmente con l'emissione da parte della banca ordinante di istruzioni per il pagamento alla banca del beneficiario. Il sistema completa quindi la riconciliazione, la conferma e, infine, il completamento della transazione, assicurando il trasferimento dei fondi tra i conti bancari. Il CBDC *wholesale* nazionale funzionerebbe allo stesso modo, con particolare attenzione, dal punto di vista della sicurezza, alle aree che necessitano di pagamenti nazionali più rapidi, affidabili e di alto valore.

Il caso d'uso per l'implementazione di CBDC *wholesale* per i pagamenti transfrontalieri è più importante rispetto ai CBDC *wholesale* nazionali. Attualmente, le transazioni transfrontaliere si affidano a vari intermediari e alle giurisdizioni competenti per i singoli pagamenti. Per risolvere i problemi delle transazioni transfrontaliere, i CBDC *wholesale* possono essere realizzati in tre diversi scenari. Si possono avere CBDC *wholesale* locali, CBDC *wholesale* trasferibili locali e CBDC *wholesale* universali.

Oltre alla classificazione dei tipi di CBDC *wholesale* per i pagamenti nazionali e transfrontalieri, è possibile trovare anche CBDC *wholesale* per le transazioni sicure. Questi tipi di CBDC potrebbero svolgere un ruolo fondamentale nel sostenere la *tokenizzazione* e la trasformazione digitale della catena del valore della sicurezza.

Account based e Token based a confronto

La CBDC *account based* si basa su un sistema di conti centralizzati presso la banca centrale o un intermediario finanziario, mentre la CBDC *token based* utilizza rappresentazioni digitali uniche (*token*) che possono essere trasferite tra gli utenti e registrate su una rete decentralizzata come la *blockchain*. Entrambi i modelli presentano vantaggi e sfide e la scelta tra CBDC *account based* e *token based* dipenderà dalle preferenze, dagli obiettivi e dalle esigenze specifiche delle banche centrali e dei sistemi finanziari.

Nel caso del CBDC *account based*, i fondi digitali sono legati direttamente a un conto o a un portafoglio digitale presso la banca centrale o un intermediario finanziario autorizzato. Gli utenti detengono un account che registra il saldo della loro CBDC, simile a un conto corrente tradizionale. Quando gli utenti effettuano una transazione, viene aggiornato il saldo del loro account CBDC. La registrazione delle transazioni avviene attraverso un sistema di contabilità digitale centralizzata. In questo modello, le transazioni sono validate e registrate in tempo reale dal sistema centralizzato della banca centrale o dell'intermediario finanziario. L'accesso ai fondi avviene tramite procedure di autenticazione e sicurezza definite, garantendo che solo il titolare dell'account abbia il controllo e l'autorità per effettuare transazioni. La CBDC *account based* offre un alto livello di sicurezza e controllo, in quanto tutte le transazioni vengono tracciate e verificate dalla banca centrale o dall'intermediario finanziario.

Nel caso del CBDC *token based*, i fondi digitali sono rappresentati sotto forma di *token* o unità digitali che fungono da rappresentazione digitale di valore. Ogni *token* CBDC è un'entità digitale unica e indivisibile che

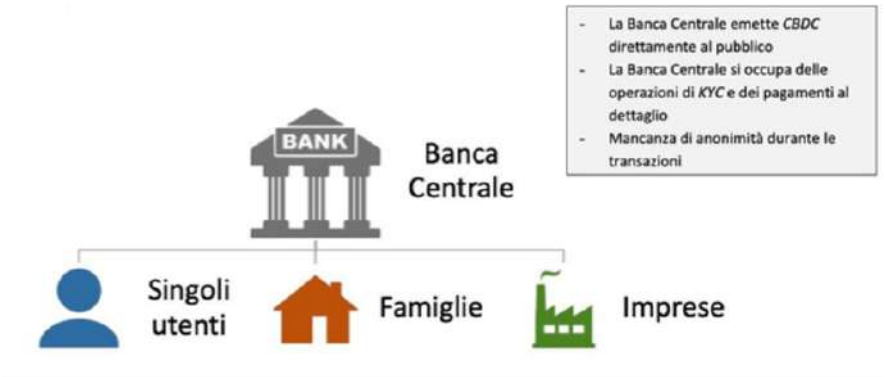
contiene informazioni sul valore e sulla provenienza. Questi *token* possono essere memorizzati su un dispositivo digitale, come uno smartphone o una smart card, e possono essere trasferiti tra utenti in modo simile alle transazioni con denaro contante. Nel modello *token based*, le transazioni avvengono tramite il trasferimento di *token* CBDC tra le parti coinvolte. Il sistema di CBDC *token based* utilizza tecnologie come la *blockchain* o registri distribuiti per registrare e validare le transazioni in modo decentralizzato. Questo permette una maggiore sicurezza, trasparenza e tracciabilità delle transazioni. Ogni *token* CBDC contiene informazioni crittografiche che ne confermano l'autenticità e la validità. Le transazioni vengono verificate dalla rete *blockchain* o dal sistema di registri distribuiti, consentendo alle parti coinvolte di scambiarsi direttamente i *token* senza la necessità di un intermediario centrale.

Modelli di implementazione

Il concetto di CBDC presenta diverse possibilità di implementazione, tra cui il modello diretto, il modello indiretto e il modello ibrido. Ogni tipo di implementazione considera la banca centrale come la parte responsabile dell'emissione e del rimborso dei CBDC. Inoltre, la definizione della giusta architettura alla base del CBDC dipende fortemente dalla scelta del ruolo operativo che deve assumere la banca centrale.

Il modello diretto è il più semplice e immediato da implementare tra i tre modelli sopra citati. È pensato per la disintermediazione e prevede che le banche centrali emettano direttamente le CBDC agli utenti finali, che detengono un conto presso la banca centrale. In questo caso, la banca

centrale detiene il pieno controllo sulla gestione, distribuzione e il monitoraggio della CBDC.



Nel modello diretto, il processo di emissione e gestione è svolto attraverso la banca centrale che crea unità di CBDC e le assegna direttamente agli utenti finali attraverso un conto digitale. Gli utenti possono accedere alle proprie monete virtuali utilizzando un'applicazione mobile, una carta o altri mezzi digitali. La banca centrale è responsabile della sicurezza, dell'identificazione degli utenti, della conformità e della protezione dei dati personali. Tale modello porta vantaggi come:

- Maggiore controllo: il modello diretto consente alla banca centrale di mantenere un controllo diretto sulla CBDC, facilitando la gestione della politica monetaria e la prevenzione di attività illegali come il riciclaggio di denaro;

- Governance: la banca centrale svolge un ruolo chiave nel controllo della CBDC, garantendo un'efficace supervisione e regolamentazione;

- Accesso universale: tutti gli utenti finali, inclusi quelli non *"bancarizzati"*, possono potenzialmente accedere alla CBDC direttamente tramite un conto digitale presso la banca centrale o un intermediario autorizzato;
- Controllo della politica monetaria: la banca centrale può regolare in modo più preciso la quantità di moneta digitale in circolazione, consentendo un maggiore controllo sulla politica monetaria e la stabilità finanziaria.

Tuttavia, questo modello porta con sé delle sfide e delle considerazioni da non sottovalutare:

- Scalabilità: la gestione di un gran numero di transazioni CBDC potrebbe rappresentare una sfida tecnica e logistica per le banche centrali;

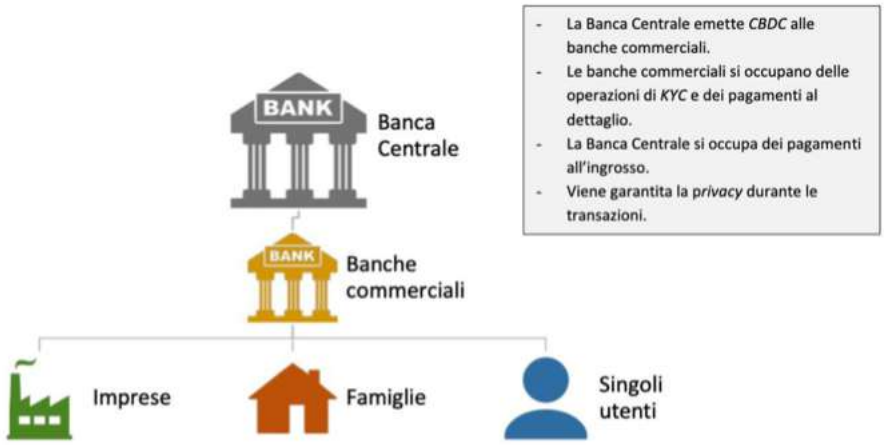
- Privacy: dovrebbero essere implementati meccanismi adeguati per garantire la privacy dei dati personali degli utenti;

- Affidabilità e sicurezza: i sistemi CBDC devono essere altamente affidabili e protetti da potenziali minacce informatiche e attacchi cibernetici;

- Trasparenza: l'elevata centralizzazione potrebbe sollevare dubbi sulla trasparenza delle operazioni e delle decisioni prese dalla BCE;

- Concentrazione del potere decisionale: il modello diretto centralizza il potere decisionale in un'unica entità, sollevando interrogativi sulla distribuzione equa del potere e delle decisioni finanziarie.

Il modello Indiretto è simile al nostro sistema attuale e prevede che le banche commerciali siano gli intermediari tra la banca centrale e gli utenti finali.



Nel processo di emissione e gestione le banche commerciali ricevono una quota di CBDC dalla banca centrale in base alle riserve depositate presso di essa. Queste banche commerciali fungono da custodi delle CBDC e le distribuiscono agli utenti finali attraverso i loro conti bancari tradizionali. Gli utenti possono accedere alle CBDC attraverso applicazioni mobili o servizi bancari online. I vantaggi di questa tipologia di modello sono:

- Coinvolgimento delle banche commerciali: il modello indiretto consente alle banche commerciali di partecipare all'ecosistema CBDC, mantenendo il loro ruolo di intermediari finanziari e favorendo la stabilità finanziaria;

- Esperienza utente: gli utenti finali possono accedere alle CBDC utilizzando i servizi bancari online o le applicazioni mobile che sono già

familiari, semplificando l'adozione della CBDC.

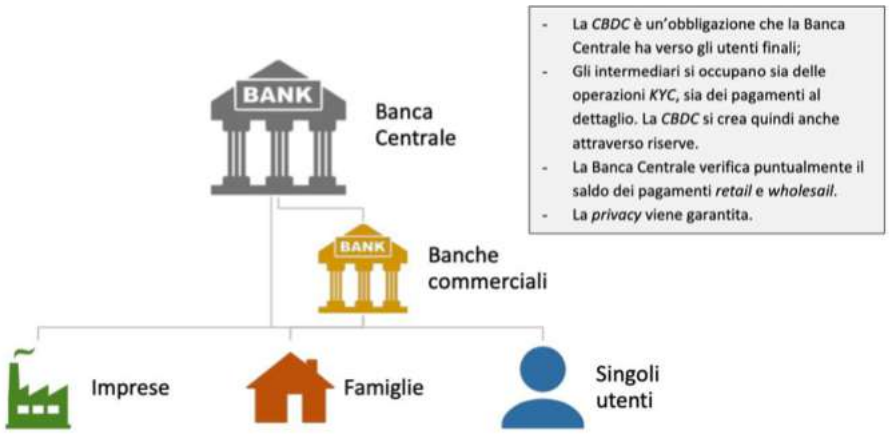
Le sfide e le considerazioni di un modello indiretto sono:

- Dipendenza dalle banche commerciali: il modello indiretto rende il sistema CBDC dipendente dalle banche commerciali, il che potrebbe sollevare preoccupazioni sulla sicurezza e la fiducia degli utenti;

- Livello di controllo della banca centrale: la banca centrale deve garantire un controllo adeguato sulle banche commerciali per evitare potenziali rischi sistemici;

- Rischio per i clienti finali: come per i depositi bancari, i clienti finali non saranno in grado di reclamare il 100% dei loro depositi in CBDC, poiché questi sono mescolati al bilancio della banca.

Il modello ibrido combina elementi dei modelli diretto e indiretto, cercando di sfruttarne i vantaggi. In questo modello, la banca centrale emette le CBDC direttamente agli utenti finali, ma si affida alle banche commerciali per la distribuzione e la gestione operativa.



Il processo di emissione e gestione, in questo caso, prevede che la banca centrale emetta le CBDC direttamente agli utenti finali attraverso un conto digitale, ma si avvale delle banche commerciali come intermediari per la gestione quotidiana delle transazioni, l'identificazione degli utenti e la prevenzione da eventuali frodi. I vantaggi sono:

- Combinazione di controllo diretto e coinvolgimento delle banche commerciali: il modello ibrido cerca di sfruttare i vantaggi di entrambi i modelli, consentendo alla banca centrale di mantenere un controllo diretto sulla CBDC e coinvolgendo le banche commerciali per sostenere l'infrastruttura operativa;

- Flessibilità: il modello Ibrido può essere adattato alle esigenze specifiche di ciascuna giurisdizione, tenendo conto delle dinamiche locali e delle preferenze degli utenti.

Le sfide e le considerazioni, invece, in questo caso sono:

- Coordinazione tra banca centrale e banche commerciali: è essenziale che entrambe le entità collaborino efficacemente per garantire il corretto funzionamento del sistema CBDC;

- Complessità operativa: l'implementazione di un modello ibrido richiede un'infrastruttura tecnologica sofisticata e protocolli di comunicazione stabiliti tra le parti coinvolte;

- Equità e inclusione finanziaria: è fondamentale assicurarsi che il modello ibrido non escluda nessun segmento della popolazione, inclusi coloro che potrebbero avere minori accesso alle risorse

finanziarie o tecnologiche.

In conclusione, l'implementazione della CBDC richiede una valutazione attenta dei diversi modelli disponibili e delle relative sfide. Ogni modello ha i suoi vantaggi e sfide specifiche e quindi una combinazione di approcci potrebbe essere adottata per garantire una CBDC efficace, sicura ed inclusiva.

Capitolo 3

Ipotesi di un euro digitale

Dopo aver trattato le tipologie e gli usi di una valuta digitale, poniamo la nostra attenzione sull'effettivo legame che esiste tra l'euro e l'ipotesi dello stesso sotto forma di moneta digitalizzata. In particolare, chiediamoci da cosa nasce l'esigenza di una CBDC europea e perché la Banca Centrale Europea (BCE) sta attualmente investendo denaro e risorse per una possibile futura implementazione di un nuovo sistema finanziario.

Il progetto della Banca Centrale Europea

Milioni di cittadini europei utilizzano euro in banconote e monete per poter effettuare pagamenti in contanti ed è ormai una pratica comune avere anche la possibilità di pagare con carta di credito o debito presso gli esercenti commerciali. Inoltre, effettuare ordini e pagamenti online in euro, ad oggi, non risulta più essere un evento sporadico. Infatti, soprattutto nell'ultimo periodo, si è notato un aumento esponenziale dell'adozione di pagamenti digitali online, contactless e mediate l'utilizzo di un dispositivo mobile e/o smartwatch, riducendo drasticamente la percentuale di pagamenti in contanti. Tutto ciò ha portato la Banca Centrale Europea ad assumere la propria responsabilità nel mantenere la stabilità dei prezzi e nell'emettere banconote affinché si assicuri il corretto funzionamento dei sistemi di pagamento.

Bisogna difatti sottolineare che anche le banche commerciali emettono monete e vi è una differenza sostanziale tra la moneta emessa da una banca centrale e quella emessa da privati. La prima tipologia di moneta è detta *"moneta pubblica"* ed è legata al concetto di contante, mentre la seconda, detta *"moneta privata"*, è invece associata al concetto di conto corrente bancario. Di conseguenza, i pagamenti effettuati tramite carta di credito o debito sono tutti trasferimenti di moneta privata in quanto comportano l'utilizzo di monete *"create*" dalle banche commerciali. Inconsciamente vediamo interagire queste due tipologie di monete quotidianamente. Di fatto, con un modello a scatola nera dal punto di vista dell'utente finale, quando si è effettua un prelievo di banconote dal proprio conto corrente, non si sta facendo altro che una conversione di moneta privata in moneta pubblica. Al contrario, quando vengono depositati dei contanti in banca, si sta convertendo moneta pubblica in moneta privata. Banalmente, affinché il sistema finanziario funzioni correttamente e si possa instaurare una solida fiducia in esso, bisogna garantire in qualsiasi momento una relazione 1:1 tra moneta pubblica e privata.

Prese in considerazione queste premesse e, come detto in precedenza, aumentata l'esigenza da parte dei cittadini di effettuare pagamenti online, la BCE si interroga sull'opportunità di associare l'euro al mondo digitale, ulteriormente spinta dai tanti paesi che si stanno affacciando verso la digitalizzazione del contante. In un articolo pubblicato sul sito della BCE si legge:

"La nostra ambizione è coniugare i benefici della moneta della banca centrale con le modalità di pagamento e utilizzo della moneta dei cittadini di oggi. In questo modo potremmo affiancare al contante una moneta pubblica in forma elettronica".

Si evidenzia come, tuttavia, una forma digitale dell'euro non andrebbe a sostituire completamente il contante, ma lo affiancherebbe, rispondendo alle nuove esigenze dei consumatori in termini di strumenti di pagamento digitali rapidi e sicuri.

Tuttavia, considerato che il cittadino ha già la possibilità di effettuare pagamenti elettronici, è spontaneo chiedersi cosa cambierebbe dal suo punto di vista e perché gli dovrebbe convenire l'adesione ad una CBDC europea. In effetti, l'utente finale continuerebbe a pagare con una normale carta di credito o attraverso un'applicazione mobile. La differenza sta nel fatto che egli pagherebbe in moneta pubblica, e non tramite moneta privata come avviene oggi, quindi sicura e garantita dalla BCE. Inoltre, dal punto di vista della banca centrale, l'introduzione di una moneta digitale gioverebbe all'innovazione, e quindi ad una crescita economica.

E' importante anche sottolineare che il crescente interessamento che oggi giorno si ha verso le cripto attività, come ad esempio *Bitcoin* ed *Ethereum*, che a loro modo sono soluzioni di pagamento alternative però non regolamentate e non basate sui principali circuiti di carte, ha sicuramente spinto la banca centrale ad interessarsi nel creare un proprio sistema finanziario che potrebbe agire in un modo analogo ma con un dettaglio importante, ovvero costruire il tutto sull'euro che significherebbe garantire in qualsiasi momento una stabilità finanziaria. Infatti, le cosiddette cripto valute non assolvono le tre funzioni cardine di una moneta: (1) essere un mezzo di scambio affidabile, (2) considerarsi una riserva di valore, (3) definirsi come unità di conto, ovvero permettere di attribuire un prezzo a beni e servizi tramite essa. Il piano dell'euro digitale invece camminerebbe di pari passo a queste tre proprietà.

In base a quanto detto fino ad ora, evince che l'effettiva creazione dell'euro digitale converrebbe sia all'utente finale che alla banca centrale.

Un punto dove però sembra quasi obbligatorio soffermarsi è il ruolo delle banche commerciali in quanto l'introduzione di una CBDC potrebbe provocare che quest'ultime non abbiano più un ruolo fondamentale o che addirittura possano subire un calo nel sistema finanziario generale. Immaginiamo un utente finale che può appunto servirsi di tutti i servizi offerti dalle banche commerciali, senza però doversi legare effettivamente ad una. In questo scenario, la banca centrale fornirebbe tutti i servizi, partendo quindi dalla vendita al dettaglio, gravando però pesantemente sul suo ruolo operativo. Ovviamente, si pensi quanto non converrebbe più avere una soluzione di questo tipo. In effetti, il ruolo delle banche commerciali resterà fondamentale per far si che tutto funzioni al meglio e verrebbe semplicemente modificato per permettere una migliore coesione con la BCE. Operazioni come KYC e Due Diligence, rimarrebbero affidate alle banche commerciali, dando così un minore impegno alla banca centrale che continuerebbe a svolgere funzioni core.

Nel dettaglio, le pratiche di KYC (*know-your-customer*) sono l'insieme di procedure che devono essere attuate da alcuni istituti e professionisti a norma di legge. Queste procedure servono per acquisire dati certi riguardo l'identità degli utenti e clienti. Si parla di Due Diligence in merito all'adeguata verifica della clientela ossia un controllo di una serie di dati e notizie, come ad esempio le generalità del cliente, che vengono utilizzate dalla banca per stimare quali rischi possono derivare dalle operazioni finanziare eseguite.

Proprio per questo motivo, invece di *"eliminare"* il concetto di banca commerciale, si prova a modificarne il *modus operandi*. La direzione che si pensa possa essere vincente è quindi dividere il lavoro, seppur con la CBDC il fine ultimo della banca centrale è quello di riacquisire il *"comando"* e quindi la sovranità monetaria. In questo modo, la BCE non sarebbe sommersa da ogni tipo di incarico e le banche commerciali continuerebbero ad avere un ruolo necessario all'interno del sistema.

In merito all'argomento di coesione, sono state proposte negli ultimi anni delle soluzioni *ad hoc*. Una proposta è arrivata da Brunnermeier e Niepelt i quali credono che una buona mossa possa essere quella in cui la BCE rifinanzi sistematicamente le banche commerciali i cui depositi sono stati convertiti in euro digitale. Di conseguenza, la banca centrale manterrebbe sempre il ruolo di *"prestatore di ultima istanza"* ma in modo meno automatico e con capacità di controllo più stringenti.

Una seconda proposta, interessante da analizzare, vede ancora al centro una partnership tra banca centrale e banche commerciali e si basa sul pensare ad una CBDC *"grezza"*, quindi un euro digitale grezzo che banche ed intermediari finanziari distribuirebbero nel sistema. In questo modo, la BCE continuerebbe ad avere l'incarico di emettere la CBDC ma gli attori privati potrebbero sviluppare nuovi servizi di pagamento come portafogli digitali e funzionalità specifiche per utenti diversi.

Far convivere nello stesso progetto futuro banca centrale e banche commerciali non sarebbe solo un modo intelligente di distribuzione del lavoro ma porterebbe anche ad avere una gamma più ampia di fornitori di servizi in modo da sostenere l'innovazione e la concorrenza tra attori privati, dato che ognuno potrebbe provare ad inserire sul mercato qualcosa

che funzioni meglio rispetto alle proposte degli altri, migliorando cosi i servizi a disposizione dei consumatori. In più, nel contempo, questo concetto si integrerebbe perfettamente con uno degli obiettivi della CBDC, ovvero migliorare la resilienza del sistema finanziario.

Attualmente, si procede con cautela verso l'euro digitale, anche se sono stati sottolineati dalla BCE diversi scenari che potrebbero rendere necessaria l'emissione del CBDC, tra cui:

1. Sostenere la digitalizzazione dell'economia europea e l'indipendenza strategia dell'UE;
2. Rispondere al significativo declino del ruolo del contante come mezzo di pagamento;
3. Creare un potenziale utilizzo per transazioni estere e interne all'UE;
4. Introduzione di un nuovo canale di trasmissione della politica monetaria;
5. Mitigare i rischi per l'erogazione di servizi di pagamento;
6. Promuovere il ruolo internazionale dell'euro;
7. Favorire il miglioramento dei costi complessivi e dell'impronta ecologica dei sistemi monetari e dei pagamenti.

Ad ogni modo, la BCE non ha ancora preso una decisione definitiva, infatti si è ancora in fase di investigazione, e, rispetto ad alcune possibili configurazioni funzionali, la banca centrale valuta attentamente cinque impieghi specifici:

- CBDC Online: nel contesto online, al CBDC gli si accede e verrebbe utilizzato tramite piattaforme digitali, come applicazioni mobile, *wallet* o sistemi di pagamento online. Gli utenti potrebbero così effettuare

transazioni, trasferimenti di fondi e pagamenti elettronici. Le transazioni verrebbero elaborate e registrate in tempo reale nei sistemi digitali;

- CBDC Offline: nel contesto offline, la CBDC verrebbe utilizzata in transazioni senza la necessità di una connessione. Ad esempio, potrebbe essere possibile effettuare pagamenti utilizzando l'euro digitale tramite tecnologie come NFC (*Near Field Communication*) o QRCode, che consentirebbero cosi la comunicazione tra dispositivi (smartphone e/o carte di debito con POS) senza la necessità di una connessione Internet attiva. Cosi, il CBDC potrebbe essere utilizzato anche in situazioni in cui la connettività online non è disponibile;

- Pagamenti presso punti vendita, ad esempio esercizi commerciali, avviati dall'ordinante;

- Pagamenti presso punti vendita, avviati dal beneficiario;

- Pagamenti nell'ambito del commercio elettronico.

Dato che non esiste ancora un euro digitale, tutto viene ancora eseguito tramite simulazioni considerando come base di appoggio una DLT (*Distributed Ledger Technologies*) ossia una rete decentralizzata con informazioni digitali sincronizzate e distribuite su un'ampia rete dove tutti i nodi della rete possiedono una copia del database e una volta che le transazioni vengono registrate sono immutabili. Si sottolinea il fatto che la *blockchain* è un esempio di DLT ma non tutte le DLT sono delle *blockchain*.

Capitolo 4

Metodi implementativi della CBDC

Caratteristiche tecnologiche di una valuta digitale

Le caratteristiche che a livello di valuta una CBDC deve soddisfare sono:

- Emissione centralizzata: caratteristica per la quale la CBDC più differisce dalle criptovalute generali. La CBDC è sostenuta dagli stati sovrani o dalle banche centrali e la politica monetaria è formulata dall'istituzione sovrana centralizzata, in modo che la CBDC abbia un valore intrinseco;

- Trasferibilità: indica che la CBDC può essere utilizzato come mezzo di circolazione e pagamento per i continui movimenti di valore nelle attività economiche. Nei pagamenti effettivi, la CBDC deve anche realizzare la divisione mantenendo il principio della somma zero per una circolazione più efficiente e conveniente;

- Conservabilità: la CBDC e la cronologia delle transazioni sono archiviati in modo sicuro sotto forma di dati elettronici in un'organizzazione o nel dispositivo elettronico dell'utente per query, pagamenti, scambi e gestione.

- Transazione offline: uno scambio di denaro tra due parti potrebbe avvenire anche in maniera offline e quindi senza la comunicazione diretta con l'host server o il sistema principale quando la transazione viene eseguita.

- Scambiabilità: per la circolazione di CBDC nel mondo digitale bisogna garantire lo lo scambio equivalente tra una CBDC e altre forme della stessa valuta sovrana, nonché il cambio estero tra CBDC e un'altra valuta sovrana CBDC.

- Regolamentazione controllabile: al fine di prevenire l'uso della CBDC per l'attuazione di attività economiche illegali, essa deve anche ottenere una regolamentazione controllabile sia in termini di politica che di tecnologia. Sebbene la regolamentazione abbia sacrificato in una certa misura il decentramento e l'anonimato, è un mezzo importante per creare un buon ambiente finanziario legale per la valuta digitale.

Data la natura digitale della CBDC, si devono risolvere una serie di problematiche di natura tecnologica:

- No Double Spending: una volta che una CBDC di proprietà di un utente è stata trasferita, non può essere utilizzato per pagare altre transazioni. A differenza di una valuta fisica, la CBDC, identificata in modo univoco da una sequenza di numeri seriali, può essere copiata e salvata più volte. Pertanto, il no double spending è la sicurezza di base che tutte le valute digitali devono considerare, compresa la CBDC;

- Contraffazione: nessuno deve avere la possibilità di falsificare le CBDC emesse dalle istituzioni sovrane o falsificare una CBDC che non sia di sua proprietà. Le CBDC contraffatte non devono superare la verifica, per cui si richiede anche una tecnologia anti-contraffazione per garantire la sicurezza della valuta, proprio come la valuta fisica;

- Non-Repudiation: prevede che tutte le azioni dei partecipanti siano registrate dall'inizio della transazione fino alla fine, inclusi il pagatore, il destinatario e il verificatore della transazione. Nessuno può negare i passaggi della transazione che ha effettuato e completato;

- Verificabilità: è necessario che tutti i record delle transazioni coinvolti nel sistema CBDC possano essere convalidati in modo efficace. Questo è un tassello fondamentale per la CBDC come valuta di circolazione e mezzo di pagamento;

- Anonimato: come la moneta fisica è anonima nella circolazione effettiva, allo stesso modo, la CBDC dovrebbe anche essere progettata per la privacy e l'anonimato degli utenti. Durante lo sviluppo delle criptovalute, l'anonimato della CBDC include principalmente l'anonimato dell'identità degli utilizzatori e l'anonimato delle transazioni. Significa che qualsiasi utente non autorizzato non possa ottenere, calcolare o dedurre l'identità di un utente e le informazioni di una transazione attraverso dati open source.

Framework basato su blockchain

Sappiamo che la blockchain è un'innovazione chiave nelle criptovalute decentralizzate, che consente trasferimenti *peer-to-peer* tra parti senza una terza parte fidata. La blockchain nello sviluppo del settore dei pagamenti e della CBDC potrebbe influenzare i seguenti fattori:

- Costo: i sistemi di pagamento basati su blockchain possono offrire costi di transazione inferiori rispetto ad altri metodi di pagamento, in particolare nei pagamenti transfrontalieri, nel cambio valuta e in altri scenari di pagamento che coinvolgono più entità intermediarie;

- Usabilità: rispetto ai metodi di pagamento tradizionali, i metodi di pagamento basati su blockchain presentano alcuni vantaggi di usabilità poiché la blockchain rende il processo di transazione più intuitivo e più facile da integrare con altri servizi;

- Anonimato: la blockchain fornisce un'architettura di rete efficace per il pagamento anonimo. Alcuni schemi di criptovaluta basati su blockchain consentono agli utenti di effettuare transazioni senza fornire le proprie credenziali reali.

I principali vantaggi, rispetto ai sistemi distribuiti e alle tecnologie di database esistenti, risiedono nell'uso di una struttura di dati specializzata che raggruppa le transazioni in blocchi e/o la trasmissione di tutti i dati a tutti i partecipanti unitamente alla sua resilienza e trasparenza. Esistono distinzioni generali del tipo di autorizzazione per le attuali architetture blockchain:

- *“Permissionless*", "*public*" o "*open*" si riferiscono a blockchain in cui l'accesso non è limitato a un insieme specifico di partecipanti controllati. In questi tipi di blockchain, i partecipanti non si conoscono e non si fidano l'uno dell'altro, quindi il comportamento corretto nell’infrastruttura è incentivato dall'esistenza di un token nativo remunerativo;

- "*Permissioned*", "*private*" o "*closed*" si riferiscono a blockchain in cui l'accesso è limitato ad un set specifico di partecipanti autorizzati. Queste blockchain operano in un ambiente in cui i partecipanti sono già conosciuti, controllati e c'è un livello di fiducia tra loro. Questo elimina la necessità di un token nativo per incentivare il buon comportamento. Inoltre i partecipanti sono ritenuti responsabili attraverso contratti e accordi legali *off-chain* e sono incentivati a comportarsi onestamente attraverso la minaccia di azioni legali in caso di comportamento scorretto;

- "Consorzio" o "federate" si riferiscono ad una blockchain in cui l'architettura potrebbe essere privata o ibrida (pubblica e privata). Questo tipo di DLT utilizza funzionalità quali: restrizione dei permessi, più autorità di controllo e consentono una condivisione delle informazioni facile ma controllata tra le varie parti interessate e altro ancora.

L'implementazione di una valuta digitale di banca centrale basata su blockchain può avvenire attraverso diversi modelli, tra cui l'utilizzo di una blockchain pubblica, una blockchain privata o una rete di consorzio.
Esaminiamo ciascuno di questi modelli per comprendere le loro caratteristiche e le implicazioni che comportano.

Una blockchain pubblica per una CBDC sarebbe aperta a tutti e consentirebbe a qualsiasi entità o individuo di partecipare al consenso e alla convalida delle transazioni. Ciò garantirebbe la massima trasparenza e decentralizzazione, poiché la responsabilità della gestione della blockchain sarebbe distribuita tra tutti i partecipanti. Tuttavia, ci sono alcune considerazioni da fare in merito a:

- Scalabilità: le blockchain pubbliche possono avere problemi di scalabilità a causa del numero di partecipanti e del volume di transazioni. La gestione di grandi volumi di transazioni finanziarie potrebbe richiedere un tempo di elaborazione significativo e potrebbe non essere efficiente per una CBDC su larga scala;

- Privacy: una blockchain pubblica offre un alto livello di trasparenza, ma può essere problematica per quanto riguarda la privacy dei dati finanziari dei partecipanti. Le autorità monetarie dovrebbero affrontare questa sfida per garantire che le informazioni finanziarie sensibili siano protette adeguatamente;

- Governance: poiché una blockchain pubblica coinvolgerebbe una vasta gamma di partecipanti, la governance potrebbe diventare un problema complesso. Sarebbe necessario stabilire meccanismi chiari per prendere decisioni e implementare modifiche sulla blockchain.

Una blockchain privata per una CBDC sarebbe gestita e controllata da un'entità centrale, come una banca centrale o un'autorità monetaria. Solo gli utenti autorizzati ne avrebbero accesso. Alcuni aspetti da considerare sono:

- Controllo centrale: con una blockchain privata, l'autorità centrale ha il controllo completo sulla gestione e la governance della reta. Ciò consentirebbe una maggiore efficienza e tempi di transazione più veloci, ma a scapito della decentralizzazione e della trasparenza;

- Privacy e sicurezza: con una blockchain privata, l'autorità centrale ha un maggiore controllo sulla privacy dei dati finanziari e può implementare misure di sicurezza più rigorose. Tuttavia, ciò comporta anche un aumento del rischio di frodi o manipolazioni da parte dell'entità centrale;

- Interoperabilità limitata: una blockchain privata potrebbe avere limitazioni nell'interoperabilità con altre blockchain o reti. Ciò potrebbe limitare l'efficacia delle transazioni transfrontaliere o la facilità di integrazione con altri sistemi finanziari.

Infine, una rete di consorzio per una CBDC coinvolgerebbe una serie di partecipanti selezionati, come banche commerciali o altre istituzioni finanziarie, che collaborano per gestire e mantenere la blockchain. Alcuni punti salienti sono:

- Consenso limitato: una rete di consorzio riduce il numero di partecipanti che prendono decisioni di consenso, il che può migliorare l'efficienza e la scalabilità rispetto ad una blockchain pubblica. Tuttavia, sarebbe ancora necessario definire i partecipanti e i metri di valutazione delle decisioni;

- Bilancio tra decentralizzazione e controllo: una rete di consorzio cerca di bilanciare la decentralizzazione e il controllo centralizzato. Mentre

diverse entità partecipano alla governance, c'è ancora un'autorità centrale o un gruppo ristretto di partecipanti che svolge un ruolo importante.

- Conformità normativa: una rete di consorzio potrebbe affrontare sfide relative alla conformità normativa, poiché i partecipanti potrebbero provenire da diverse giurisdizioni con regolamenti e requisiti diversi.

La scelta tra questi modelli dipenderà dalle esigenze specifiche dell'autorità monetaria e dalle considerazioni riguardanti la privacy, la sicurezza, la scalabilità, la governance e la conformità normativa. È possibile che vengano adottate soluzioni ibride che combinano elementi di più modelli per ottenere un equilibrio tra le varie esigenze e sfide.

La CBDC potrebbe costruirsi sopra un framework basato su blockchain, seguito dal livello normativo, dal livello di rete e dal livello utente:

1. Livello normativo: qui si evince la principale differenza tra uno schema CBDC con emissione centralizzata e l'architettura di una criptovaluta decentralizzata. Questo è principalmente incaricato di controllare e governare l'intero ciclo di vita della CBDC attraverso gli aspetti tecnici e politici, in modo da mantenere la salute e la stabilità dell'ambiente finanziario basato sulla CBDC. Il livello normativo comprende principalmente la banca centrale, l'infrastruttura a chiave pubblica (PKI), con l'autenticazione dell'identità come nucleo, e altri organismi di regolamentazione come le istituzioni sovrane. Questi ultimi mirano a implementare la supervisione di oggetti come banche e terze parti a livello di rete, utenti e transazioni a livello utente. Il livello normativo non è completamente centralizzato. Gli organismi di

regolamentazione devono cooperare e limitarsi a vicenda;

2. Livello di rete: il livello di rete nella CBDC è un ponte tra i principali regolatori e gli utenti ordinari ed è diverso dalla struttura di rete *p2p* adottata principalmente dalle criptovalute decentralizzate. Questo adotta due diverse strutture di rete:
   a. Una struttura gerarchica ad albero, incentrata sulla banca centrale e altre agenzie di regolamentazione;
   b. Una struttura distribuita locale composta da banche commerciali ed intermediari.

   La prima potrebbe aiutare la CBDC a integrarsi meglio con le strutture finanziarie bancarie esistenti e facilitare l'attuazione delle regolamentazioni. La seconda potrebbe utilizzare la blockchain per risolvere i problemi di sovraccarico dell'entità centrale, arricchire la struttura dell'organizzazione finanziaria e fornire agli utenti modalità di pagamento convenienti, veloci e diversificate.

   Inoltre, la struttura distribuita, aiuterebbe anche ad aumentare le interazioni commerciali tra banche ed intermediari e a migliorare la sicurezza e l'affidabilità del livello di rete CBDC;

3. Livello utente: il livello utente è costituito dagli utenti finali e dalle loro transazioni. Essi sono la principale fonte di dati per la verifica e l'elaborazione del livello di rete. Inoltre il livello utente include scambio di contanti, deposito e/o prelievo di CBDC, pagamento interbancario, pagamento transfrontaliero e cambio valuta. Quando gli utenti finali effettuano delle transazioni interagiscono con gli altri livelli attraverso un modello a scatola nera.

Il flusso di una CBDC, dal momento della sua nascita a quello di prelievo, segue diverse fasi:

- Autenticazione dell'utente: questa fase è molto importante per garantire che gli utilizzatori dispongano di un'identità digitale legale ed è la base per stabilire il framework del sistema CBDC. L'autenticazione nel sistema CBDC include la generazione dell'identità degli utenti, l'autorità di certificazione (CA) delle banche commerciali e degli intermediari. Il processo è il seguente:

    1. Una CA rilascia certificati a banche commerciali e operatori terzi autorizzati dalla banca centrale a concedere loro identità digitali legali;
    2. Le filiali delle banche commerciali che adottano una gerarchia ad albero possono essere sub-ramificate dalle loro sedi centrali;
    3. Gli utenti possono richiedere identità e i diversi indirizzi di conto tramite diverse banche commerciali;
    4. Gli utenti possono anche richiedere un'identità digitale legittima e un indirizzo di account ad un intermediario che ha ottenuto un certificato da una CA. I diversi ID di un utente sono associati all'identità fisica univoca dell'utente;
    5. La banca centrale può interrogare e verificare le informazioni sull'identità di un determinato istituto e utente attraverso una CA;

- Emissione di valuta: l'emissione di CBDC è funzionalmente simile alle transazioni *coinbase* in Bitcoin. Se in quest'ultimo la moneta non è emessa da una banca centrale o da un'agenzia di regolamentazione

autorizzata da un'autorità sovrana, che segue una politica monetaria riconosciuta legalmente, dall'altro lato l'emissione di CBDC si basa su dei protocolli preventivamente concordati. L'emissione di CBDC adotta una struttura gerarchica ad albero con una banca centrale come nodo principale e raggiunge infine la circolazione tra gli utenti attraverso le banche commerciali. Supponendo un sistema basato su un modello indiretto, si avrebbero i seguenti passi:

1. La banca centrale assegna CBDC a varie banche commerciali autorizzate dopo la firma mediante transazione di zecca;
2. Le banche commerciali assegneranno le CBDC che hanno ricevuto alle loro filiali;
3. Gli utenti ottengono CBDC tramite cambio valuta, prelievo e altri mezzi;

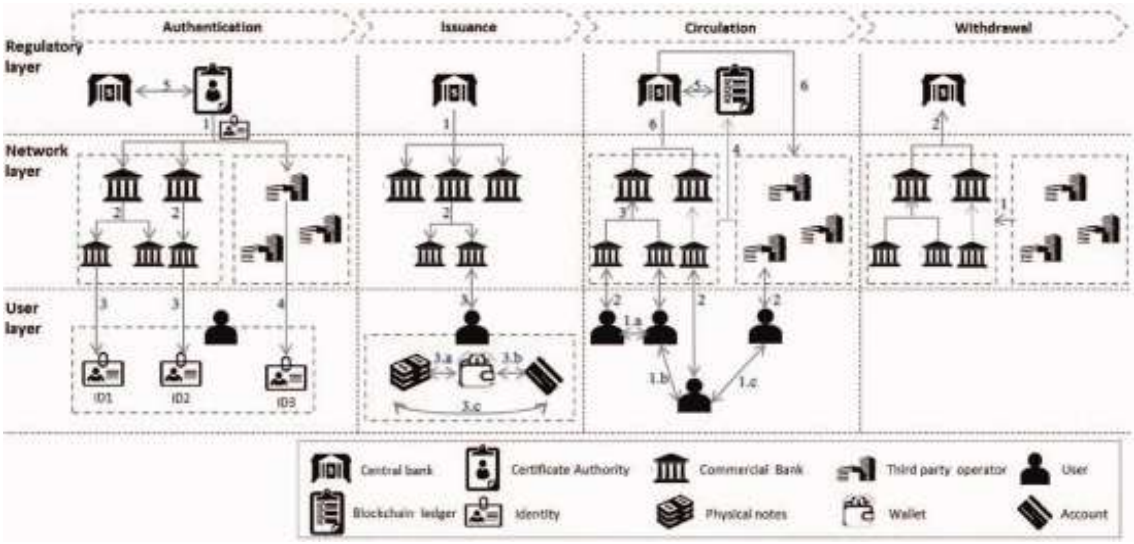
- Circolazione della moneta: la circolazione della CBDC descrive principalmente l'intero processo, dall'utente che invia una transazione contenente CBDC alla sua registrazione sulla blockchain:

1. Un utente seleziona un ID di sua proprietà ed effettua una transazione su un client fornito da una banca commerciale o da un intermediario. Le transazioni che gli utenti possono effettuare includono pagamento interbancario, pagamento tra banche, bonifico transfrontaliero;
2. L'utente invia una transazione alla filiale della banca commerciale corrispondente o all'intermediario . Le banche commerciali e gli questi ultimi sono incaricati della verifica delle transazioni, della registrazione, della gestione dell'account e del portafoglio durante la circolazione delle CBDC;

3. Dopo aver ricevuto la transazione inviata dall'utente, la filiale della banca commerciale la verifica ed esegue le operazioni anti-riciclaggio (AML, ossia *Anti Money Laundering*), quindi invia l'esito della transazione e della verifica alle banche commerciali superiori;
4. Le banche commerciali e gli intermediari inviano le transazioni verificate alla rete blockchain e le registrano sul loro *"libro mastro"* attraverso un protocollo di consenso;
5. La banca centrale può accedere alla blockchain e monitorare le transazioni degli utenti;
6. La banca centrale supervisiona anche tutte le operazioni delle banche commerciali e degli intermediari;

- Prelievo di moneta: il prelievo della CBDC è una funzione simmetrica alla sua emissione ed vantaggioso per aggiornare le sue versioni, migliorare la funzionalità e la sicurezza. Il processo principale è il seguente:

1. Gli intermediari non partecipano direttamente all'emissione della CBDC né inviano direttamente il prelievo della CBDC alla banca centrale, ma realizzano il prelievo e la spesa attraverso interazioni con le banche commerciali.
2. Le banche inviano CBDC dalle filiali sottostanti livello per livello ed, Infine, la CBDC viene recuperata dalla banca centrale in conformità con la politica monetaria.



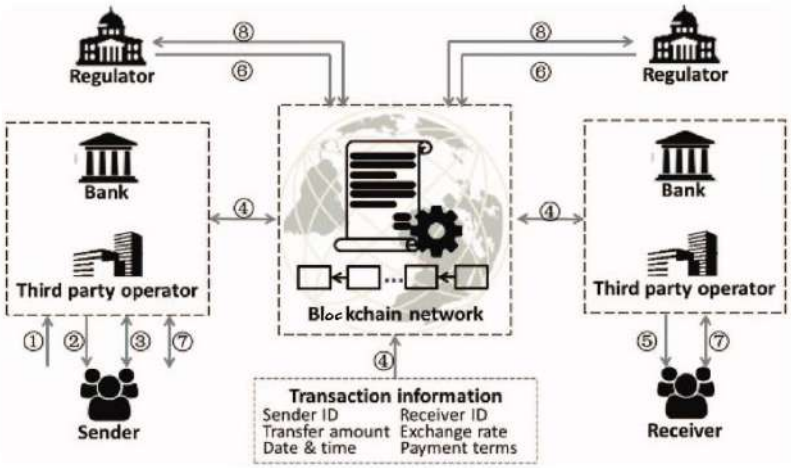
Per differenziare l'euro digitale da altri servizi di pagamento esistenti, offrendo opportunità di creare valore aggiunto, si ritiene che esso debba offrire funzioni di programmabilità nativa per i pagamenti e, quindi, essere costruito all'interno di un ambiente DLT.

Pagamento transfrontaliero tramite CBDC

Uno dei maggiori vantaggi del framework CBDC risiede nel pagamento transfrontaliero tramite CBDC. Quest'ultimo corrisponde al trasferimento di valore attraverso confini geografici. È un caso d'uso importante per la progettazione della CBDC, il quale potrebbe fornire accordi in tempo reale e ridurre i costi, consentendo nuovi modelli di business e istituendo nuovi modelli di supervisione normativa:

1. Il mittente crea una transazione con un ID di sua proprietà e la invia alla banca corrispondente o all'intermediario verificato;

2. Alla ricezione di una richiesta di transazione, la banca o l'intermediario effettua operazioni anti-riciclaggio per verificare la conformità della transazione;
3. Se la transazione è conforme, la CBDC viene bloccata all'interno della transazione. In caso contrario, verrà segnalato al mittente un messaggio di errore;
4. La banca del mittente interagisce con la banca del destinatario attraverso la rete blockchain, utilizzando le informazioni sulla transazione come *trigger* per avviare uno *smart contract* di pagamento transfrontaliero;
5. La banca o l'intermediario del ricevente compie operazioni anti-riciclaggio per verificare se il ricevente e l'operazione contengano violazioni;
6. Se lo *smart contract* viene eseguito con successo, la banca del mittente gli invia un messaggio di successo ed aggiorna il conto CBDC o le informazioni sul portafoglio. La banca del ricevente invia un messaggio di ricevuta al destinatario. Nel frattempo, il destinatario può sbloccare la CBDC e conservarla nel portafoglio o conto. Se l'esecuzione fallisce, la banca invia al mittente un messaggio di errore e restituisce le CBDC.
7. Gli organi regolatori possono anche verificare e recuperare le operazioni concluse.



Meccanismi di sicurezza

Nel contesto di una CBDC, la tecnologia blockchain può offrire diversi meccanismi di sicurezza specifici per garantire la protezione dei dati finanziari e la sicurezza delle transazioni. Alcuni di questi meccanismi includono:

- Autenticazione e identità digitale: la blockchain può essere utilizzata per implementare meccanismi di autenticazione robusti e verificabili, consentendo agli utenti di accedere alla CBDC in modo sicuro. Inoltre può essere utilizzata anche per la gestione delle identità digitali, garantendo che solo gli utenti autorizzati abbiano accesso alla valuta digitale;

- Firma digitale: la firma digitale basata su crittografia a chiave pubblica può essere utilizzata per garantire l'autenticità delle transazioni. Ogni transazione può essere firmata digitalmente per dimostrare che proviene da un mittente specifico e che non è stata alterata durante la

trasmissione;

- Sicurezza dei dati finanziari: i dati finanziari sensibili possono essere crittografati sulla blockchain, garantendo che solo le persone autorizzate possano accedervi. Inoltre, i meccanismi di accesso basati su chiave privata possono essere utilizzati per proteggere i portafogli digitali degli utenti e garantire la sicurezza delle transazioni;

- Controllo degli accessi e permessi: la blockchain può consentire la gestione granulare degli accessi e dei permessi per garantire che solo le parti autorizzate possano partecipare alle operazioni di convalida delle transazioni e alla governance della blockchain della CBDC;

- Audit e tracciabilità: la natura immutabile della blockchain consente una completa verificabilità e tracciabilità delle transazioni finanziarie. Questo può facilitare l'individuazione di frodi e attività sospette e migliorare la conformità normativa;

- Protezione dai rischi informatici: sia distribuzione sia la decentralizzazione della blockchain riducono il rischio di attacchi informatici. Inoltre, l'utilizzo di meccanismi di consenso distribuito aumenta la resistenza della rete ai tentativi di manipolazione o falsificazione delle transazioni.

È però importante notare che la sicurezza di una CBDC basata su blockchain dipende anche da altri fattori, come la sicurezza delle infrastrutture di rete, la protezione delle chiavi private degli utenti e la gestione dei sistemi di identificazione da parte dei relativi gestori.

Dal lato della privacy, il sistema offline sicuramente risulta più sicuro in quanto ogni cosa che viene fatta sfruttando la rete implica un flusso di dati che in qualche modo può essere alterato, rubato o l'infrastruttura stessa essere soggetta ad attacchi.

In un sistema indiretto il flusso di dati è sicuramente maggiore di uno diretto in quanto le informazioni devono circolare tra più parti, ma è anche vero che con gli intermediari si creano più livelli di sicurezza, in quanto oltre a quella fornita dall'Eurosistema c'è anche quella di terze parti. L'anonimato sicuramente andrebbe a eliminare molti problemi di privacy ma porterebbe rischi molto pericolosi: l'euro digitale potrebbe diventare uno strumento di illeciti. Se gli utenti hanno accesso diretto, la BCE deve provvedere a fornire tutti i servizi necessari per l'utilizzo, mentre, se gli utenti hanno un accesso indiretto, gli intermediari fornirebbero tutte le strutture ed i servizi necessari al funzionamento. In quest'ultimo caso, la Banca Centrale Europea dovrebbe preoccuparsi dell'attività svolta dagli intermediari affinché non ci siano problemi e gli utilizzatori non perdano fiducia nel sistema.

Un punto molto discusso riguarda la limitazione all'utilizzo dell'euro digitale. Esiste la possibilità di circoscrivere l'uso dell'euro digitale ad un'area e ad una platea di individui ed entità limitate. Un utilizzo internazionale comporterebbe troppi rischi, mentre una cooperazione tra banche centrali sarebbe ottimale affinché i cittadini di un Paese che visitano uno stato con una valuta diversa abbiano a disposizione la valuta del posto. Un altro punto controverso riguarda la remunerazione che un euro digitale potrebbe avere. Questa caratteristica potrebbe essere sfruttata nella politica monetaria ma anche nella stabilità finanziaria per cercare di ridurre la domanda di euro come investimento e far mantenere il ruolo di primaria

importanza nei pagamenti al dettaglio. Un euro digitale essendo una passività della BCE avrebbe un rischio molto basso, per questo la sua remunerazione deve essere molto vicina allo zero. La banca centrale potrebbe legare la remunerazione ai tassi d'interesse già esistenti per regolare il suo valore e la sua disponibilità.

Un modello diretto si addice in modo migliore ad un'infrastruttura centralizzata mentre, viceversa, quando il modello configurato è ibrido o indiretto, per via della presenza di innumerevoli istituti privati, la migliore infrastruttura da abbinare risulta quella decentralizzata. Quest'ultima potrebbe migliorare significativamente l'accessibilità, la resilienza del sistema e la continuità nell'offerta del servizio.

Per quanto riguarda la raccolta, l'aggiornamento e la condivisione dei dati, in una infrastruttura centralizzata questi avvengono in collegamento con una *repository* unica, gestita esclusivamente dall'autorità regolatrice. In un ambiente decentralizzato ogni nodo di una rete *p2p* partecipa attivamente al processo di collezione delle transazioni con la CDBC, inviandone i *records* tramite liste *broadcast* all'interno di un *distribuited ledger*: con questa modalità si riducono notevolmente sia i tempi che i costi connessi, non solo con la raccolta dei dati ma anche con l'esecuzione degli algoritmi di data mining che non saranno eseguiti verticalmente sui server del gestore ma che si ripartiranno tra i vari nodi della rete in base al protocollo di consenso scelto. Inoltre, l'utilizzo della tecnologia decentralizzata permetterebbe di sfruttare i cosiddetti *smart contracts* a proprio vantaggio e ridurre le tempistiche connesse con la ricezione dei fondi sia da parte dei commercianti che da parte di chi emette titoli obbligazionari. Questo avviene grazie ad un'esecuzione automatica del trasferimento della CDBC dal cliente al relativo destinatario. Gli *smart contracts* renderebbero

possibile lo sviluppo della procedura chiamata *"pagamento programmabile"* avviandosi in determinate situazioni o eventi. Gli *smart contracts* garantirebbero infine l'esecuzione di micropagamenti, ossia pagamenti frazionati, e di pagamenti definiti *bulk*, ovvero pagamenti molteplici effettuati in un *time range* ridotto.

Per quanto riguarda la modalità di autenticazione di un utente alla CBDC, in un approccio account-based, per effettuare una transazione sarà necessario l'utilizzo di una password e di un codice OTP. Quando la transazione sarà verificata, il record viene aggiornato automaticamente aumentando o diminuendo proporzionalmente il saldo dell'account. In un approccio token-based, invece, per avviare un trasferimento, il titolare di un token è tenuto a dimostrare di controllare il token, solitamente firmando un pagamento attraverso la chiave privata associata a quel determinato token. Infine, i token individuali non possono essere spesi parzialmente mentre il il token trasferito viene generalmente separato in due token più piccoli di nuova creazione con lo stesso valore totale, uno per il destinatario dell'azione e l'altro restituito al mittente come resto.

Sia i sistemi basati su account che i sistemi basati su token possono essere configurati con diverse soluzioni di identità, che spaziano da un'anonimità completa fino ad una soluzione con un'identificazione completamente trasparente. Tuttavia, né un approccio basato su account e né un approccio basato su token consentirebbero dei trasferimenti simili al contante in cui il pagamento può essere effettuato senza fare riferimento a terzi o intermediari. Sotto un punto di vista operativo, un approccio basato su token o account potrebbe essere in grado di fornire la gamma di funzionalità di cui necessita una CDBC.

Da una parte si ha che l'ID digitale del modello account-based, permette un forte controllo ed una grande tracciabilità dei movimenti coprendo diverse finalità legali, dal KYC all'AML fino alle incombenze fiscali, dall'altra negherebbe una delle principali caratteristiche del denaro contante, ovvero l'anonimato. L'alternativa è un sistema token-based, ovvero la possibilità della banca centrale di riconoscere la proprietà del denaro, il deposito, un credito e una transazione attraverso un token digitale anonimo, ad esempio la parte privata di una chiave pubblica conosciuta dalla banca centrale. Nella pratica questa potrebbe anche essere fornita da carte o app rilasciate da soggetti privati (es. banche). Si dovrebbe, inoltre, definire come il sistema di pagamento debba gestire gli scambi transfrontalieri e se, nel caso di un modello retail alla base, debba gestire ogni account direttamente o piuttosto solo scambi wholesale tra le banche centrali.

Bisognerebbe progettare le CBDC affinché fin dall'inizio prevedano elementi per garantire token, account e transazioni di soggetti che appartengono ad altri circuiti, questo accorcerebbe l'attuale modello di pagamento e garantirebbe una competizione alla pari con le *stablecoin*. In particolare, le soluzioni DLT e token-based, rappresentano le scelte più aperte per poter rispondere alle esigenze presenti e future di una CBDC.

Capitolo 5
Cryptofuture

Attualmente ci troviamo in un punto di transizione che potrebbe cambiare e stravolgere per sempre il concetto di contante e, in generale, i sistemi di pagamento mediante quella potrebbe essere una vera e propria rivoluzione finanziaria.

Tuttavia, si tenga in considerazione che l'effettiva implementazione ed emissione di un euro digitale dovrebbe seguire delle linee guida, facendo particolare attenzione a quelle che potrebbero essere le possibili problematiche. Infatti, l'uso eccessivo di una CBDC come forma di investimento e il rischio associato alle improvvise riallocazioni dei depositi bancari all'euro digitale andrebbero evitati. Inoltre, la moneta digitale dovrebbe essere disponibile tramite intermediari vigilati e i rischi connessi al progetto informatico, ad esempio quelli legati a ritardi e a costi inattesi, andrebbero minimizzati. Da non sottovalutare sono anche le possibili minacce cibernetiche: i servizi legati alla valuta digitale dovrebbero essere estremamente sicuri e resistenti. La CBDC dovrebbe mirare a rispettare gli standard regolamentari, anche in assenza di un obbligo e, infine, andrebbero sicuramente definite le condizioni per il suo uso al di fuori dell'area dell'euro.

Sviluppo della CBDC nel mondo

Si evince, dunque, che sono ancora molte le sfide da affrontare e importanti i problemi da risolvere, almeno per quanto riguarda il progetto europeo. Infatti, l'Europa non è ovviamente l'unica entità mondiale ad essersi interessata all'argomento. Nelle varie parti del mondo, quasi ogni nazione si è messa al lavoro per portare avanti il proprio progetto in merito alla CBDC e non tutte si trovano nella stessa fase. Analizziamo dunque le diverse fasi che compongono solitamente un progetto di questo tipo e lo stato attuale nel mondo.

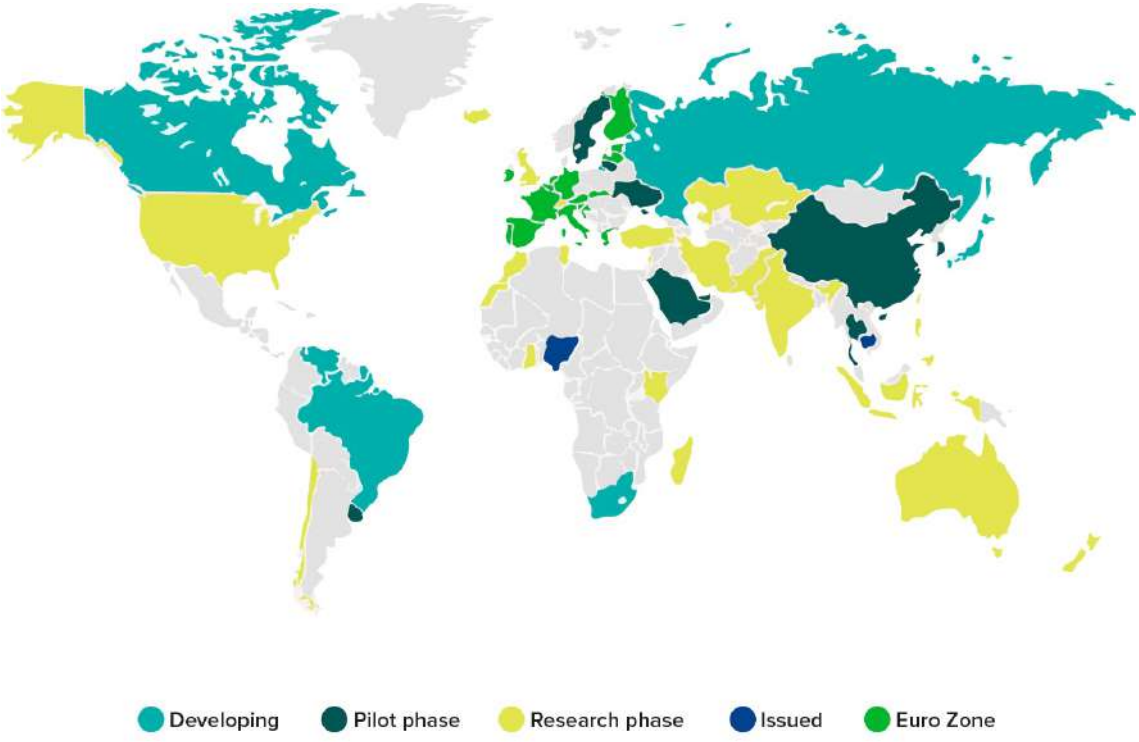


FIGURA 1: Lo stato delle CBDC a livello globale – mappa aggiornata a febbraio 2022

La fase iniziale è quella di studio e ricerca il cui fine è produrre un'analisi propedeutica ad uno sviluppo successivo. Stati Uniti, Australia ed Europa

sono attualmente in questa fase. Negli Stati Uniti, la Federal Reserve ha pubblicato un paper che esamina i pro e i contro relativi all'emissione di una moneta digitale statunitense. Il documento riassume lo stato attuale dei sistemi di pagamento nazionali e i più recenti metodi, andando anche a trattare tematiche inerenti a *stablecoins* e altre criptovalute. Tale documento rappresenta in maniera evidente il primo passo per una consultazione pubblica che mira a raccogliere i pareri e le opinioni di tutte quelle che saranno le parti coinvolte. Parallelamente, l'Australia ha pubblicato un rapporto per celebrare la positiva conclusione del progetto *"Atom"* il quale dimostra il potenziale di una CBDC di tipo *wholesale* nel migliorare l'efficienza, la gestione del rischio e l'innovazione nelle transazioni dei mercati finanziari. Interessante è anche il caso Meta (Facebook). La famosa azienda di Zuckerberg, affascinata dall'argomento, sta lavorando da tempo alla propria *stablecoin* legata al dollaro, chiamata DIEM. Tuttavia, ha dovuto interrompere l'iniziativa a causa di numerose difficoltà riscontrate lungo il percorso, tra cui le opposizione delle banche centrali. Infine, in Europa, dopo una fase di sperimentazione tecnica, l'UE ha dato inizio alla fase investigativa sulle modalità di implementazione di una CBDC europea dalla durata di due anni, partita nel luglio del 2021 e che si concluderà nell'autunno del 2023. In particolare, la Francia ha testato delle transazioni interbancarie e su un mercato secondario utilizzando una blockchain privata. Allo stesso tempo, insieme alla Banca Nazionale Svizzera, sta sperimentando transazioni di CBDC *wholesale*. Un ulteriore paese che lavora sulla digitalizzazione della propria moneta è il Regno Unito, che, per quanto sia ancora all'inizio, ha già proposto un *"pound digitale"* basato su DLT mediante l'uso di un'ottima strategia di marketing e comunicazione.

Un giorno nella vita di un utente di libbra digitale

7:00

Controlla il tuo saldo sul portafoglio digitale della sterlina.

10 del mattino

Compra una tazza di tè con sterline digitali usando il tuo smartphone - basta toccarlo sullo stesso dispositivo utilizzato per le carte di credito e di debito.

15:00

Paga l'elettricista in sterline digitali - entrambi ricevi una notifica istantanea che il pagamento è completo.

18:00

Ordina generi alimentari online e pagali utilizzando l'opzione sterlina digitale sul checkout del sito web.

20:00

Trasferisci denaro dal tuo conto bancario al tuo portafoglio digitale.

Esempio riportato sul sito della Banca Centrale d'Inghilterra

La successiva fase di sviluppo è la fase implementativa in cui la banca centrale realizza le infrastrutture che verranno utilizzate per l'emissione e la gestione della valuta digitale. Attualmente, gli Stati coinvolti in questa fase sono Canada, Russia e Brasile.

La terza fase è quella di test, in cui la moneta virtuale viene sperimentata sul campo in vista di un lancio successivo. La Svezia si trova in una prima fase di test della sua e-Krona, basata su DLT privata in cui la banca svedese funge da proprietaria e decide chi può parteciparvi. Tuttavia, l'esempio più acclamato è sicuramente quello cinese, che ha coinvolto circa 35 banche commerciali. La Cina ha già emesso l'equivalente di circa 40 milioni di dollari in e-CNY, ossia la forma digitale dello Yuan. In particolare, la Banca

Popolare Cinese (BPC) si occupa solo di emettere la CBDC la quale, successivamente, viene distribuita dalle sole banche commerciali. Di fatto, la banca centrale controlla e gestisce l'e-CNY in tutte le fasi del suo percorso e traccia le transazioni di ogni wallet digitale. Nello specifico, tale moneta digitale è stata pensata per uso domestico e dunque si tratta di una CBDC di tipo *retail*, implementata su un modello ibrido che unisce i vantaggi dell'account-based e quelli del token-based. Affinché i cittadini potessero effettivamente utilizzare l'e-CNY e i suoi servizi, è stata anche rilasciata una semplice *"applicazione portafoglio"* in modo tale da rendere il sistema dello Yuan virtuale in grado di supportare l'interoperabilità con i tradizionali sistemi di pagamento elettronico e sfruttare a pieno le già esistenti infrastrutture finanziarie. Tutto ciò è stato possibile anche grazie alla compatibilità offerta dalla piattaforma di pagamento online Alipay e dal servizio di messaggistica WeChat, che con il proprio servizio di portafoglio elettronico *in-app* permette agli utenti di completare transazioni online e trasferire denaro. Inoltre, la Cina non ha escluso la possibilità di implementare una CBDC wholesale destinata alle transazioni interbancarie, istituzionali e internazionali, su cui anche il presidente della BPC ha voluto esprimere il suo parere positivo sull'adozione di un sistema DLT come base, appuntando però il problema della scalabilità.

L'ultima fase è quella di emissione, in cui la moneta virtuale viene ufficialmente lanciata all'interno della nazione in cui opera la banca centrale. Ad oggi sono poche le realtà che hanno già lanciato una propria CBDC, tra cui la Central Bank of the Bahamas nell'ottobre 2020, diventando così il primo paese al mondo ad emettere ufficialmente una CBDC e seguita successivamente dalla banca centrale della Nigeria e da quella della Cambogia. Nello specifico, quest'ultima ha rilasciato anche un'applicazione gratuita per effettuare pagamenti e trasferire denaro tramite qualsiasi

banca sulla piattaforma, anche senza disporre di un conto corrente tradizionale.

Mentre le banche centrali di tutto il mondo approfondiscono il tema delle valute digitali, Visa, una delle più note società leader nei pagamenti digitali, ha siglato una partnership con ConsenSys, società specializzata in tecnologia blockchain, con l'obiettivo di sfruttare la propria rete di reti al fine di collegare la CBDC con l'ecosistema finanziario esistente e di svilupparne l'infrastruttura, avviando il progetto *"Visa CBDC Payments Module"*.

Un'intervista pubblicata sul sito di Visa, mostra alcuni interessanti casi d'uso, tra cui l'esempio di una comunità alle prese con serie difficoltà economiche. In questo scenario, i residenti di tale comunità potrebbero ricevere nei loro wallet digitali assistenza governativa immediata, senza dover aspettare un assegno tramite posta o che i fondi siano liquidati sul conto.

Come si può notare, la situazione mondiale è molto eterogenea e merita quindi un appunto anche il concetto di *time-to-market*, fondamentale nella corsa alle CBDC. Nella sua definizione più generale, *time-to-market* indica il periodo di tempo che intercorre tra l'ideazione di un prodotto e la sua effettiva commercializzazione. Considerando i diversi livelli di avanzamento delle banche centrali, ci si interroga su quali possano essere i prossimi step per il percorso di affermazione delle CBDC. Inoltre, se da un lato è vero che la Cina potrebbe lanciare ufficialmente la propria moneta nel breve periodo, dall'altro la BCE ha previsto 24 mesi di analisi, a cui dovranno seguire una fase di sviluppo e una di test, fissando dunque un ipotetico rilascio non prima del 2025. Di conseguenza, la vera preoccupazione

riguarda la strategia cinese e come la Cina possa influenzare la politica monetaria mondiale, soprattutto senza una pronta risposta europea e statunitense, e ci si chiede se l'UE sarà ancora in tempo o se dovrebbe pensare a come fronteggiare la diffusione di valute digitali estere con delle soluzioni che abbiano un *time-to-market* ridotto.

Conclusioni

L'innovazione digitale sta velocemente ridisegnando i meccanismi di funzionamento del sistema economico-finanziario e le dinamiche sociali che orientano le iterazioni tra i cittadini, gli operatori dell'industria finanziaria e non finanziaria e le Istituzioni pubbliche.

In questa tesina vi è posta una lente di ingrandimento sul concetto di CBDC. Nel 2020 la Banca Centrale Europea ha instituito una task force con l'obiettivo di individuare delle soluzioni operative adeguate a disegnare un euro digitale. Gli esperti della task force hanno preso in considerazione e testato diverse opzioni e i risultati delle loro analisi aprono la strada a molteplici impieghi della blockchain e dell'euro programmabile nel sistema finanziario e nell'economia reale.

La più ampia e completa trasformazione digitale del sistema economico-finanziario che si desidera raggiungere in Europa, tuttavia, non potrebbe realizzarsi senza l'impegno profuso sul fronte delle conoscenze digitali dei cittadini. Infatti, il contesto che si creerebbe richiederebbe di fatti competenze specifiche.

Non sappiamo effettivamente quali saranno i reali risvolti da parte dell'Unione Europea e del mondo intero. Sicuramente dovremo ancora attendere qualche anno per avere, in Europa, una concreta soluzione e affinché il concetto e l'adozione di CBDC diventi pratico. Nel frattempo, in questa corsa alla digitalizzazione, godiamoci l'appartenenza ad un'era che potrebbe risultare una rivoluzione finanziaria e monetaria senza pari.

Sitografia

L'Europa e la sfida delle central bank digital currencies - siamo ancora in tempo?, Reply, https://www.reply.com/it/financial-services/central-bank-digital-currencies

Un euro digitale, Banca Centrale Europea, https://www.ecb.europa.eu/paym/digital_euro/html/index.it.html

CBDC e criptovalute: la corsa alla moneta digitale, Young Platform Academy, 15 settembre 2021, https://academy.youngplatform.com/blockchain/cbdc-criptovalute-moneta-digitale/#4

Massimo Amato e Alessandro Bonetti, *Dall'euro digitale cambiamenti imprevedibili. Che andranno governati*, Il sole 24 ore, 7 gennaio 2021, https://www.econopoly.ilsole24ore.com/2021/01/07/euro-moneta-digitale-cambiamenti/

The digital pound, Bank of England, https://www.bankofengland.co.uk/the-digital-pound

Uno sguardo al futuro delle valute digitali, Visa Italia, 24 gennaio 2022, https://www.visaitalia.com/visa-everywhere/blog/bdp/2022/01/13/uno-sguardo-al-1642090154018.html

Mario Di Giulio e Rosanna Tirenna, *Valute digitali, come cambia il ruolo delle banche: modelli, prospettive e sfide,* Agenda digitale, 16 marzo 2022 https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/valute-digitali-come-cambia-il-ruolo-delle-banche-modelli-prospettive-e-sfide/

Gwyneth Iredale, *Central Bank Digital Currency: Know the architecture of retail CBDC, 101 Blockchains,* 21 ottobre 2021 https://101blockchains.com/retail-cbdc-architecture/

Diego Geroni, *Understanding the types of central bank digital currencies (CBDC), 101 Blockchains,* 16 settembre 2021, https://101blockchains.com/types-of-central-bank-digital-currencies/

Elena Vianello, *La moneta virtuale: le CBDC ed il progetto dell'euro digitale, Luiss,* 2022, *http://tesi.luiss.it/33559/1/248171_VIANELLO_ELENA.pdf*

CBDC: Come evolvono le valute nell'euro delle cripto, Etherevolution , 8 marzo 2020, https://etherevolution.eu/central-bank-digital-currency/

Xuan Han, Yong Yuan, Fei-Yue Wang, *A blockchain-based framework for central bank digital currency*, IEEE Ixplore, 13 gennaio 2020, https://ieeexplore.ieee.org/abstract/document/8955032

NOSTR

UN SOCIAL NETWORK DECENTRALIZZATO

E. Abate, C. Bertolini, M. Bosio, N. Gallo

Nostr,
un social network decentralizzato

Progetto di Blockchain e Criptoeconomia

Abate E., Bertolini C., Bosio M., Gallo N.

Indice

1 Introduzione **2**
1.1 Le origini del Web 2
1.2 Il Web 1.0 2
1.3 Il Web 2.0 2
1.3.1 I primi punti deboli 3
1.4 Il Web 3.0 4

2 Nostr **6**
2.1 La struttura 6
2.1.1 Client 7
2.1.2 Relay 8
2.2 Nostr Implementation Possibilities 8
2.2.1 NIP-01, Basic protocol flow description 9
2.2.2 Altri NIP 13

3 User experience di Nostr **19**

4 Confronto con altri Social Network **21**
4.1 Confronto con Twitter 21
4.2 Confronto con Mastodon 21
4.3 Confronto con SSB 22

5 Nostr e la privacy **24**
5.1 Miglioramento della privacy e della scalabilità di BIP47 24
5.2 Nostr Pay-To-Endpoint 25
5.3 Nostr per Conjoins 27
5.4 Superamento dei requisiti IP con Nostr 28

6 Limitazioni e potenziali sviluppi **30**
6.1 Problemi di gestione delle chiavi 30
6.2 Da cosa dipende la crescita di Nostr 32
6.2.1 La pubblicità 32
6.2.2 Micropagamenti 32

7 Conclusione **34**

1 Introduzione

La nuova generazione di Internet è spesso indicata con il nome di Web 3.0 e il suo intento è quello di promuovere sempre più protocolli decentralizzati, nella speranza di ridurre la dipendenza dalle grandi multinazionali tecnologiche. Ad oggi infatti il panorama è decrivibile come un oligopolio, con enormi colossi che occupano gran parte di tutto ciò che gli utenti possono fare utilizzando Internet, basti pensare a Google, Amazon, Netflix, ecc.

1.1 Le origini del Web

Le origini del Web risalgono al periodo della Guerra Fredda, durante la quale il suo utilizzo principale aveva a che fare con la difesa e la ricerca. Successivamente, da strumento militare e scientifico, iniziò ad evolversi in qualcosa di differente: fu presto ideato un prototipo di e-mail e dopodichè varie università iniziarono a collegarsi alla rete. Da lì la crescita fu lenta ma senza sosta, sempre più agevolata dai miglioramenti tecnologici, divenendo sempre più internet come lo conosciamo oggi. Nel 1988 il finlandese Jarkko Oikarinen ideò il primo sistema di messaggistica online: IRC (Internet Relay Chat), che sopravvive ancora oggi con circa 500 network differenti e 2000 server connessi.

1.2 Il Web 1.0

La prima versione di Internet vera e propria (il cosiddetto **Web 1.0**) arrivò alla fine degli anni '90 e consisteva in una serie di collegamenti e homepage di siti non particolarmente interattivi: si poteva usufruire di una serie di contenuti gratuiti, ma pur sempre in modo passivo. Nonostante ciò, la portata di tale innovazione fu a dir poco rivoluzionaria e dirompente, in quanto generò una decentralizzazione ed una democratizzazione delle informazioni senza precedenti nella storia.

Attraverso il web era finalmente possibile comunicare con persone che altrimenti non si sarebbero mai potute incontrare o venire a conoscenza di informazioni che non si sarebbero mai potute trovare. Internet ha consentito per la prima volta di abbattere un'infinità di barriere.

1.3 Il Web 2.0

Non ci misero molto gli utenti a voler aumentare la dinamicità del sistema e a portare il web ad una nuova versione: il **Web 2.0**. L'intento questa volta era quello di occupare una posizione attiva, creando e modificando i contenuti e portando al massimo l'interazione nella rete. Un simbolo di questa nuova dinamicità è stata, ad esempio, Wikipedia (aperta all'inizio del 2001), la prima e tuttora più diffusa enciclopedia online, libera e collaborativa, a cui ogni utente può offrire il proprio contributo in termine di informazioni. Il web iniziava così ad essere interattivo. Da una fruizione puramente passiva della rete, risultato di milioni di pagine web statiche, stava diventando possibile inserire dati a supporto di applicazioni create da altre persone. Da quel punto gli utenti ebbero la possibilità non solo di consumare contenuti, ma di darne vita a nuovi e pubblicarli su versioni primordiali dei classici blog, oppure su dei forum. Uno dei fenomeni più dirompenti del Web 2.0 è stata la diffusione dei social network, capitanati da Facebook nel 2004, che ha riscosso un successo senza precedenti.

1.3.1 I primi punti deboli

Non passò molto tempo prima di vedere emergere i primi problemi. Il punto maggiormente critico del Web 2.0 è legato a privacy e trattamento dei dati personali, raccolti dai giganti della tecnologia e utilizzati per creare pubblicità e campagne di marketing su misura. Inoltre, i casi in cui le informazioni degli utenti siano state cedute o sottratte sono numerosi, senza contare le censure a cui vengono sempre più spesso sottoposti gli utenti che propongono contenuti online.

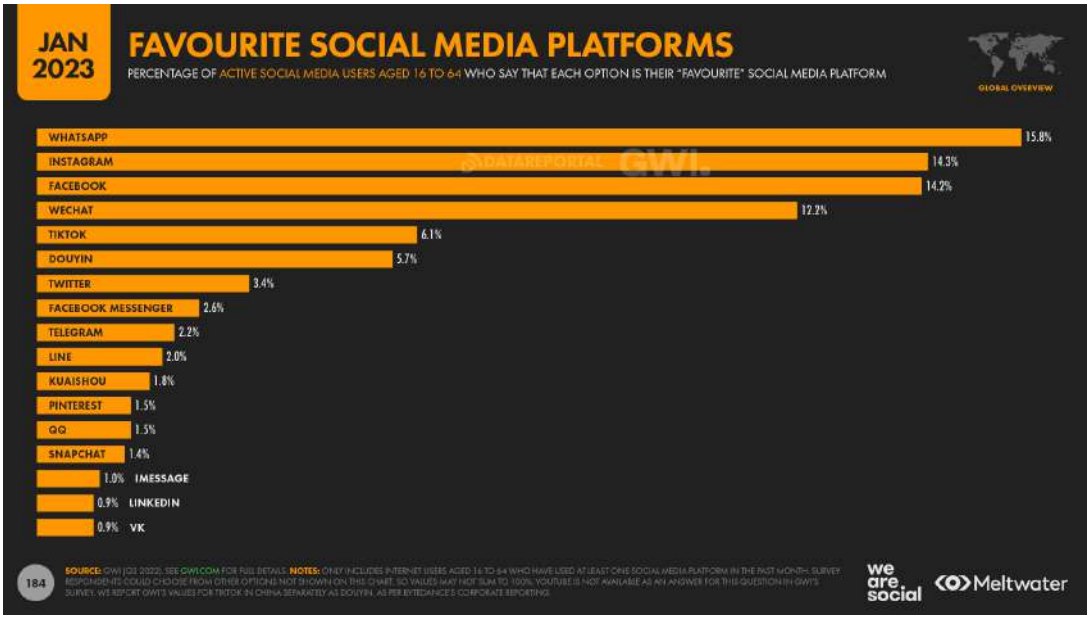


Figure 1: Whatsapp, Instragram e Facebook (tutte di Meta) sono le 3 piattaforme social più utilizzate

Ci si è trovati quindi in un sistema in cui la centralizzazione dei dati così potente da apparire sostanzialmente irreversibile, al punto che si è cercato (e si sta tuttora cercando) di porvi rimedio. Dunque, se da un lato il Web 2.0 ha portato al mondo straordinari servizi gratuiti, dall'altro ha anche stancato molti utenti, facendo in modo che si spingesse verso nuove soluzioni.

Secondo alcuni dati pubblicati all'inizio del 2022 dal World Economic Forum, Google controlla attualmente l'87% delle ricerche sulla rete, mentre Meta può contare su oltre 3,6 miliardi di utenti unici, registrati sui vari social network della holding, in particolare Facebook, Instagram e Whatsapp. Si tratta di cifre prossime al monopolio assoluto, e la cosa non sorprende se consideriamo come, già nel 2019, il 43% del traffico totale sul web fosse concentrato soltanto sui servizi di realtà come Google, Amazon, Meta, Netflix, Microsoft e Apple.

La centralizzazione dei dati costituisce e costituirà un problema enorme per la società, e bisogna tenere in considerazione anche il fatto che i governi non sono ancora riusciti a limitare in maniera efficace lo strapotere dei big tech, soprattutto a fronte di condotte discutibili dal punto di vista etico, prima ancora che normativo. Il controllo che questi fanno dei dati acquisiti dai loro utenti spesso viola evidentemente la loro privacy e, nei casi più critici, la loro libertà.

I dati stanno diventando al giorno d'oggi una fonte di ricchezza importante: chi ne dispone ed è in grado di analizzarli, sarà sicuramente in grado di arricchirsi notevolmente. Le big tech hanno teso una "trappola perfetta" a miliardi di utenti che si sono illusi di godere gratuitamente dei servizi da loro offerti, ignorando o avendo scarsa percezione delle conseguenze che il controllo dei dati immessi puntualmente comporta.

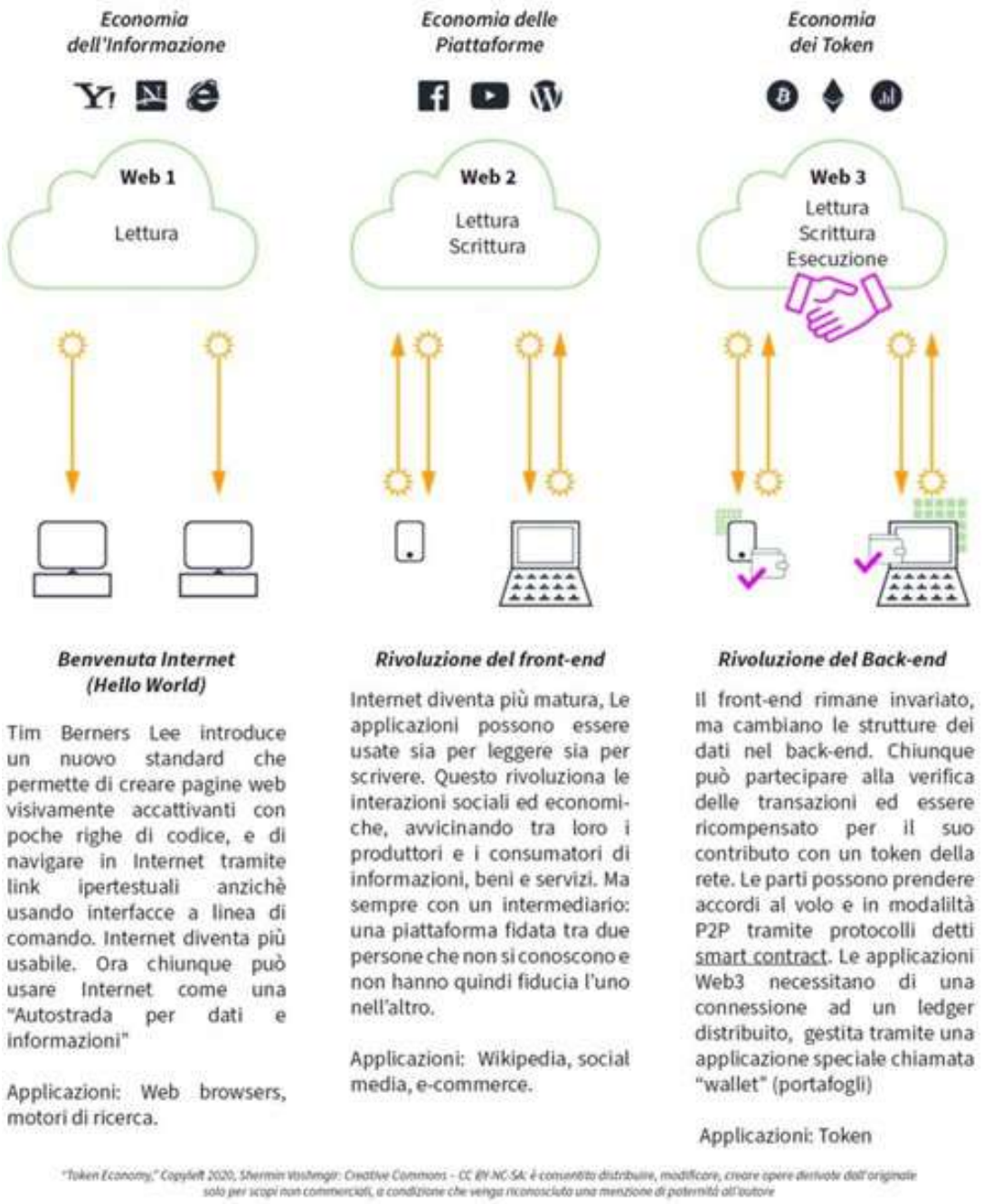


Figure 2: Il percorso del Web

1.4 Il Web 3.0

Decentralizzazione e specializzazione sono potenziali soluzioni ad alcune problematiche del Web 2.0. Da un lato, decentralizzare impedisce ad un singolo grande gestore di rac-

cogliere e trattare i dati di tutti i propri utenti per scopi pubblicitari e di imporre regole di utilizzo decise dall'alto. Dall'altro lato, creare diversi spazi dedicati per diverse comunità di utenti risolve il problema della selezione e della censura dei contenuti alla radice, in quanto saranno gli utenti stessi a selezionarsi e scegliere il network che fa per loro, con i contenuti che essi stessi desiderano vedere e condividere.

Il **Web 3.0** è una nuova fase di *lettura*, *scrittura* e *proprietà* di Internet, dove gli utenti partecipano direttamente al funzionamento dei protocolli stessi. Vede coinvolta un'ampia varietà di tecnologie, come possibile risultato delle convergenza di blockchain, NFT (Not Fungible Token), crypto (DeFi), Intelligenza Artificiale, realtà aumentata, realtà virtuale e big data con le risorse IT disponibili grazie al cloud computing.

L'obiettivo diventa quello di creare un'economia decentralizzata, aperta e permissionless, le cui applicazioni sono progettate in maniera user-centric. Il Web 3.0 è molto più di una semplice evoluzione tecnologica, in quanto comporta un autentico e radicale cambio di paradigma, in favore della più assoluta decentralizzazione. In questo mondo ideale, internet acquisirebbe una dimensione più equa ed inclusiva.

Attualmente è evidente che il Web 3.0 non rappresenti un corpus alternativo all'attuale World Wide Web, ma la sommatoria di più applicazioni distinte, ispirate da presupposti decentralizzati, sia dal punto di vista del design che delle tecnologie utilizzate per svilupparlo. Inoltre, è praticamente impossibile ad oggi fare previsioni sulla riuscita o meno dell'intento, tuttavia la sfida rappresenta un evento fondamentale nella storia della tecnologia.

2 Nostr

I social costituiscono al giorno d'oggi uno strumento potentissimo: sono un luogo dove tutti possiamo diventare "editori" ed esprimere (quasi) ogni cosa che vogliamo. Col tempo hanno acquisito sempre più potere mediatico, fino ad arrivare ad avere un grande impatto anche economico. Nonostante i loro molteplici lati positivi, hanno però dato origine a numerosi problemi, tra i quali, ad esempio, quello della censura: molto spesso infatti la libertà di espressione non è veramente raggiunta.

In un contesto del genere, Nostr nasce dall'esigenza di mantenere solo gli aspetti positivi di un social, nonchè dalla volontà di creare un ambiente libero da qualsivoglia censura e dalla possibilità di generare un profitto dall'utilizzo di un social. Per rendere possibile tutto questo, Nostr si avvale di una rete di client e relay decentralizzata e di un sistema di monetitazzione del tutto unico.

Nostr, abbreviazione di "Notes and other stuff transmitted through relays" (letteralmente "Appunti ed altre informazioni trasmesse attraverso relay"), è un nuovo protocollo di comunicazione creato nel 2021 da `fiatjaf`, uno sviluppatore di Lightning Network, una rete decentralizzata che utilizza la funzionalità degli smart contract nella blockchain per consentire pagamenti istantanei attraverso una rete di partecipanti e che ha avuto origine dal tentativo di Ben Arc (sviluppatore di LNBits) di creare un mercato completamente decentralizzato chiamato Diagon Alley.

Il protocollo Nostr consiste in un network decentralizzato non peer-to-peer basato su chiavi crittografiche, nonché una rete "sociale" globale resiliente alla censura. I suoi punti di forza sono:

- **Resilienza:** poiché Nostr non si affida a un piccolo numero di server fidati per spostare o memorizzare i dati, è molto resiliente. Anzi, è proprio la mancanza dei server all'interno della rete a rendere il protocollo decentralizzato.
- **Verificabilità:** poiché gli account Nostr si basano sulla crittografia a chiave pubblica, è facile verificare che i messaggi siano stati realmente inviati dall'utente in questione.
- **Monetizzazione:** a differenza di altre piattaforme di social media, che si basano sui ricavi pubblicitari per pagare i creatori di contenuti, Nostr consente a questi di monetizzare direttamente i loro contenuti e ricevere mance dai loro follower. I fornitori di infrastrutture di Nostr possono monetizzare in modo simile i servizi che forniscono tramite pagamenti lightning.
- **Open Source:** il codice sorgente di Nostr è disponibile e chiunque e può vederlo, usarlo e modificarlo a suo piacimento. Questo garantisce trasparenza e collaborazione nello sviluppo del protocollo.

2.1 La struttura

La struttura della rete è molto semplice. Esistono solo due tipi di nodi: **client** e **relay**.

- Ogni utente accede alla rete tramite il suo client e utilizza uno o più relay.

- Ogni utente è identificato da una chiave pubblica.
- Ogni post è firmato.
- Tutti i client validano le firme.
- I client recuperano dati da relays a scelta, i quali non parlano tra loro, ma solo direttamente agli utenti.

Ad esempio, per seguire qualcuno, un utente indica semplicemente al proprio client di interrogare i relay che conosce per i post di quella chiave pubblica.

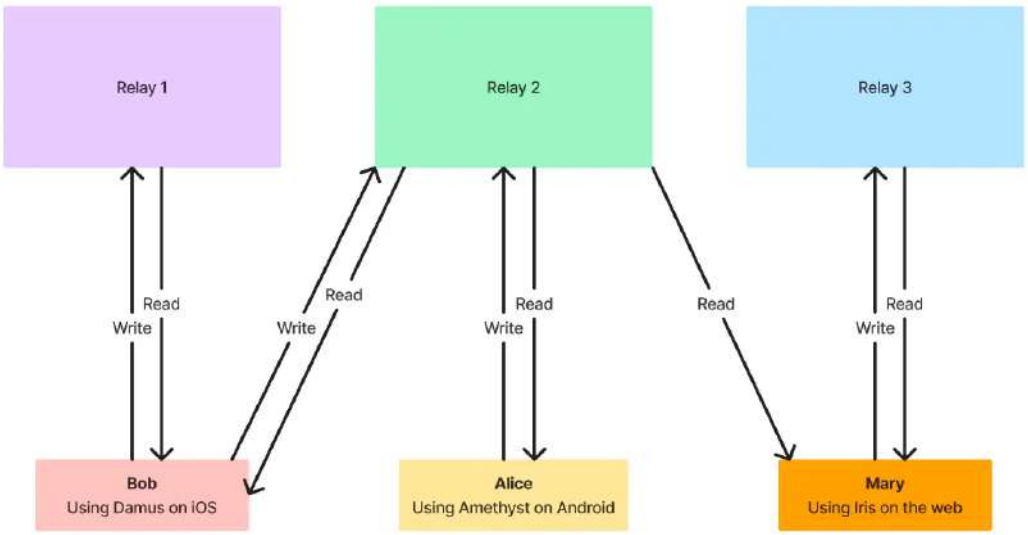


Figure 3: Rete relay-client

2.1.1 Client

I client sono dispositivi hardware e software che permettono all'utente di interfacciarsi con la rete. Ad esempio, un computer che tramite una rete informatica richiede uno o più servizi ad un server mediante uno o più protocolli di rete è un *client hardware*. Invece un programma di posta elettronica, come Outlook, Thunderbird o Eudora, che interroga un server di posta elettronica attraverso il protocollo di transmissione è un *client software*. In definitiva, il client all'interno della rete rappresenta l'utente che si connette.

Dato che Nostr è un protocollo molto flessibile, esistono molteplici client sia hardware che software. Questi sono connessi solo a nodi relay (poiché il protocollo Nostr non è peer to peer) e comunicano attraverso il **protocollo WebSocket**, che fornisce canali di trasmissione bidirezionale simultanea (full-duplex, cioè client e relay possono comunicare in contemporanea l'uno con l'altro).
Qui di seguito una lista di client più usati:

- **Web:** Astral, Snort, Coracle, Iris, Yosup, Primal;
- **iOS:** Nos, Damus;

- **Android:** Nostros, Amethyst, Camelus, Nozzle;
- **iOS e Android:** Plebstr, Current;
- **Desktop:** Gossip, More-speech, Lume.

2.1.2 Relay

I Relay sono come i server nel "dietro le quinte" di Nostr e permettono al client di scrivere messaggi che possono essere o meno memorizzati e passati agli altri client connessi al relay. L'universo dei relay cambia molto velocemente per cui si prevedono dei grossi cambiamenti nel il futuro.

E' da notare che, poichè Nostr è un social decentralizzato e dipende dai relay per memorizzare e trasmettere dati, se si nota che il relay a cui è collegato il proprio client è lento, se ne possono agganciare di ulteriori così da velocizzarlo. E' proprio la possibilità di agganciare più relay che "garantisce" in un certo qual modo l'incensurabillità dell'account: più relay si agganciano, meglio ci si potrà difendere dalla censura. Inoltre, se il collegare più relay non dovesse ancora far sentire abbastanza al sicuro dalla censura, su Nostr è anche possibile creare il proprio relay. Questo garantirebbe di avere sempre a disposizione una copia dei propri post e messaggi all'interno di Nostr.

2.2 Nostr Implementation Possibilities

I NIP (Nostr Implementation Possibilities) esistono per promuovere l'interoperabilità, infatti documentano ciò che può essere implementato da un software relay e client Nostr compatibile. Per uno sviluppatore non è una buona idea trovare delle soluzioni a problemi comuni e implementarle solo nella propria app: è meglio per tutti implementare soluzioni compatibili tra loro e disponibili a più persone. I NIP esistono per coordinare questo processo. Allo stesso modo, una nuova idea potrebbe sembrare ottima solo sull'app di alcuni sviluppatori, ma sarà sicuramente molto meglio se molte altre app implementano lo stesso standard e possono interagire bene. Tutti i NIP sono di dominio pubblico.

Ora, la domanda sorge spontanea: perchè uno sviluppatore dovrebbe pensare agli interessi di tutti e della rete in generale, e non solamente ad ottimizzare le sue applicazioni? La risposta è che Nostr è totalmente decentralizzato e non è di proprietà di un servizio centralizzato (come ad esempio Twitter). Ciò significa che di fatto la direzione del protocollo è nelle mani di tutti noi. Possiamo suggerire e promuovere modifiche e offrire un feedback sulle idee proposte dagli altri. Essere una parte attiva della comunità dà il "potere" di influenzare la direzione della rete. I NIP pubblicati nel repository principale sono già approvati. L'aggiunta di nuove idee avviene tramite una Pull Request su quel repository.

Ci sono alcuni criteri per l'accettazione dei NIP:

- Dovrebbero essere implementati in almeno due client e un relay, quando applicabile.
- Dovrebbero avere un senso.
- Dovrebbero essere opzionali e retrocompatibili. Bisogna fare attenzione che i client

e i relay che scelgono di non implementarli non smettano di funzionare quando interagiscono con quelli che scelgono di farlo.

- Non dovrebbe esserci più di un modo per fare la stessa cosa.
- Altre regole possono essere stabilite quando necessario.

2.2.1 NIP-01, Basic protocol flow description

Il NIP-01 descrive il protocollo di base che dovrebbe essere implementato da tutti.

- Ogni utente ha una coppia di chiavi.
- Firme, chiavi pubbliche e codifiche sono fatte con le firme standard di Schnorr per la curva `secp256k1`.
- Gli eventi sono l'unità atomica del protocollo Nostr e sono l'unico tipo di oggetto presente sul network.

Gli eventi hanno la seguente forma:

```
{
  "id": <32-bytes lowercase hex-encoded sha256 of the serialized event data>
  "pubkey": <32-bytes lowercase hex-encoded public key of the event creator>,
  "created_at": <unix timestamp in seconds>,
  "kind": <integer>,
  "tags": [
    ["e", <32-bytes hex of the id of another event>, <recommended relay URL>],
    ["p", <32-bytes hex of a pubkey>, <recommended relay URL>],
    ... // other kinds of tags may be included later
  ],
  "content": <arbitrary string>,
  "sig": <64-bytes hex of the signature of the sha256 hash of the serialized event data, same as "id">
}
```

Per ottenere l'id, basta usare `sha256` sull'evento serializzato. La serializzazione è fatta sulla stringa serializzata `UTF-8 JSON` (senza spazi o trattini) con la seguente struttura:

```
[
  0,
  <pubkey, as a (lowercase) hex string>,
  <created_at, as a number>,
  <kind, as a number>,
  <tags, as an array of arrays of non-null strings>,
  <content, as a string>
]
```

La proprietà `created_at` è un timestamp UNIX impostato dal creatore dell'evento, normalmente al momento in cui è stato creato anche se, non essnedo critico, non vengono fatti controlli che sia effettivamente così.
Il `kind` è un numero intero che indica il tipo di evento, quelli basici sono:

- **0**: è un evento "metadati", il contenuto è un oggetto JSON stringato

  `{name: <username>, about: <string>, picture: <url, string>}`,

  utilizzato dagli utenti per fornire dettagli su se stessi, ad esempio il nome e l'immagine del profilo. Un relay può eliminare i metadati vecchi quando ne ha uno nuovo per la stessa chiave pubblica.

- **1**: è una nota di testo, cioè una normale, semplice e breve nota in chiaro, destinata

ad essere utilizzata nel feed, con risposte e commenti simili a Twitter. Si possono mantenere molti eventi di tipo 1 per ogni chiave.

- **2**: è il recommendserver, in cui il contenuto è un URL di un relay che il creatore dell'evento vuole raccomandare ai suoi follower.

I `tag` dipendono anche dal tipo, ma alcuni tag comuni che di solito appaiono in eventi `kind:1` (ma anche in altri tipi) sono `"p"`, che viene utilizzato per menzionare una chiave pubblica ed `"e"`, usato per riferirsi a un altro evento.

Per quanto riguarda la comunicazione tra client e relay, i relay espongono un *endpoint WebSocket* a cui i client possono connettersi. Il client può inviare al relay degli eventi e creare sottoscrizioni attraverso 3 tipi di messaggi, che devono essere array JSON, secondo i seguenti modelli:

- `["EVENT", <event JSON as defined above>]`, utilizzato per pubblicare eventi.
- `["REQ", <subscription_id>, <filters JSON>...]`, utilizzato per richiedere eventi e sottoscrivere nuovi aggiornamenti.
- `["CLOSE", <subscription_id>]`, utilizzato per interrompere le sottoscrizioni precedenti.

In particolare, `<subscription_id>` è una stringa arbitraria, non vuota, di lunghezza massima di 64 caratteri, che deve essere utilizzata per rappresentare una sottoscrizione. `<filters>` è un oggetto JSON che determina quali eventi verranno inviati in tale sottoscrizione, può avere i seguenti attributi:

```
{
  "ids": <a list of event ids or prefixes>,
  "authors": <a list of pubkeys or prefixes, the pubkey of an event must be one of these>,
  "kinds": <a list of a kind numbers>,
  "#e": <a list of event ids that are referenced in an "e" tag>,
  "#p": <a list of pubkeys that are referenced in a "p" tag>,
  "since": <an integer unix timestamp, events must be newer than this to pass>,
  "until": <an integer unix timestamp, events must be older than this to pass>,
  "limit": <maximum number of events to be returned in the initial query>
}
```

Dopo aver ricevuto un messaggio `REQ`, il relay dovrebbe interrogare il proprio database interno e restituire gli eventi che corrispondono al filtro, quindi archiviare tale filtro e inviare nuovamente tutti gli eventi futuri ricevuti allo stesso websocket fino alla chiusura del websocket. L'evento `CLOSE` viene ricevuto con lo stesso `<subscription_id>` o viene inviato un nuovo `REQ` utilizzando lo stesso `<subscription_id>`, nel qual caso dovrebbe sovrascrivere la sottoscrizione precedente.

Gli attributi di filtro contenenti elenchi (ad esempio id, tipi o #e) sono matrici JSON con uno o più valori. Almeno uno dei valori della matrice deve corrispondere al campo pertinente in un evento affinché la condizione stessa possa essere considerata una corrispondenza. Per gli attributi di evento scalari come il tipo, l'attributo dell'evento deve essere contenuto nell'elenco dei filtri. Per gli attributi di tag come #e, in cui un evento può avere più valori, i valori delle condizioni di evento e filtro devono avere almeno un elemento in comune.

Gli elenchi `ids` e `authors` contengono stringhe esadecimali minuscole, che possono corrispondere esattamente a 64 caratteri o a un prefisso del valore dell'evento. Una corrispondenza di prefisso è quando la stringa di filtro è un prefisso stringa esatto del valore dell'evento. L'uso di prefissi consente filtri più compatti in cui viene interrogato un numero elevato di valori e può fornire una certa privacy per i client che potrebbero non voler rivelare gli autori o gli eventi esatti che stanno cercando.

Tutte le condizioni di un filtro specificate devono corrispondere a un evento affinché possa passare il filtro, ovvero più condizioni vengono interpretate come condizioni &&.

Un messaggio `REQ` può contenere più filtri. In questo caso, gli eventi che corrispondono a uno qualsiasi dei filtri devono essere restituiti, ovvero più filtri devono essere interpretati come condizioni ||.

La proprietà `limit` di un filtro è valida solo per la query iniziale e può essere ignorata in seguito. Quando `limit:n` è presente, si presuppone che gli eventi restituiti nella query iniziale saranno gli ultimi n eventi. È sicuro restituire meno eventi di quanto specificato dal limite, ma si prevede che i relay non restituiscano più eventi di quelli richiesti in modo che i client non vengano inutilmente sopraffatti dai dati.

I Relay possono mandare tre tipi di messaggi ai client, i quali devono essere array JSON, secondo i seguenti modelli:

- `["EVENT", <subscription_id>, <event JSON as defined above>]`, utilizzato per inviare eventi richiesti dai client.
- `["EOSE", <subscription_id>]`, utilizzato per indicare la fine degli eventi memorizzati e l'inizio degli eventi appena ricevuti in tempo reale.
- `["NOTICE", <message>]`, usati per inviare messaggi di errore leggibili dall'uomo o altre cose ai client. Questo NIP non definisce regole su come i messaggi `NOTICE` devono essere inviati o trattati.

I messaggi `EVENT` devono essere inviati solo con un `subscription_id` correlato a una sottoscrizione precedentemente avviata dal client (utilizzando il messaggio `REQ` sopra).

Valgono inoltre le seguenti considerazioni:

- I client non devono aprire più di un websocket per ogni relay. Un canale può supportare un numero illimitato di abbonamenti.
- L'array di `tag` può memorizzare un identificatore di tag come primo elemento di ogni sottoarray, oltre ad informazioni arbitrarie in seguito (sempre come stringhe). Questo NIP definisce "p" (che sta per "pubkey" e che indica una chiave pubblica di qualcuno a cui si fa riferimento nell'evento) ed "e" (che significa "evento" e che indica l'id di un evento che questo evento sta citando, rispondendo o a cui si riferisce in qualche modo).
- L'elemento `<URL di inoltro consigliato>` presente sui tag "e" e "p" è un URL facoltativo (potrebbe essere impostato su "") di un inoltro che il client potrebbe tentare di connettere per recuperare l'evento taggato o altri eventi da un profilo

con tag. Può essere ignorato, ma esiste per aumentare la resistenza alla censura e rendere la diffusione degli indirizzi di inoltro più fluida tra i client.

- I client devono utilizzare il campo `created_at` per giudicare l'età di un evento di metadati e sostituire completamente gli eventi di metadati meno recenti con eventi di metadati più recenti, indipendentemente dall'ordine in cui arrivano. I client non devono unire i campi compilati all'interno di eventi di metadati meno recenti in campi vuoti di eventi di metadati più recenti.

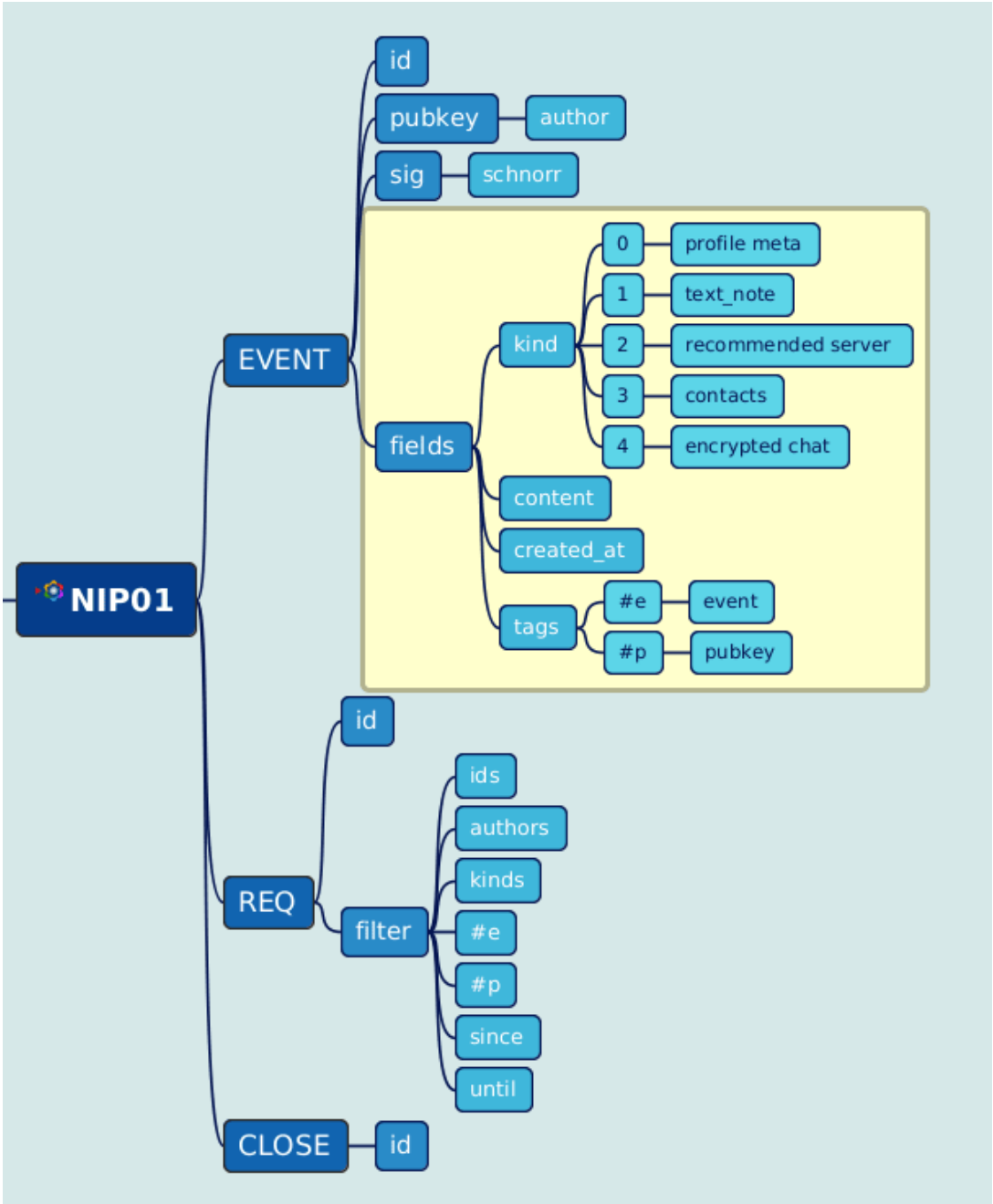


Figure 4: Rappresentazione del NIP-01

2.2.2 Altri NIP

Generalmente, sono necessari solamente eventi di tipo 0 e 1 per costruire un'app Nostr di social networking di base, ma altri tipi sono stati inventati per necessità dagli utenti, per fornire funzionalità aggiuntive. Alcuni tipi infatti, non sono correlati al social networking e soddisfano altre esigenze specifiche per queste altre funzionalità. L'idea è che, per ogni nuovo caso d'uso che si possa pensare in Nostr, un sottoprotocollo debba essere pensato e proposto come un NIP, per la massima interoperabilità tra gli utenti esistenti e futuri che potrebbero essere interessati a implementare tale funzionalità, garantendo al contempo la compatibilità con le versioni precedenti e piacevoli fallback per tutto ciò che esiste e non si vuole cambiare. Vediamone alcuni esempi.

Il **NIP-02** è "Contact list and pet names". Un evento speciale con `kind:3`, che significa "elenco di contatti" è definito come un elenco di tag `p`, uno per ciascuno dei profili seguiti o noti che si sta seguendo. Ogni entrata del tag deve contenere la chiave per il profilo, un URL di inoltro in cui è possibile trovare gli eventi di quella chiave (può essere impostato su una stringa vuota se non necessario) e un soprannome (o "petname") per quel profilo (può anche essere impostato su una stringa vuota o non fornito), cioè,

```
["p", <32-bytes hex key>, <main relay URL>, <petname>].
```

Il contenuto può essere qualsiasi cosa e dovrebbe essere ignorato. Ad esempio:

```
{
  "kind": 3,
  "tags": [
    ["p", "91cf9..4e5ca", "wss://alicerelay.com/", "alice"],
    ["p", "14aeb..8dad4", "wss://bobrelay.com/nostr", "bob"],
    ["p", "612ae..e610f", "ws://carolrelay.com/ws", "carol"]
  ],
  "content": "",
  ...other fields
}
```

Ogni nuovo elenco di contatti che viene pubblicato sovrascrive quelli passati, quindi dovrebbe contenere tutte le voci. I relay e i client dovrebbero eliminare gli elenchi di contatti passati non appena ne ricevono uno nuovo. Ci sono molteplici usi:

- Backup della lista di contatti. Se si ritiene che un relay memorizzerà i propri eventi per un tempo sufficiente, è possibile utilizzare questo evento di tipo 3 per eseguire il backup dell'elenco seguente e ripristinarlo su un dispositivo diverso.

- Individuazione del profilo e aumento del contesto. Un cliente può fare affidamento sull'evento `kind:3` per visualizzare un elenco di persone seguite dai profili che si sta navigando, fare elenchi di suggerimenti su chi seguire in base alle liste di contatti di altre persone che si potrebbero seguire o navigare o mostrare i dati in altri contesti.

- Relay sharing. Un client può pubblicare un elenco completo di contatti con buoni relay per ciascuno dei suoi contatti in modo che altri client possano utilizzarli per aggiornare i loro elenchi di inoltro interni, se necessario, aumentando la resistenza alla censura.

- Schema di petname. I dati di questi elenchi di contatti possono essere utilizzati dai client per costruire tabelle locali "petname" derivate da elenchi di contatti di altre persone. Ciò allevia la necessità di nomi globali leggibili dall'uomo. Per esempio,

un utente ha un elenco di contatti interno così:

```
[
  ["p", "21df6d143fb96c2ec9d63726bf9edc71", "", "erin"]
]
```

e riceve due liste di contatti, una da `21df6d143fb96c2ec9d63726bf9edc71` che dice:

```
[
  ["p", "a8bb3d884d5d90b413d9891fe4c4e46d", "", "david"]
]
```

e un'altra da `a8bb3d884d5d90b413d9891fe4c4e46d` che dice:

```
[
  ["p", "f57f54057d2a7af0efecc8b0b66f5708", "", "frank"]
]
```

Quando l'utente vede

`21df6d143fb96c2ec9d63726bf9edc71`,

il client può mostrare *erin*.

Quando invece l'utente vede

`a8bb3d884d5d90b413d9891fe4c4e46d`,

il client può mostrare *david.erin*.

Infine, quando l'utente vede

`f57f54057d2a7af0efecc8b0b66f5708`,

il client può mostrare *frank.david.erin*.

Il **NIP-05** viene utilizzato per associare un nome comprensibile all'occhio umano a una data chiave pubblica. Durante gli eventi di tipo 0 (`set_metadata`), è possibile specificare la chiave `nip05` con un identificatore di internet (simile a un indirizzo email) come valore. NIP-05 assume che la parte `<local-part>` sarà limitata ai caratteri $a - z0 - 9$ e non farà distinzione tra maiuscole e minuscole. Al vedere ciò, il client suddivide l'identificatore in `<local-part>` e `<domain>` ed utilizza questi valori per effettuare una richiesta `GET` a

`https://<domain>/.well-known/nostr.json?name=<local-part>`.

Il risultato dovrebbe essere un oggetto JSON con una chiave "names" che a sua volta dovrebbe essere un mapping di nomi a chiavi pubbliche formattate in esadecimale. Se la chiave pubblica per il dato `<name>` corrisponde alla chiave pubblica dell'evento `set_metadata`, il client deduce quindi che la chiave pubblica fornita può effettivamente essere referenziata dal suo identificatore. Per esempio, se un client vede un evento come:

```
{
  "pubkey": "b0635d6a9851d3aed0cd6c495b282167acf761729078d975fc341b22650b07b9",
  "kind": 0,
  "content": "{\"name\": \"bob\", \"nip05\": \"bob@example.com\"}"
  ...
}
```

allora manderà una `GET` request a

`https://example.com/.well-known/nostr.json?name=bob`

a cui seguirà una risposta simile a

```
{
  "names": {
    "bob": "b0635d6a9851d3aed0cd6c495b282167acf761729078d975fc341b22650b07b9"
  }
}
```

oppure specificando anche il campo opzionale `relays`, dove saranno specificati i relays in cui trovare l'user specificato:

```
{
  "names": {
    "bob": "b0635d6a9851d3aed0cd6c495b282167acf761729078d975fc341b22650b07b9"
  },
  "relays": {
    "b0635d6a9851d3aed0cd6c495b282167acf761729078d975fc341b22650b07b9":
        [ "wss://relay.example.com", "wss://relay2.example.com" ]
  }
}
```

Un client può anche implementare il supporto per trovare le chiavi pubbliche degli utenti dagli identificatori di internet, il flusso è lo stesso di quanto descritto sopra, ma invertito: prima il client recupera l'URL ben noto e da lì ottiene la chiave pubblica dell'utente, quindi cerca di recuperare l'evento di tipo 0 per quell'utente e verifica se ha un "nip05" corrispondente.

Il **NIP-13** è la "Proof of work" di Nostr. Infatti, questo NIP definisce un modo per generare e interpretare Proof of Work per le note di Nostr.

La Proof of Work (PoW) è un modo per aggiungere una prova di lavoro computazionale ad una nota e costituisce una prova portante che tutti i relay e i client possono convalidare universalmente con una piccola quantità di codice. Può anche essere utilizzata come mezzo di deterrenza dallo spam.
La difficoltà è definita come il numero di zero bit iniziali nell'ID NIP-01. Ad esempio, l'id

`000000000e9d97a1ab09fc381030b346cdd7a142ad57e6df0b46dc9bef6c7e2d`

ha una difficoltà di 36 (ha 36 bit iniziali 0). 002F... è 0000 0000 0010 1111... in binario, che ha 10 zeri iniziali. Non bisogna dimenticare di contare gli zeri iniziali per le cifre esadecimali <= 7.
Per generare PoW per una nota NIP-01, viene utilizzato un tag nonce:

`"content": "It's just me mining", "tags": [["nonce", "1", "21"]]`

Durante il mining, la seconda voce del tag nonce viene aggiornata e quindi l'id viene ricalcolato. Se l'id ha il numero desiderato di zero bit iniziali, la nota è estratta. Si

consiglia di aggiornare anche il `created_at` durante questo processo. La terza voce al tag nonce dovrebbe contenere la difficoltà target. Ciò consente ai clienti di proteggersi da situazioni in cui gli spammer di massa che prendono di mira una difficoltà inferiore sono fortunati e corrispondono a una difficoltà più alta. Impegnarsi in una difficoltà target è qualcosa che tutti i minatori onesti dovrebbero essere disposti a fare, e i client possono rifiutare una nota corrispondente a una difficoltà target se manca un impegno di difficoltà.

Per quanto riguarda la validazione, qui di seguito viene riportato un codice C di riferimento per calcolare la difficoltà (ovvero il numero di bit zero iniziali) in un ID evento Nostr:

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int countLeadingZeroes(const char *hex) {
    int count = 0;

    for (int i = 0; i < strlen(hex); i++) {
        int nibble = (int)strtol((char[]){hex[i], '\0'}, NULL, 16);
        if (nibble == 0) {
            count += 4;
        } else {
            count += __builtin_clz(nibble) - 28;
            break;
        }
    }

    return count;
}

int main(int argc, char *argv[]) {
    if (argc != 2) {
        fprintf(stderr, "Usage: %s <hex_string>\n", argv[0]);
        return 1;
    }

    const char *hex_string = argv[1];
    int result = countLeadingZeroes(hex_string);
    printf("Leading zeroes in hex string %s: %d\n", hex_string, result);

    return 0;
}
```

Poiché i relay consentono la ricerca sui prefissi, è possibile utilizzarli come un modo per filtrare le note di una certa difficoltà:

```
$ echo '["REQ", "subid", {"ids": ["000000000"]}]'  | websocat wss://some-relay.com | jq -c '.[2]'
{"id":"000000000121637feeb68a06c8fa7abd25774bdedfa9b6ef648386fb3b70c387", ...}
```

Infine, poiché l'ID della nota NIP-01 non si impegna in alcuna firma, la PoW può essere esternalizzata ai fornitori di PoW, anche a pagamento. Ciò fornisce ai clienti un modo per far arrivare i loro messaggi a relay con restrizioni PoW senza dover fare alcun lavoro da soli, il che è utile per dispositivi con energia limitata come i telefoni cellulari.

Il **NIP-25** viene utilizzato per standardizzare le reazioni. Una reazione è una nota di tipo 7 che viene utilizzata per reagire ad altre note. La reazione generica, rappresentata dal contenuto impostato su una stringa preceduta da "+", dovrebbe essere interpretata come un "mi piace" o un "upvote" mentre una reazione con il contenuto impostato su "-" dovrebbe essere interpretata come un "non mi piace" o un "downvote". Un client potrebbe anche scegliere di contare i mi piace rispetto ai non mi piace in un sistema simile a Reddit di upvote e downvote, o visualizzarli come conteggi separati. Il contenuto potrebbe essere un emoji, in questo caso potrebbe essere interpretato come un "mi piace" o "non

mi piace", oppure il client potrebbe visualizzare questa reazione emoji nel post.

Il **NIP-40** è la "Expiration timestamp". Il tag di scadenza consente agli utenti di specificare un timestamp UNIX in cui il messaggio deve essere considerato scaduto (da relay e client) e deve essere eliminato dai relay. Dunque:

```
tag: expiration
values:
 - [UNIX timestamp in seconds]: required
```

Ad esempio:

```
{
    "pubkey": "<pub-key>",
    "created_at": 1000000000,
    "kind": 1,
    "tags": [
      ["expiration", "1600000000"]
    ],
    "content": "This message will expire at the specified timestamp and be deleted by relays.\n",
    "id": "<event-id>"
}
```

Si noti che il timestamp deve essere nello stesso formato del timestamp `created_at` e deve essere interpretato come l'ora in cui il messaggio deve essere eliminato dai relay. I client devono comportarsi nel seguente modo:

- I client devono utilizzare il campo `supported_nips` per sapere se un relay supporta questo NIP. I client non devono inviare eventi di scadenza a relay che non supportano questo NIP.
- I client dovrebbero ignorare gli eventi scaduti.

I relay devono avere il seguente comportamento:

- I relay non possono eliminare i messaggi scaduti immediatamente alla scadenza e possono mantenerli a tempo indeterminato.
- I relay non devono inviare eventi scaduti ai client, anche se sono archiviati.
- I relay dovrebbero eliminare tutti gli eventi pubblicati se sono scaduti.
- Un timestamp di scadenza non influisce sull'archiviazione di eventi effimeri.

Si suggerisce l'uso di timestamp di scadenza nei seguenti casi:

- Annunci temporanei. Ad esempio, un organizzatore di eventi potrebbe utilizzare questo tag per pubblicare annunci su un evento imminente.
- Offerte a tempo limitato. Questo tag può essere utilizzato dalle aziende per fare offerte a tempo limitato che scadono dopo un certo periodo di tempo.

Bisogna fare attenzione al fatto che gli eventi potrebbero essere scaricati da terze parti in quanto sono accessibili al pubblico tutto il tempo sui relay. Quindi non bisogna considerare i messaggi in scadenza come una funzione di sicurezza per le proprie conversazioni o altri usi.

Il **NIP-50** è stato proposto per fornire una funzione di ricerca generale, oltre alle query strutturate basate su tag o ID. I dettagli degli algoritmi di ricerca possono variare a seconda del tipo di evento, ma questa NIP descrive solo un framework generale ed estendibile per eseguire tali query. Il campo di ricerca è una stringa che descrive una query in forma leggibile dall'utente, ad esempio "migliori app Nostr". I relays dovrebbero interpretare al meglio la query e restituire gli eventi corrispondenti confrontando la query con il contenuto del campo degli eventi e, se ha senso nel contesto di un tipo specifico, possono confrontarla anche con altri campi.

```
{
  ...
  "search": <string>
}
```

I client possono specificare diversi filtri di ricerca, ad esempio:

```
["REQ", "", { "search": "arancione" }, { "kinds": [1, 2], "search": "viola" }]
```

includendo tipi, ID e altri campi di filtro per limitare i risultati della ricerca a determinati tipi di evento.

I client dovrebbero utilizzare il campo `supported_nips` per verificare se un relay supporta i filtri di ricerca e in caso affermativo potrebbero inviare query di filtro di ricerca a qualsiasi relay, se sono pronti a filtrare le risposte superflue dai relays che non supportano questa NIP. Inoltre sarebbe buona pratica interrogare diversi relays che supportano questa NIP per compensare eventuali differenze di implementazione tra i relays e eventualmente, dopo aver verificato che gli eventi restituiti da un relay corrispondano alla query specificata in un modo che sia adatto al caso d'uso del client, potrebbero smettere di interrogare i relays che hanno una bassa precisione.

3 User experience di Nostr

Essendo Nostr open source, chiunque può implementare il suo front-end come più ritiene, opportuno scegliendo quali NIP implementare e quali no. Per questo motivo la user experience varia molto da client a client.

Di seguito verrà utilizzato il web client `https://coracle.social` per mostrare come creare un account di prova e interagire con l'applicazione usando le funzionalità messe a disposizione.

Prima di tutto sarà necessario creare un account che consiste effettivamente nel creare una chiave privata con la quale firmeremo le nostre note. Questo passaggio può essere fatto direttamente nel client oppure, in modo più sicuro, attraverso l'utilizzo di un wallet esterno come Alby.

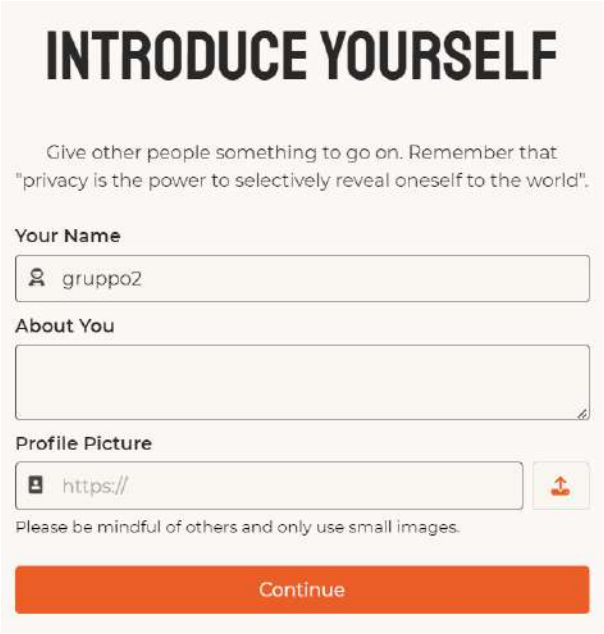


Figure 5: Sign up form

Sucessivamente, utilizzando il tab "Search" possiamo cercare utenti che dopo aver seguito compariranno nel nostro feed esattamente come Twitter.

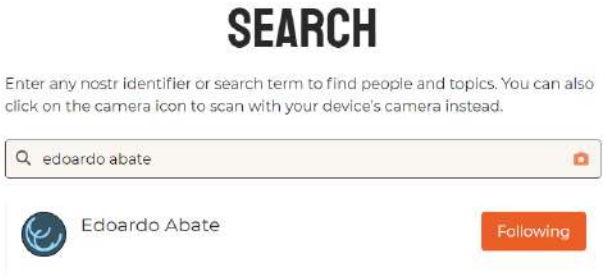


Figure 6: Search tab

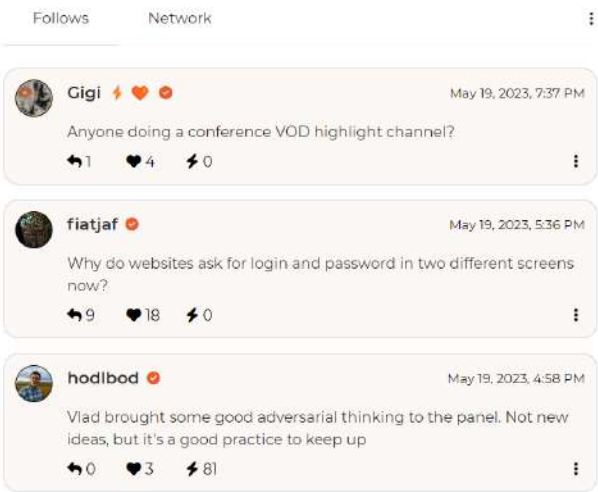


Figure 7: Feed

Implementate nel client "coracle" possiamo trovare altre funzioni come i messaggi privati o le chat di gruppo.

Figure 8: Chat

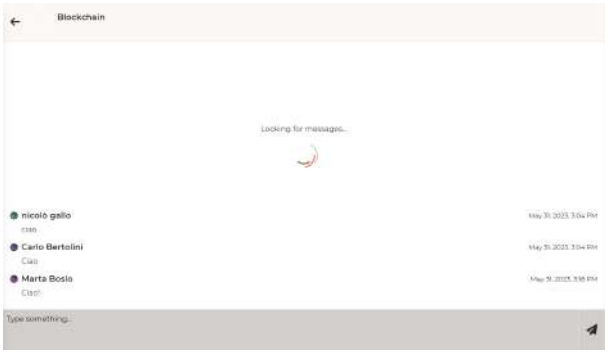


Figure 9: Chat di gruppo

4 Confronto con altri Social Network

Nostr non è il primo progetto che ha alla base l'idea del social media "aperto". Anche se attualmente per l'utente medio la maggior parte dei social può sembrare un luogo dove poter condividere liberamente i propri pensieri e i propri contenuti, è inutile dire che questa libertà è purtroppo solo apparente. I social più utilizzati al giorno d'oggi sono infatti tutt'altro che aperti e liberi. In molti stanno cercando di allontanarsi dai sistemi attuali e, come Nostr, si stanno sviluppando molte altre idee simili, per esempio quella di Mastodon, un software libero e una rete sociale di microblogging decentralizzato che permette di pubblicare messaggi brevi.

4.1 Confronto con Twitter

Il confronto più naturale e diretto per Nostr è quello con Twitter, anche se non è nella ricerca delle caratteristiche di ques'ultimo che sta la vera sfida di Nostr. Infatti, definire Nostr come un "Twitter decentralizzato" sarebbe veramente molto riduttivo.

La filosofia alla base di Nostr è ben più profonda: voler diventare uno standard tecnologico fondamentale per il futuro dei social, ma soprattutto per la condivisione dei dati in senso generale, mettendo al centro questioni chiave come proprietà dei dati e privacy. In quest'ottica, la tecnologia deiventerebbe uno strumento realmente utile alle persone, in grado di migliorare la capacità di interazione, di condivisione e di costruzione di un dibattito pubblico reale. Tutto ciò grazie alla possibilità che le persone siano proprietarie dei propri dati. Le reti sociali decentralizzate come Nostr danno agli utenti un maggiore controllo sui propri dati e comunicazioni anziché affidarsi a server centralizzati o intermediari per gestire e archiviare le informazioni. Nostr aiuta a proteggere la privacy degli utenti e a prevenire violazioni dei dati.

Su Nostr chiunque può gestire un relay il cui compito è semplicemente accettare i post da alcune persone e inoltrarli ad altre. "I relay non devono essere affidabili. Le firme vengono verificate sul lato client", afferma Nostr. Utilizzando questo sistema, Nostr risolve i problemi di censura, divieto degli utenti, chiusura dei server, spam, archiviazione dei dati e contenuti pesanti come i video.

Una curiosità che lega Nostr a Twitter: la piattaforma sta ricevendo molto sostegno dallo stesso ex CEO di Twitter Jack Dorsey che ha donato circa 14 BTC per finanziare lo sviluppo di Nostr. Dorsey ha anche consigliato a Musk di non combattere Nostr perché potrebbe essere "l'unica cosa che può salvare la sua attività", notando che il problema politico centrale di Twitter è un'insidia per i contenuti che controllano in modo esclusivo.

4.2 Confronto con Mastodon

Come detto in precedenza, l'ambizione di Nostr non è assolutamente unica nel suo genere. Un social simile e molto in crescita al momento è Mastodon.

Mastodon è una piattaforma open source nata nel 2016, il cui codice sorgente può essere modificato, o meglio migliorato, da chiunque. Il social non appartiene a nessuna grande big tech, non ci sono algoritmi che individuano le preferenze degli utenti per sug-

gerirgli post da leggere e non ha nemmeno pubblicità. Non c'è un server centralizzato, ma una rete di server federati tra loro.

Mastodon sembrava una grande iniziativa per decentralizzare i social media un decennio fa, quando Internet era più amichevole e ci si poteva fidare che i proprietari di server fossero cooperativi, ma in realtà non affronta la questione cruciale della censura.

Le principali limitazioni di Mastodon, che Nostr cerca di superare, sono:

- Le identità degli utenti sono associate a nomi di dominio controllati da terze parti e queste possono bannare gli utenti, proprio come le piattaforme di social media centralizzate. I proprietari di server possono anche bloccare altri server.
- La migrazione tra i server è difficile e può essere eseguita solo se i server cooperano.
- Mastodon è un'implementazione del protocollo ActivityPub, protocollo complesso e difficile da implementare. Infatti, nessuno lo implementa davvero per intero e la maggior parte dei server cerca solo di essere compatibile con qualunque cosa Mastodon faccia, e anche in questo caso non è efficiente.
- Non ci sono chiari incentivi per eseguire i server, quindi tendono ad essere gestiti da appassionati e persone che vogliono avere il proprio nome associato a un dominio interessante.
- Poiché i server tendono ad essere gestiti da dilettanti, vengono spesso abbandonati.
- Ci sono problemi con la duplicazione dei dati tra i server.

Tuttavia ci sono anche delle buone idee nel progetto di Mastodon, che Nostr cerca di seguire. Una buona idea che Nostr prende da Mastodon è che utilizza una rete di server, e quindi gli utenti non devono eseguire i server da soli. Inoltre, questi server generalmente hanno i propri utenti e sono gestiti e utilizzati da persone che la pensano allo stesso modo e possono quindi avere conversazioni tematiche. Si tratta di proprietà che possono essere replicate sui relay Nostr senza compromettere nessuna delle sue altre funzionalità.

4.3 Confronto con SSB

Secure Scuttlebutt (SSB) è un protocollo di comunicazione peer-to-peer, una rete mesh e un ecosistema di social media self-hosted creato nel 2014. In SSB ogni utente ospita sia il propri contenuti che i contenuti dei peer che segue, il che fornisce tolleranza ai guasti e coerenza finale. I messaggi sono firmati digitalmente e aggiunti a un elenco di soli messaggi pubblicati da un autore.

Ai tempi, SSB rappresentò una grande innovazione perchè, a differenza delle principali piattaforme di social media aziendali, i dati e i contenuti degli utenti non sono monetizzati, non vengono prese decisioni di progettazione del software al fine di massimizzare il coinvolgimento degli utenti o aumentare le metriche di marketing e non ci sono pubblicità.

SSB è il primo protocollo di social networking relativamente riuscito che utilizza chiavi pubbliche che ha avuto una certo successo e che ha aperto la strada a Nostr.

Le principali limitazioni di SSB, che Nostr cerca di superare, sono le seguenti.

- Poiché è ottimizzato per i social network "locali", cioè persone che si incontrano effettivamente, SSB è caratterizzato da alcune scelte progettuali intorno alla strutturazione del feed di ogni persona (ogni nota deve fare riferimento a quella precedente in una singola catena di eventi) per renderlo facile da sincronizzare. Queste scelte sono in realtà molto limitanti nella pratica e hanno contribuito a non ottenere il successo che probabilmente SSB meritava.

- Per lo stesso motivo di cui sopra, SSB ha il problema di non consentire alle persone di mantenere la stessa identità in più dispositivi e app, il che ne limita drasticamente lo scopo e la portata.

- Inoltre, dal momento che condividere i feed su Internet è un di più per SSB, è davvero difficile iniziare e sfogliare i feed degli altri, e quindi ottenere attenzione al di fuori di gruppi di interesse ben consolidati.

- Il protocollo è inutilmente complesso.

5 Nostr e la privacy

Sebbene Nostr non sia un protocollo di privacy di per sé - tra le altre problematiche, i client per impostazione predefinita rivelano agli altri nodi IP degli utenti - il protocollo Nostr potrebbe apportare miglioramenti alla privacy di Bitcoin.

5.1 Miglioramento della privacy e della scalabilità di BIP47

BIP47 è una proposta di miglioramento di Bitcoin per creare codici di pagamento riutilizzabili garantendo la privacy degli utenti per pagamenti ricorrenti. Senza BIP47, gli utenti devono generare manualmente nuovi indirizzi per evitare il riutilizzo di indirizzi. Quando un utente riutilizza un indirizzo per le transazioni, consente a chiunque stia osservando la blockchain di raggruppare facilmente tutte le transazioni appartenenti all'indirizzo riutilizzato e creare un grafico dello storico dei pagamenti e del valore netto dell'utente. La prevenzione del riutilizzo degli indirizzi è quindi una pratica consigliata per la privacy in Bitcoin ed è già implementata di default in molti portafogli Bitcoin. Tuttavia, quando un utente desidera stabilire pagamenti ricorrenti con un'altra parte, come in una relazione tra un commerciante e un cliente, la frequente generazione di nuovi indirizzi può risultare scomoda.

Con BIP47, un cliente può generare un insieme di indirizzi da utilizzare per i pagamenti verso un commerciante. Se un cliente effettua acquisti mensili, il commerciante dovrebbe inviare al cliente un indirizzo ogni mese. Con BIP47, il cliente crea un codice di pagamento dedicato per il commerciante, che funziona in modo simile a una chiave pubblica estesa. Ciò consente al cliente di generare automaticamente nuovi indirizzi per il commerciante, anziché il commerciante dover creare indirizzi per il cliente.

BIP47 fa uso di indirizzi di notifica, che vengono monitorati da portafogli HD per le transazioni in output. In una transazione di notifica, il commerciante invia al cliente una chiave pubblica oscurata e un codice di catena tramite il campo `OP_RETURN`, insieme a un segreto condiviso per mantenere riservati gli indirizzi condivisi sulla blockchain pubblica. Questo scambio crea diversi problemi a causa dell'architettura della rete Bitcoin. I primi due sono di natura economica: una transazione di notifica consiste di 80 byte, il che può diventare costoso per gli utenti quando le commissioni sulla rete Bitcoin sono elevate. Inoltre, le transazioni di notifica creano output non spendibili, che gonfiano l'insieme degli UTXO (Unspent Transaction Output) nel tempo. Ciò aumenta il carico computazionale sui nodi Bitcoin che devono memorizzare l'intero insieme degli UTXO, ovvero ogni output Bitcoin che non è stato utilizzato come nuovo input per garantire la validità delle transazioni.

Una transazione di notifica crea il cosiddetto "toxic change" (cambio tossico). Quando un utente riceve un resto da una transazione di notifica e spende il resto verso un terzo, chiunque stia osservando la blockchain è in grado di correlare i pagamenti ricorrenti dell'utente ai suoi pagamenti non ricorrenti, anche quando gli indirizzi non vengono riutilizzati. Un indirizzo di notifica esiste anche solo una volta per ogni portafoglio. Se un commerciante volesse stabilire pagamenti ricorrenti con 10 clienti, chiunque stia osservando la blockchain sarebbe in grado di ottenere informazioni sulla base di clienti del commerciante, poiché tutti e 10 i clienti dovrebbero creare transazioni di notifica per il

commerciante verso lo stesso indirizzo di notifica.

Invece di utilizzare transazioni di notifica per scambiare codici di pagamento tra commercianti e clienti, i codici di pagamento potrebbero essere scambiati tramite Nostr. A differenza di altri metodi di comunicazione, Nostr è adatto allo scambio di codici di pagamento BIP47 poiché non esiste un'autorità centrale che potenzialmente possa censurare lo scambio di messaggi. Allo stesso tempo, tutti i messaggi diretti su Nostr sono crittografati per impostazione predefinita, eliminando la necessità di calcolare segreti condivisi. Utilizzando BIP47 tramite Nostr, gli utenti possono evitare la creazione di un ingrossamento dell'insieme degli UTXO attraverso output non spendibili ed eliminare la correlazione tra pagamenti ricorrenti e non ricorrenti, così come la divulgazione delle basi di clienti attraverso l'evitamento del "toxic change" e il riutilizzo di indirizzi di notifica.

5.2 Nostr Pay-To-Endpoint

In Bitcoin, i servizi di analisi della blockchain utilizzano l'euristica della "common input ownership" (proprietà di input comuni) per mappare le transazioni alle identità. In questa euristica, una transazione contenente diversi indirizzi pubblici usati come input viene classificata come appartenente a una sola persona. A causa della sua architettura basata sugli UTXO, attraverso la quale input e output delle transazioni sono collegati, il protocollo Bitcoin è anche soggetto all'analisi del subset sum. Nell'analisi del subset sum, gli avversari sono in grado di calcolare la probabilità che input e output appartengano alla stessa entità, anche quando vengono utilizzati diversi indirizzi pubblici come input per una transazione.

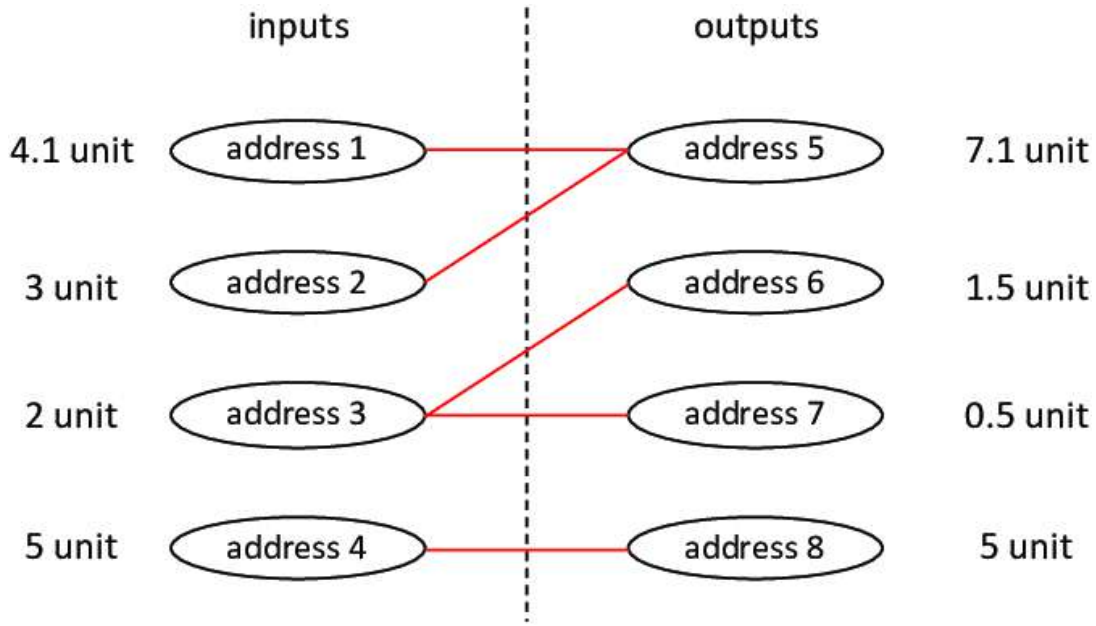


Figure 10: Esempio di come dagli output si può risalire agli input.

Pay-to-EndPoint (P2EP) è una reinvenzione orientata alla privacy del Pay-to-IP (P2IP) di Satoshi Nakamoto, implementata nel client Bitcoin originale. Una forma di transazione P2EP sono i PayJoin, che sono transazioni progettate per rompere l'euristica della proprietà di input comuni. In una transazione PayJoin, sia il mittente che il des-

tinatario contribuiscono con input alla transazione per rompere l'euristica dell'input comune. Con i PayJoin, gli utenti scambiano informazioni su quali UTXO verranno utilizzati come input tramite qualsiasi canale di comunicazione, come ad esempio Tor Onion, che funge da punto finale, per costruire una transazione Bitcoin parzialmente firmata (PSBT). Una volta che entrambe le parti hanno accettato le condizioni e firmato la transazione, una transazione PayJoin appare come qualsiasi altra transazione Bitcoin sulla blockchain. Poiché le parti coinvolte agiscono sia come mittenti che come destinatari, una transazione PayJoin rompe l'euristica della proprietà comune e l'analisi del subset sum.

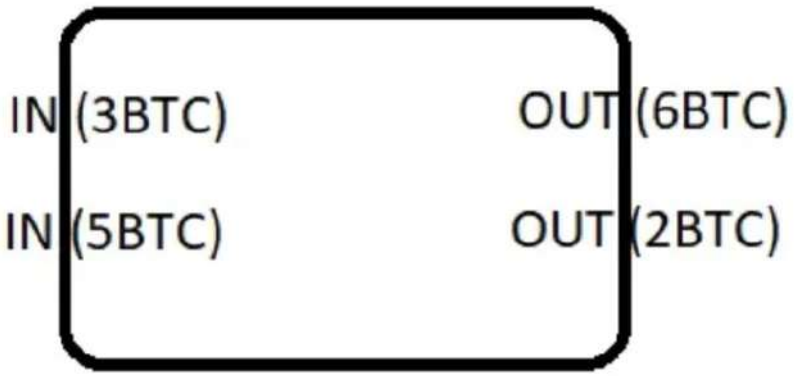


Figure 11: Le parti possono contribuire con input di 3 e 5, mentre la transazione genera output di 6 e 2.

Tuttavia c'è un problema, le transazioni PayJoin sono complesse da coordinare, poiché i partecipanti devono essere online contemporaneamente quando si utilizza un dominio clearnet o punti finali Tor Onion. Se un utente avvia una transazione P2EP e, ad esempio, chiude il computer o interrompe in altro modo la connettività di rete, la transazione non può essere comunicata. In Nostr, la comunicazione è asincrona: gli utenti recuperano le informazioni dai relays una volta ripristinata la connettività di rete. Utilizzando le chiavi Nostr invece delle Tor Onion come punti finali per le transazioni P2EP, le transazioni P2EP potrebbero essere coordinate in modo più semplice.

Un'altra implementazione di P2EP è l'LNURL, molto dibattuto. Con LNURL, invece di dover generare tediosamente nuove fatture per ogni transazione, gli utenti possono ricevere un endpoint statico che punta a un server web per generare automaticamente nuove fatture. Tuttavia, poiché i server web dipendono dal servizio di denominazione dei domini (DNS) globale, gli utenti di LNURL inevitabilmente rivelano la propria identità al provider di hosting, così come il proprio indirizzo IP ai destinatari se non vengono prese adeguate precauzioni. Un'ampia adozione di LNURL sarebbe quindi un danno a discapito della pseudonimia della Lightning Network. Invece di utilizzare un server web come endpoint per LNURL, gli utenti potrebbero utilizzare le chiavi Nostr come endpoint per le transazioni LNURL per nascondere le loro identità.

5.3 Nostr per Conjoins

Sebbene un PayJoin sia ottimo per rompere l'euristica della proprietà comune e l'analisi del subset sum, i PayJoin non sono in grado di offrire privacy sia al mittente che al destinatario nei confronti della controparte che collabora. I PayJoin sono essenzialmente CoinJoin tra due parti, limitati a due partecipanti: ciò significa che sia il mittente che il destinatario sono consapevoli dei propri input e output, lasciando identificabili gli input e gli output del loro partner. A meno che un PayJoin non venga facilitato con transazioni CoinJoin, gli utenti rischiano di rivelare i saldi del loro portafoglio, nonché transazioni passate e future ai loro partner PayJoin.

Nei sistemi di credenziali di importo anonimo, come il protocollo di Wasabi Wallet per il coordinamento di CoinJoin, WabiSabi, le chiavi Nostr possono fungere da punti finali di comunicazione per il coordinamento di una transazione CoinJoin. Ciò consente al mittente e al destinatario di una transazione CoinJoin di scambiare le credenziali necessarie per partecipare alle fasi CoinJoin, consentendo essenzialmente una forma di pagamenti discreti all'interno di un CoinJoin. Utilizzando le chiavi Nostr come endpoint nelle transazioni CoinJoin, le parti che collaborano rimangono ignare dei saldi e delle transazioni dei loro controparti nascondendosi nella folla. Allo stesso tempo, l'utilizzo delle chiavi Nostr come endpoint per le transazioni CoinJoin aiuta gli utenti PayJoin a risparmiare sulle commissioni facilitando i pagamenti direttamente all'interno del CoinJoin, anziché CoinJoining per facilitare il pagamento successivamente.

Un altro utilizzo di Nostr nei CoinJoin risiede nella scoperta dei coordinatori. Mentre la maggior parte dei coordinatori CoinJoin funziona dietro Tor per oscurare l'identità dei partecipanti ai CoinJoin, attualmente gli utenti non sono in grado di scoprire facilmente nuovi coordinatori ai quali unirsi, ad eccezione di JoinMarket, un mercato CoinJoin rivolto a utenti CoinJoin più esperti. Mentre gli utenti CoinJoin possono aggiungere coordinatori personalizzati a Wasabi Wallet, un'operazione banale che consiste nello scambio di un URL nel back-end, non esiste un modo per automatizzare il processo di aggiornamento dei coordinatori a causa della mancanza di una piattaforma per la pubblicazione. Invece, per scoprire nuovi coordinatori, gli utenti devono cercare sui social media e nei forum, come Reddit o Twitter, per aggiungere manualmente i coordinatori. Tuttavia, la pubblicazione di un servizio di coordinamento tramite social media o forum può rappresentare un rischio per i fornitori di coordinamento a seconda delle politiche applicate al servizio, poiché determinate pagine possono essere facilmente chiuse.

Se Tor è un remailer anonimo, ovvero un protocollo che facilita l'inoltro anonimo e la ricezione di messaggi tra i partecipanti, Nostr può funzionare come un bacheca anonima. I coordinatori CoinJoin possono pubblicare i loro servizi tramite un tipo di evento Nostr, e i portafogli CoinJoin possono essere configurati per recuperare automaticamente da quei relays per visualizzarli all'interno dei loro client. La diffusione di server coordinatori tramite Nostr, come facilitato tramite il plugin CoinJoin di BTCPay Server e proposto nel software CoinJoin abilitato per Lightning Vortex, può eliminare la necessità di cercare e aggiungere manualmente i coordinatori CoinJoin nei client CoinJoin, contribuendo a decentralizzare ulteriormente il panorama di coordinamento CoinJoin.

5.4 Superamento dei requisiti IP con Nostr

Come accennato in precedenza, il protocollo Nostr è stato originariamente ideato per realizzare un mercato completamente decentralizzato chiamato Diagon Alley. Con l'evoluzione del protocollo Nostr, Diagon Alley è diventato l'estensione LNbits NostrMarkets: un mercato nativo di Nostr che consente ai commercianti e ai clienti di gestire e interagire con negozi online tramite relay. In NostrMarkets, i clienti possono sottoscrivere la chiave pubblica di un commerciante per ottenere i prodotti dai relay anziché accedere al sito di un commerciante tramite un negozio online. Ciò aumenta la resistenza alla censura dei negozi online, poiché i commercianti non dipendono da siti web sequestrabili, ma il negozio di un commerciante è ospitato con tutti i relay che il negozio configura per comunicare. Anche se il server del commerciante venisse sequestrato, il suo negozio potrebbe essere facilmente configurato in una posizione diversa, poiché tutti i prodotti sono archiviati con i relay sulla rete Nostr. NostrMarkets gestisce il coordinamento degli ordini e dei pagamenti tramite messaggi diretti Nostr criptati, mentre i pagamenti vengono facilitati attraverso la Lightning Network.

Oltre alla sua resistenza alla censura, l'estensione LNbits NostrMarkets consente mercati completamente anonimi. Invece di esporre l'indirizzo IP di un commerciante all'intero mondo, sia i commercianti che i clienti rivelano solo il loro IP ai relay a cui si connettono, il che può essere facilmente mitigato eseguendo un client o un negozio tramite Tor. Come vantaggio di eseguire completamente un negozio tramite Tor, che rende il negozio accessibile solo tramite il browser Tor e le pagine web `.onion`, NostrMarkets può funzionare su qualsiasi browser web o smartphone, migliorando l'esperienza utente delle comunicazioni client-server orientate alla privacy. Poiché i pagamenti vengono negoziati tramite messaggi diretti Nostr criptati e facilitati tramite la Lightning Network, i pagamenti in NostrMarkets rimangono relativamente privati finché il nodo Lightning del negozio viene eseguito tramite Tor, poiché un messaggio diretto di coordinamento dei pagamenti è indistinguibile dagli altri messaggi diretti in Nostr.

Un altro modo per aggirare il requisito degli indirizzi IP nella comunicazione server-client è tramite NOSTREST. REST, acronimo di "representational state transfer", fa parte dell'architettura software del World Wide Web ed è utilizzato per facilitare la comunicazione tra server e client tramite richieste GET, POST, PUT, DELETE e PATCH. Tuttavia, quando un client invia una richiesta REST a un server, gli indirizzi IP vengono rivelati, potenzialmente esponendo informazioni personalmente identificabili. Su GitHub, `escapee` ha proposto un ponte REST API basato su Nostr, chiamato NOSTREST. Utilizzando le chiavi Nostr senza intestazioni di identificazione, sia gli utenti che gli operatori dei server non hanno bisogno di conoscere gli indirizzi IP dei loro interlocutori. Un'implementazione di NOSTREST può quindi migliorare la privacy delle applicazioni Bitcoin che utilizzano REST, poiché i server non hanno bisogno degli indirizzi IP dei client.

Un esempio potrebbe essere l'esecuzione di mints di e-cash custodiali di Chaum, una forma di sistemi di credenziali con importo anonimo. In un mint di e-cash, l'operatore del mint non conosce i saldi o il valore scambiato dai suoi utenti. Tuttavia, a causa dell'attuale architettura di REST, apprende l'indirizzo IP dell'utente a meno che non venga eseguito di default dietro Tor, come nel sistema di e-cash Cashu. Ma l'implementazione e la

gestione del supporto a Tor sono tediose. Con il ponte NOSTREST, i progetti possono facilmente preservare la privacy dei loro utenti. Eseguendo un mint di e-cash dietro Tor utilizzando NOSTREST per la comunicazione tra server e client, la comunicazione può essere facilitata in modo asincrono, mentre sia l'operatore del server che l'utente apprendono solo le rispettive chiavi pubbliche, eliminando il rischio di identificazione tramite IP.

6 Limitazioni e potenziali sviluppi

6.1 Problemi di gestione delle chiavi

Le coppie di chiavi pubbliche e private degli utenti sono fondamentali per il funzionamento di Nostr come protocollo. Non ci sono nomi utente o qualsiasi tipo di identificatori controllati da un server di rete da associare agli utenti individuali. Sono semplicemente le chiavi di questi utenti che sono completamente sotto il loro controllo.

Questo crea un legame stretto tra l'utente effettivo e il modo in cui viene identificato dagli altri, impedendo a qualsiasi server di rete di separare queste due cose, ad esempio, fornire l'identificatore di qualcuno ad un altro utente. Ciò risolve uno dei problemi fondamentali più grandi delle piattaforme utilizzate per la comunicazione tra le persone: la mancanza di controllo sulle proprie identità degli utenti. Tuttavia, introduce anche tutti i problemi legati alla gestione delle chiavi che si presentano quando si possiede una chiave privata. Le chiavi possono essere smarrite o compromesse e, in caso di tali eventi, gli utenti non hanno nessuno a cui rivolgersi per assistenza, proprio come avviene con Bitcoin. Non c'è un servizio di assistenza clienti per recuperare la chiave, se la perdi, è per sempre.

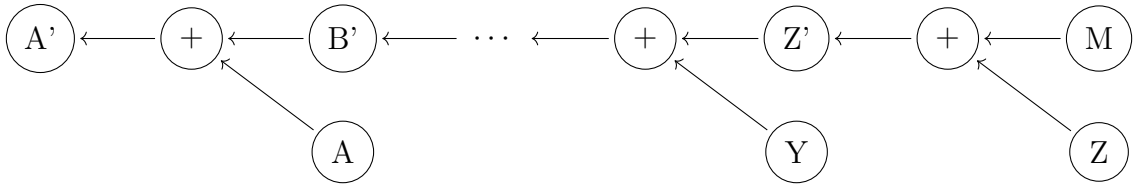
Ciò inevitabilmente richiederà uno schema per consentire agli utenti di passare da una coppia di chiavi all'altra in modo verificabile e scopribile per gli altri utenti con cui interagiscono tramite il protocollo. L'intero protocollo si basa sulla prova che un evento provenga da un utente specifico (chiave di identità), quindi tutte queste garanzie svaniscono una volta che le chiavi di qualcuno vengono compromesse.

Per affrontare questo problema si potrebbe controllare il rispettivo account Twitter, ma allora non sarebbe un sistema molto decentralizzato se si richiede l'utilizzo di una piattaforma centralizzata in cui l'utente non ha il controllo della propria identità per verificare la propria identità Nostr. Si potrebbe inoltre fare sì che altri utenti attestino la legittimità di una nuova chiave, ma questo non affronta situazioni come compromissioni di massa delle chiavi o la mancanza di conoscenza sufficiente di persone vicine da poter fidarsi delle loro attestazioni.

Nostr ha bisogno di un vero schema crittografico che leghi la rotazione di una chiave a un'altra. C'è una proposta dell'autore `fiatjaf` per uno schema di base che potrebbe potenzialmente risolvere questo problema. L'idea sarebbe quella di prendere un lungo insieme di indirizzi derivati da un'unica chiave master e creare un insieme di chiavi "modificate", cioè concatenare gli impegni all'indietro, dalla fine all'inizio, in modo che ogni chiave modificata contenga effettivamente una prova che la chiave modificata successiva è stata utilizzata per crearla.

Immaginiamo di partire con la chiave Z, l'ultima nella catena. La modificheremmo con qualcosa e quindi andremmo all'indietro e creeremmo una versione modificata della chiave Y utilizzando la chiave Z modificata (Z' + Y = Y'). Da qui prendiamo Y' e la utilizziamo per modificare la chiave X (Y' + X = X'). Facciamo questo fino a raggiungere la chiave A per ottenere A', e da lì iniziamo ad utilizzare quella chiave. Quando viene compromessa, l'utente può diffondere un evento contenente la chiave non modificata A e la chiave modificata B'. Questo conterrà tutti i dati necessari per dimostrare che B' è

stato utilizzato per generare A', e gli utenti possono immediatamente smettere di seguire A' e invece seguire B'. Sarebbero certi che B' sia la prossima chiave dell'utente da seguire.



Questa proposta presenta ancora alcuni problemi. Innanzitutto, bisogna generare in anticipo tutte le chiavi che saranno usate in futuro e non offre un modo per passare ad un intero nuovo set di chiavi. Questo potrebbe essere risolto impegnandosi in questa procedura iniziale ad una chiave principale che potrebbe notarizzare tali rotazioni, o semplicemente generando fin dall'inizio un set molto ampio di chiavi. Entrambe le soluzioni sarebbero valide, ma richiederebbero infine di mantenere al sicuro una chiave principale o una key material e di esporre solo le singole chiavi attive agli utenti di Nostr.

Tuttavia, questo schema non protegge gli utenti né offre un meccanismo per il recupero dell'identità nel caso in cui la key material principale venga perso o compromesso. Ciò non vuol dire che non ci sia un vantaggio nello schema proposto da `fiatjaf`, ma è importante sottolineare che nessuna soluzione risolve tutti i problemi.

Per approfondire un po' le potenziali soluzioni, si immagini invece di avere una chiave modificata non solo con la catena di chiavi proposta, ma anche con una chiave maestra offline che deve essere utilizzata per firmare l'evento di rotazione da una chiave all'altra. Si ha la chiave A', che è derivata dall'aggiunta di A e M (la chiave maestra), e l'evento di rotazione sarebbe formato da A, M e B' (generato dall'aggiunta di B e M) con una firma da parte di M. M potrebbe essere una chiave multisig a soglia. Ciò potrebbe potenzialmente aggiungere ridondanza contro la perdita e fornire un meccanismo sicuro per la rotazione delle chiavi. Ciò apre anche la possibilità di utilizzare servizi per aiutare nel recupero o di distribuire alcune di queste chiavi tra amici fidati. Offre tutta la flessibilità che la multisig offre con Bitcoin stesso.

Inoltre, NIP26 è una proposta che potrebbe essere molto utile per gestire questo problema. Specifica un'estensione del protocollo per gli eventi che consente a una chiave di autorizzare un'altra chiave a pubblicare eventi per conto suo. Il "token" o prova di delega della firma sarebbe quindi incluso in tutti gli eventi pubblicati dalla seconda chiave a nome della prima. Potrebbe persino avere una scadenza temporale in modo che i token di delega scadano automaticamente e debbano essere rinnovati.

In definitiva, indipendentemente dal come, questo problema deve essere risolto a lungo termine per Nostr. Un protocollo basato interamente su coppie di chiavi pubbliche/private utilizzate come identità non può guadagnare slancio e adozione se l'integrità di tali identità non può essere protetta e mantenuta per gli utenti. Alla fine, ciò si ridurrebbe a dover costantemente utilizzare piattaforme esterne e centralizzate per verificare nuove chiavi e coordinare le persone che seguono la nuova identità quando qualcosa viene perso o compromesso, e a quel punto, tali piattaforme esterne diventano un mezzo per seminare confusione e praticare la censura.

Le problematiche legate alla gestione delle chiavi e alla sicurezza rappresentano grandi problemi con un ampio spazio di progettazione pieno di compromessi e punti critici, ma sono problemi che dovranno essere risolti all'interno del contesto di Nostr perché funzioni.

6.2 Da cosa dipende la crescita di Nostr

L'intero protocollo Nostr dipende dal fatto che persone in qualche luogo eseguano un server di relay. Non esiste una "rete Nostr", ci sono solo relay e client che si connettono ai relay. È necessario fornire incentivi affinché le persone eseguano i relay e, a lungo termine, ciò sarà un elemento fondamentale per determinare fino a che punto i relay possono scalare. Non ci saranno mai relay Nostr con la stessa portata dei server di Twitter a meno che non possano essere gestiti in modo redditizio o, almeno, generare abbastanza denaro per coprire i costi del loro funzionamento.

6.2.1 La pubblicità

La pubblicità sarebbe molto facile da bloccare completamente, rendendola una soluzione non fattibile, date le modalità di funzionamento di Nostr come protocollo. Un server di relay potrebbe provare a utilizzare la pubblicità come modello di guadagno, che ovviamente è il modello di guadagno dominante per praticamente ogni servizio gratuito presente online, ma il problema è che gli utenti dovrebbero essenzialmente optare per essa. I relay potrebbero facilmente inserire annunci negli eventi che inviano ai client, ma i client potrebbero anche semplicemente filtrarli dall'interfaccia utente se gli eventi pubblicitari non sono stati creati da una chiave pubblica a cui hanno intenzionalmente sottoscritto. Anche se un operatore di relay producesse un client che non lo facesse, non c'è modo di impedire agli utenti di utilizzare altri client che invece lo facessero, recuperando i dati dal loro relay. Gli utenti non saprebbero nemmeno se il client di qualcuno stia nascondendo gli annunci o meno, e a causa di questa mancanza di informazioni, questo modello è praticamente destinato al fallimento a meno che gli utenti non optino intenzionalmente per esso. E anche in quel caso, l'operatore di relay non avrebbe una base solida per mostrare qualsiasi informazione sull'interazione agli inserzionisti.

6.2.2 Micropagamenti

I micropagamenti sono un'altra soluzione evidente, specialmente alla luce dei tentativi attuali di integrare più strettamente Lightning nelle applicazioni Nostr. Questo modello offrirebbe molta flessibilità in termini di come addebitare i costi. I relay potrebbero addebitare solo per la pubblicazione degli eventi, potrebbero addebitare per il download degli eventi da leggere, potrebbero fare una combinazione di entrambi e regolare il prezzo di ognuno in base a quanto delle loro risorse viene consumato da ciascuno. I micropagamenti per il contenuto stanno dimostrando di essere fattibili in molti settori di nicchia basati su Lightning, ma ci sono due problemi fondamentali che impediscono una vera scalabilità a livello globale. Prima di tutto, al momento non c'è abbastanza adozione di Bitcoin per supportare tale modello. Anche se tutti si accontentassero di pagare per ogni piccola interazione di servizio su Nostr, non ci sono abbastanza persone che detengono Bitcoin per supportarlo su una scala così massiccia come Twitter. I relay potrebbero addebitare abbonamenti in valuta fiat, ma tali sistemi di pagamento non supporterebbero pagamenti di frazioni di centesimo per ogni evento pubblicato o scaricato. In secondo luogo, le persone sono cresciute abituate a servizi di questo tipo gratuiti.

Potrebbe esserci un modo per rendere i micropagamenti "più solidi" o più sostenibili senza imporli letteralmente a ogni categoria di utenti che utilizzano il relay. Si è discusso molto sulla possibilità di costruire diversi tipi di applicazioni su Nostr oltre a un clone di Twitter: GitHub, Wikipedia e persino app decentralizzate per lavoratori autonomi come Uber. Quest'ultimo è la chiave qui. Qualcosa come Twitter o Google è solo un servizio che le persone hanno dato per scontato come gratuito per tutta la loro vita. Le transazioni economiche non sono un campo in cui queste aspettative sono profondamente radicate nelle persone. Le persone sono abituate a pagare una tariffa per pubblicare un annuncio di lavoro da qualche parte o a pagare una commissione a un operatore di un marketplace quando ordinano qualcosa online. Semplicemente lo assumono e se lo aspettano fin dall'inizio. Ciò potrebbe offrire ai relay un modo per creare un reddito affidabile dai propri utenti senza creare un elevato attrito o violare le aspettative dell'utente medio potenziale.

Se i micropagamenti saranno un fattore importante, l'operatore di relay dovrà gestire un nodo Lightning per ricevere fondi dagli utenti in primo luogo. Ciò potrebbe potenzialmente amplificare i ricavi se sincronizzato correttamente con il modello di micropagamento implementato da un relay. Più un server di relay genera ricavi, maggiore sarà la liquidità necessaria sulla Lightning Network per agevolare tali transazioni. Se gli operatori pianificano adeguatamente come distribuire o allocare tale liquidità sulla rete, il semplice atto di gestire un nodo di routing potrebbe potenzialmente diventare una fonte di reddito non trascurabile, oltre a quanto vengono addebitati per accettare o fornire dati attraverso il loro relay.

7 Conclusione

In conclusione, Nostr Protocol rappresenta un notevole passo avanti verso una maggiore resistenza alla censura, garantendo una maggiore privacy e protezione dei dati personali rispetto ai tradizionali social network. I vantaggi offerti da questa tecnologia sono molteplici, tra cui la possibilità di gestire i propri dati senza essere esposti a terze parti e un'ampia gamma di potenzialità applicative.

Tuttavia, è importante considerare anche gli svantaggi. L'esperienza su Nostr di un utente potrebbe risultare leggermente compromessa a causa della sua natura decentralizzata e, soprattutto, della sua breve storia. Inoltre, la mancanza di incentivi a possedere un relay potrebbe limitare la diffusione e l'adozione di questa piattaforma.

Infine, sebbene sia improbabile che Nostr Protocol sostituirà completamente i social network tradizionali, rappresenta comunque una valida alternativa per coloro che sono vittime di censura e controllo della libertà di espressione. La possibilità di godere di una maggiore resistenza alla censura e di mantenere la propria privacy potrebbe attirare coloro che cercano un ambiente digitale più sicuro e privato per comunicare e condividere informazioni.

Bibliografia

[1] Nicoletta Boldrini. *Web 3.0, cos'è la prossima generazione del web, perché ci condurrà nel metaverso*. URL: https://thecryptogateway.it/web-3-0/. (accessed: 22.05.2023).

[2] BTCCasey. *THNDR Games releases new game to earn Bitcoin alongside gaming reputation system on Nostr*. URL: https://bitcoinmagazine.com/business/thndr-games-releases-new-game-to-earn-bitcoin. (accessed: 22.05.2023).

[3] Davide Grammatica. *Web 3.0: tutto sull'evoluzione del Web 2.0*. URL: https://tech4future.info/web-30-dal-web-1-al-web3-la-storia-del-web/. (accessed: 22.05.2023).

[4] L0la L33tz. *The Nostr privacy paradox*. URL: https://bitcoinmagazine.com/technical/how-nostr-can-improve-bitcoin-privacy. (accessed: 22.05.2023).

[5] Nostr. *Nostr WebSite*. URL: https://nostr.com/. (accessed: 22.05.2023).

[6] Shinobi. *Nostr will only scale if it can incentivize users to run relays*. URL: https://bitcoinmagazine.com/culture/can-nostr-grow-to-twitter-size. (accessed: 22.05.2023).

[7] Shinobi. *To become Bitcoin's go-to platform, Nostr will have to solve its key management issues*. URL: https://bitcoinmagazine.com/technical/solving-nostr-key-management-issues. (accessed: 22.05.2023).

SOMNIUM SPACE

Giorgia Appolloni, Valerio Gallo, Simran Singh, Gianluca Turco

POLITECNICO DI TORINO

Tesina Blockchain e Criptoeconomia

Somnium Space

Prof. Danilo Bazzanella

Giorgia Appolloni s303841

Valerio Gallo s302671

Simran Singh s303369

Gianluca Turco s303386

Anno Accademico 2022-2023

Indice

1 Introduzione **3**
1.1 Cos'è il metaverso 3
1.2 Cos'è Somnium Space 4
1.3 Tecnologie utilizzate 5

2 Aspetti economici **6**
2.1 Assets e NFT 6
2.2 Blockchain 11
2.2.1 Una soluzione ibrida con Polygon e Ethereum 11
2.2.2 Una criptomoneta proprietaria: CUBEs 11

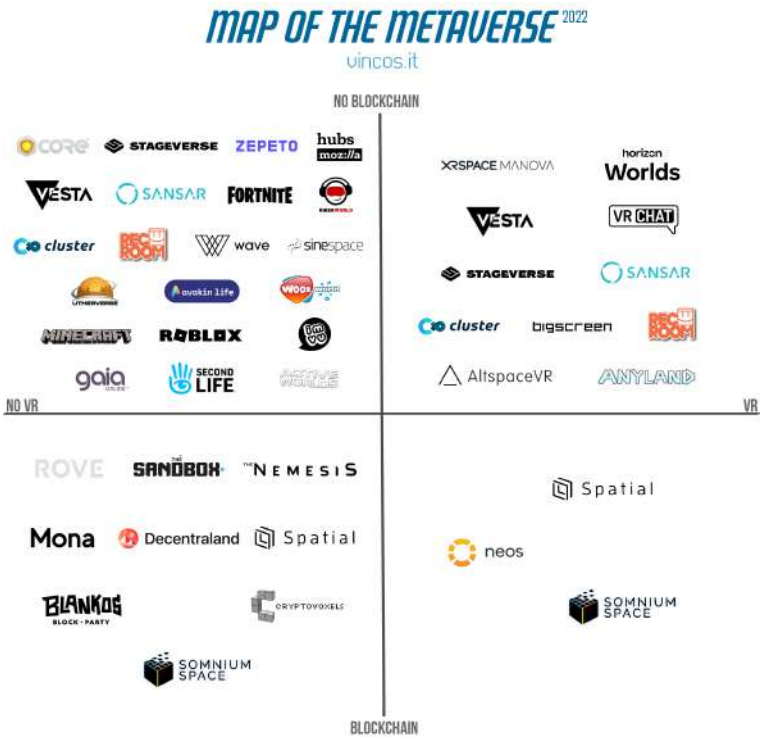
3 Sviluppi futuri **13**
3.1 Road Map 13
3.2 Karma 14
3.3 Modalità Live Forever 15

4 Conclusione **17**

Capitolo 1

Introduzione

1.1 Cos'è il metaverso



Metaverso è un termine nato nel mondo cyberpunk nel 1992 e salito di recente alla ribalta, anche in seguito all'annuncio da parte di Facebook di cambiare il proprio nome in "Meta".

Il metaverso può essere definito come uno spazio tridimensionale all'interno del quale le persone fisiche possono muoversi, condividere beni ed esperienze e interagire tra loro.

In altri termini, il metaverso può essere considerato come una sorta di ambiente di vita virtuale che si sovrappone al mondo fisico della vita reale, permettendo agli utenti di interagire in modo più diretto e immediato rispetto ai comuni social networks, partecipando anche a varie attività in maniera molto coinvolgente.

Un mondo virtuale che, quindi, ricalca quello di tutti i giorni, cancellandone però i limiti spaziali. Un'esperienza di questo tipo è resa possibile da dispositivi e infrastrutture quali la realtà aumentata (AR), la realtà virtuale (VR), connessioni superveloci e blockchain, le cui caratteristiche permettono l'implementazione di un sistema economico, oltre a un'elevata quantità di dati e informazioni. Gli utenti sono rappresentati da avatar tridimensionali con un proprio stile capaci di interagire fra loro.

Bisogna però specificare che al momento il metaverso non esiste. Si tratta di un progetto in corso di sviluppo che diverse società, Meta e Somnium in primis, puntano a realizzare nei prossimi anni.

1.2 Cos'è Somnium Space

Somnium Space è un mondo virtuale aperto, social e costruito su blockchain, dove tutti sono in grado di acquistare e scambiare assets, monetizzare facilmente le proprie esperienze digitali ed immergersi in una realtà completamente alternativa.

Somnium space è una società ceca nata nel 2017 da un'idea dell'attuale CEO Artur Sychov, che ha lavorato per diversi anni come trader di investimenti prima di diventare un imprenditore di start up innovative.

Si tratta di un mondo con una mappa finita, composta di 5026 appezzamenti di terreno, detti "parcel", di varie dimensioni e connessi da strade. Un appezzamento di terreno può essere acquistato o venduto da un utente in sicurezza, grazie alla piattaforma Blockchain.

Il possessore acquisisce anche la facoltà di costruirci ciò che vuole. Così, nonostante l'intervento iniziale di un team di programmatori informatici e designer grafici, Somnium Space è un mondo che sarà modellato e costruito interamente dagli utenti.
Dal 2018 Somnium fa parte della VRBA (*Virtual Reality Blockchain Association*), un'associazione di aziende che si occupano di realtà virtuale che mirano a creare un'identità digitale per l'utente che sia portabile tra diversi mondi virtuali, oltre che a regolamentare i costi degli acquisti in gioco. La presenza di un'identità digitale universale, di un avatar che non sia limitato al mondo virtuale in cui è stato creato, è ovviamente una tappa fondamentale della strada verso la creazione del metaverso.

1.3 Tecnologie utilizzate

Somnium Space ha scelto di essere multipiattaforma.

Ne esistono due versioni: una per desktop, scaricabile gratuitamente, e una versione web, accessibile quindi anche da altri dispositivi, limitata in alcune funzionalità.

Per ottenere la migliore esperienza di gioco è consigliato l'utilizzo di un visore a realtà virtuale, anche se non è strettamente necessario.

È garantita la compatibilità con tutti i principali visori in commercio, ma l'azienda ambisce nei prossimi anni a sviluppare un proprio visore, che avrà la caratteristica di essere modulare e open source, in modo da rendere ancora più personalizzabile l'esperienza dell'utente.

Inoltre sono già supportati sistemi di tracking del corpo, delle dita, delle labbra e degli occhi, e in futuro progettano di aggiungere la compatibilità a maschere multisensoriali, che permetterebbero per esempio di percepire gli odori e di aumentare ulteriormente l'immersività.
La personalizzazione delle costruzioni e degli avatar è resa possibile da Somnium Space UnitySDK, un software creato dall'azienda stessa basato sul motore di gioco Unity.
Lo sviluppo di un unico grande server permette agli utenti di accedere tutti allo stesso mondo persistente, senza essere divisi in sotto-servers e istanze duplicate.

Capitolo 2

Aspetti economici

Somnium Space si basa sulla tecnologia di Ethereum, il che significa che utilizza la rete Ethereum come infrastruttura sottostante per consentire interazioni e transazioni sicure e trasparenti all'interno del mondo virtuale.

Ethereum è una piattaforma blockchain che supporta la creazione e l'esecuzione di smart contracts, che sono programmi autonomi che eseguono automaticamente azioni specificate quando si verificano determinate condizioni. Somnium Space sfrutta gli smart contracts di Ethereum per gestire aspetti come la proprietà e il trasferimento dei beni virtuali.
Recentemente sono state rese supportate anche transazioni sulla blockchain di Solana, rendendo Somnium una realtà multichain. Allo stesso tempo anche gli NFT di Solana sono ora supportati.

2.1 Assets e NFT

La blockchain di Ethereum consente di "tokenizzare", ovvero trasformare in NFT (di tipo ERC721) parcels di terra virtuale, assets digitali ed esperienze attraverso mercati decentralizzati. Il mercato utilizzato da Somnium è quello della loro azienda partner OpenSea. Tra gli assets che si possono rendere NFT e dunque monetizzare ci sono:

• **Parcels:** al momento la vendita di terreni è la principale forza trainante dell'economia di Somnium, ed il gioco offre i seguenti tipi di proprietà terriera: Small, con limite di altezza e profondità pari a 10 metri; Medium, con limite di altezza e profondità di 25 metri; Extra Large, limite di altezza e profondità di 50 metri. Ad ogni modo i giocatori saranno in grado anche di acquistare più parcels confinanti e combinare più terreni assieme per formare spazi più grandi.

Figura 2.1: Mappa del mondo di Somnium Space

L'esperienza di gioco in Somnium inizia in una zona detta Somnium Waypoint, la quale corrisponde al punto nevralgico/centrale dell'intero mondo virtuale. Ciò ha ovviamente un forte impatto nel gioco, infatti più il tuo appezzamento di terreno si troverà vicino al centro, più interazioni e visite il tuo possedimento otterrà e di conseguenza maggiori possibilità di monetizzazione. Non a caso i terreni più costosi sono tipicamente quelli vicino al centro, vicino ai corsi d'acqua (sia per motivi di trasporto che di panorama virtuale) e vicino a grossi appezzamenti, composti di più parcels, tutti con un unico proprietario. Questo è per pure ragioni speculative, perché si suppone che potrebbero appartenere ad una grande azienda che in futuro potrebbe creare un proprio spazio virtuale, donando importanza alla zona.

I terreni, che sono in numero finito, possono essere ottenuti mediante delle aste organizzate da Somnium stessa. I giocatori possono offrire criptomonete per cercare di aggiudicarsi uno o più appezzamenti.

Nella mappa spaziale di Somnium i vari terreni sono collegati da strade. Acquistando più di un lotto, le strade e i territori tra essi compresi potranno essere utilizzati come ulteriore superficie edificabile.

A tal proposito il "Builder" diventa di fondamentale importanza nel metaverso, essendo il solo strumento per iniziare a sviluppare creazioni sulla propria terra, facendo uso di un'interfaccia appositamente progettata per le costruzioni digitali.

Si possono costruire territori da zero scegliendo tra le varie risorse, appositamente progettate e offerte dal "Somnium Store", per migliorare ulteriormente le proprie creazioni.

È anche possibile importare e modificare i propri modelli dai più popolari software di modellazione 3D, oltre che venderli nel Somnium Store e monetizzare tali creazioni; infatti chi acquista direttamente modelli già pronti per l'uso nello Store può godersi immediatamente le relative esperienze senza bisogno di svolgere alcun ulteriore lavoro.

• **Worlds:** i worlds sono istanze indipendenti all'interno del mondo virtuale, create utilizzando UnitySDK di Somnium. Ogni worlds di Somnium Space è un

token che una volta comprato può essere piazzato nel proprio parcel di terreno. Possedendo un world si ottiene il diritto di caricare un certo ammontare di contenuto sui server di Somnium, in base alla dimensione del token posseduto:
Small world - 75MB
Medium world - 200MB
Extra Large world - 500MB
La dimensione del world che può essere piazzato su un terreno dipende dalla dimensione del parcel corrispondente.

Gli utenti, una volta entrati nell'appezzamento, vedranno automaticamente un portale che condurrà al world. Come tutti i token, anche i worlds sono assets e quindi possono essere commerciati all'interno del mercato. Se si compra un world vuoto è possibile costruirlo da zero inserendo oggetti tramite UnitySDK di Somnium. I Worlds tipicamente sono riempiti con giochi interattivi, casino e altre esperienze per gli utenti. Partecipando a queste attività si possono vincere ricompense sotto forma di CUBEs, la criptomoneta proprietaria di Somnium Space. Uno dei vantaggi dell'uso dei Worlds sta nel fatto che l'utente può partecipare alle attività senza pagare una gas fee per ogni singola esperienza di gioco.

• **Wearings:** abbigliamento e accessori vengono creati direttamente da Somnium Space in collaborazione con artisti o designer e messi in vendita nel mercato di Somnium, oppure sono creati dagli utenti in cambio di Cubes esattamente come gli Avatar.

Essi vengono formati e modellati in base all'abilità del giocatore e dei suoi gusti, per essere venduti sul Marketplace dedicato agli utenti di Somnium ad altri utenti.

Alcuni oggetti di vestiario possono essere rari o esclusivi, il che significa che potrebbero essere disponibili solo per un periodo limitato o in quantità limitate. Questi oggetti possono diventare dei veri e propri collezionabili, aumentando il loro valore nel tempo.

Una volta prodotto un capo d'abbigliamento o un accessorio, è possibile coniarlo come un NFT su Ethereum o Polygon, per poi tenerlo sul proprio parcel mentre viene messo in mostra sul "negozio virtuale" dell'utente.

È anche possibile rimanere sul proprio terreno per fornire assistenza ai clienti che sono interessati ad acquistare l'abbigliamento in vendita.

• **Mezzi di trasporto:** uno degli aspetti che rendono particolarmente immersivo questo mondo virtuale è legato ai trasporti. Gli spostamenti da un parcel ad un altro infatti non sono immediati, come ci si potrebbe aspettare in un videogioco, ma richiedono del tempo per spostarsi lungo le strade che collegano i

vari appezzamenti di terra. Nello specifico, gli avatar camminano ad una velocità di 4 mph (6.44 km/h) e, considerando che la mappa di Somnium è all'incirca un quadrato con lato di 6 km, questo può significare tempi considerevoli per spostarsi tra due punti della mappa. Anche per questo i parcel in posizione centrale sono venduti a prezzi mediamente più alti di quelli periferici. Se un utente non vuole perdere tempo negli spostamenti però ha la possibilità di acquistare dei mezzi di trasporto, anch'essi sotto forma di NFT e per i quali il blocco corrispondente nella blockchain costituisce il contratto di proprietà. Al momento si possono comprare auto che permettono di spostarsi a 25 mph (40.23 km/h) e in futuro verranno introdotti altri mezzi con diverse caratteristiche in termini di velocità ed accelerazione, oltre che nuovi design, principalmente ad opera di CryptoMotors, la prima società produttrice di auto digitali che si basa sulla tecnologia di Ethereum. Il proprietario è l'unico che può guidare un'auto e attualmente ne esistono solo 5 nel mondo di Somnium. Per il futuro però i creatori immaginano una sorta di car sharing, con auto lasciate in giro per la mappa che possano essere utilizzate da tutti gli utenti in cambio di un pagamento basato sul tempo di utilizzo.
L'altro mezzo disponibile per l'acquisto è il kayak, che ovviamente permette di muoversi attraverso gli specchi d'acqua presenti sulla mappa.

- **Teletrasporti:** se la velocità delle auto non fosse sufficiente, nel mondo di Somnium c'è anche la possibilità di acquistare dei teletrasporti, che ovviamente consentono spostamenti istantanei. Esistono attualmente 50 teletrasporti di due tipi diversi, Indiegogo Founder's e ILO. Questi NFT hanno un costo non indifferente: uno degli ultimi ad essere stati venduti ad esempio è stato pagato 32 ETH. Quando un utente compra un teletrasporto può scegliere se tenerlo privato o piazzarlo sul proprio terreno rendendolo pubblico. Così gli altri utenti potranno teletrasportarsi da e per quel terreno pagando un biglietto o un abbonamento mensile. Tutti i ricavi di questo tipo vengono messi insieme e spartiti, una volta al mese, tra i 50 possessori di teletrasporti pubblici più attivi. Le due tipologie di teletrasporti inoltre ricevono un diverso incremento del guadagno: 200% in più per quelli di tipo Indiegogo Founder's e 50% in più per quelli di tipo ILO.

- **Tickets:** esistono anche NFT che fungono da biglietti e che consentono l'accesso, a chi li possiede, ad una determinata parcel di terra. Questi vengono usati perchè sul mondo virtuale di Somnium vengono organizzati svariati tipi di eventi, da concerti a performance live di artisti, da sfilate di moda ad aste per l'acquisto di NFT di vario tipo. Chi non possiede il biglietto corretto semplicemente non vedrà e sentirà nulla nella parcel in questione. Questo meccanismo permette di creare nel mondo virtuale veri e propri musei dove gli artisti possono esporre le loro opere, sotto forma di NFT, e gli utenti possono ammirarle pagando il biglietto.

Tra i vari eventi che vengono organizzati c'è stata ad esempio nel 2022 la prima sfilata di moda virtuale, dove i modelli sfruttavano le tute aptiche Teslasuit per trasferire i movimenti ai loro avatar. In Italia la prima sperimentazione di questo tipo è stata fatta dal comico Maccio Capatonda che ha realizzato lo spettacolo "Maccioverse", che poteva essere seguito nel mondo virtuale e permetteva agli spettatori di interagire direttamente con lui.

In attesa che venga implementata l'idea futura di dare periodicamente delle criptomonete agli utenti come una sorta di stipendio, seguendo un meccanismo che verrà illustrato in seguito, per ora i metodi che ha un utente per guadagnare *in game* sono, oltre agli scambi con altri utenti e alle ricompense dei teletrasporti, le cacce al tesoro. Periodicamente infatti vengono organizzati in diversi punti della mappa mini-giochi, labirinti o simili, che si concludono col ritrovamento di un codice QR che consente di riscattare il premio, sotto forma di ETH o di CUBEs.
Somnium invece, essendo un gioco gratuito, guadagna principalmente dalle pubblicità mostrate su cartelloni presenti sulla mappa virtuale e dalla vendita degli appezzamenti di terra tramite aste. Attualmente sono state effettuate 4 aste. La terza ad esempio è durata 4 settimane ed ha fruttato circa 400000 USD.
Le più grandi aziende a livello mondiale stanno acquistando o hanno già acquistato grandi appezzamenti di terra virtuale per creare strutture di vario tipo. Tesla ad esempio ha creato un concessionario virtuale dove è possibile visionare nei dettagli un modello tridimensionale delle loro auto e dove nel 2018 il co-fondatore di Somnium Space Tomas Mika ha potuto acquistare una Tesla model 3, completando il primo acquisto di un'auto in realtà virtuale. Uno dei punti di forza portati dall'uso di una blockchain è infatti la possibilità di creare un'economia nel gioco, ma sempre mantenendola strettamente connessa con l'economia del mondo reale.

2.2 Blockchain

2.2.1 Una soluzione ibrida con Polygon e Ethereum

Quando vengono effettuate transazioni frequenti sulla rete Ethereum, le gas fees aumentano, rendendo le transazioni più costose durante i periodi di maggiore afflusso. Al contrario, quando il volume delle transazioni è basso, le gas fees diminuiscono. Per questo le soluzioni di secondo livello stanno diventando sempre più popolari nel contesto di Ethereum. Somnium si appoggia alla blockchain di Polygon, precedentemente noto come Matic, una criptomoneta che crede nel fornire transazioni ETH meno costose all'interno della propria rete, anche perché è meno affollata. Gli utenti potranno inviare ETH e Cubes dal loro stesso indirizzo Ethereum su Polygon con un semplice click, utilizzando poi gli stessi ETH e Cubes su una piattaforma diversa, simile a OpenSea. Somnium faciliterà questo processo per rendere l'utilizzo più semplice e user friendly. Con pochi click nello spazio di Somnium, insieme a una transazione Ethereum, gli utenti potranno effettuare migliaia di transazioni gratuite, o quasi. Infine, con un altro click su un pulsante e pagando una gas fee, sarà possibile inviare nuovamente ETH, Cubes e NFT sulla rete principale di Ethereum.

2.2.2 Una criptomoneta proprietaria: CUBEs

Somnium Cubes (CUBE) è una valuta di gioco sviluppata sulla tecnologia blockchain di Ethereum (ERC20) per semplificare i trasferimenti di denaro tra i giocatori. All'interno di Somnium Space, i token CUBE potranno essere spesi per accedere a giochi arcade e parchi divertimenti, utilizzare auto e teletrasporti. Gli artisti potranno vendere biglietti in CUBE, consentendo ai visitatori di partecipare a musei creati dagli utenti o assistere a concerti.

Somnium progetta di sviluppare nuovi smart contracts per migliorare la gestione dei CUBEs, consentendo transazioni quasi gratuite all'interno del mondo virtuale a velocità molto elevate, per favorire il vr-commerce.
Il vantaggio di usare una moneta di gioco sta nel fatto che gli utenti, invece di utilizzare pagamenti in USD con carte di credito per ogni transazione, potranno sfruttare i CUBEs per svolgere le attività all'interno del mondo virtuale più rapidamente e con meno costi di transazione.

CUBE è disponibile su diverse piattaforme di scambio di criptovalute, tra cui Uniswap, Gemini, CoinEx e Bitget. È importante sottolineare che i Somnium Cubes (CUBE) sono una valuta di gioco e non sono progettati né intesi come strumenti finanziari per speculazione o investimenti. I Cubes sono utilizzati esclusivamente per facilitare lo scambio di servizi e beni all'interno di un'economia funzionante

all'interno di un mondo di realtà virtuale.

Un indirizzo Ethereum può contenere diversi tipi di asset digitali, tra cui ETH, token CUBE, token NFT (token non fungibili basati sullo standard ERC721 di Ethereum) e token di side-chains, come Solana.

La valuta CUBE è attualmente classificata al 710º posto (giugno 2023) su CoinMarketCap, con una capitalizzazione di mercato di 13.638.249 EUR. Ha un'offerta circolante di 12.500.000 CUBE e un'offerta massima di 100.000.000 CUBE.

Figura 2.2: Valore CUBE/EURO nell'ultimo anno (giugno 2023) - Coinmarketcap.com

Capitolo 3

Sviluppi futuri

Somnium Space ha pubblicato un *Economy Paper*, con lo scopo di illustrare la visione del team e quelli che sono i progetti di sviluppo futuri.

Un ulteriore obiettivo è quello di inserire aggiornamenti, riguardo l'esperienza stessa nella realtà virtuale.
Queste nuove possibilità, oltre che sull' *Economy Paper*, sono pubblicati su diverse piattaforme social (ad esempio *@SomniumSpace* su Twitter) e sulla Road Map ufficiale di Somnium Space [6].

3.1 Road Map

La **Road map** di Somnium Space è un ottimo modo per seguire i progressi dei progetti di Somnium Space.

Al suo interno si può trovare una lista esaustiva di ciò su cui attualmente sta lavorando il team di sviluppo, suddivisa in 3 sezioni: pianificato, in corso e completato.

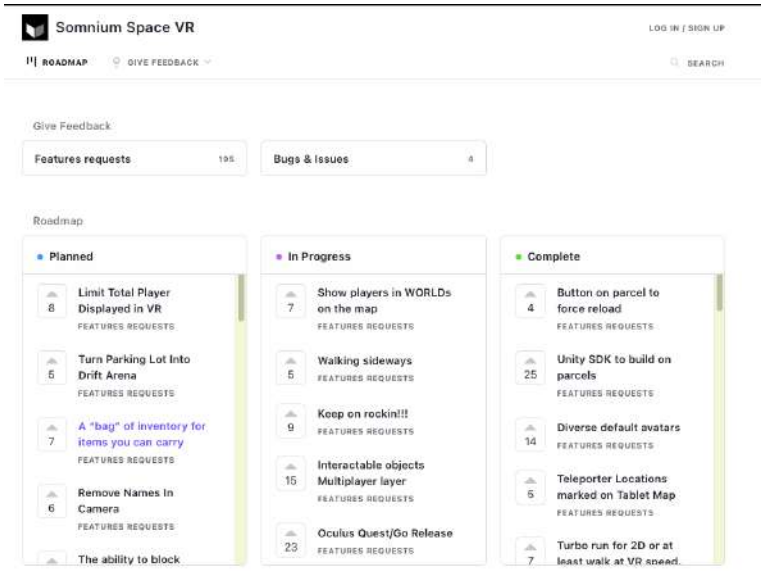


Figura 3.1: Road Map di Somnium Space

3.2 Karma

All'interno dell'Economy Paper si rimanda ad aggiornamenti riguardo le ricompense ottenibili in base al Karma level.

Il **Karma Level** rappresenta lo status sociale dell'abitante virtuale e come gli altri lo percepiscono.
Il Karma level è calcolato combinando diversi fattori:

- **Valutazione degli altri giocatori.** I giocatori più rispettabili con un livello di Karma più alto possono influenzare il Karma Level degli altri con la loro valutazione.

- **Coinvolgimento all'interno del mondo di Somnium Space.** Il tempo totale di gioco, la percentuale di scoperta del mondo, la proprietà di terreni e l'interazione attiva nelle transazioni economiche.

- **Altri fattori.** L'attività di costruzione delle proprietà, l'organizzazione e la partecipazione agli eventi, ecc.

Nei futuri aggiornamenti sarà introdotta la possibilità per i giocatori di Somnium di guadagnare Somnium Cubes (CUBE) in base al loro livello di Karma.

Gli utenti che sono attivi nella comunità e forniscono valore e servizi come guide turistiche, istruttori, ecc. avranno la possibilità di guadagnare ricompense sotto forma di Karma che possono essere convertite in Somnium Cubes (CUBE) per ottenere valore spendibile immediato.

3.3 Modalità Live Forever

Uno dei progetti più ambiziosi del fondatore Artur Sychov prende il nome di modalità "**Live forever**".

Si tratta di una funzionalità che consente all' utente di memorizzare come dati i propri movimenti e conversazioni, quindi duplicarli in un avatar che si muove e parla proprio come lui e può continuare a farlo per molto tempo dopo la sua morte. L'obiettivo principale è quello di entrare in contatto con i defunti ogni volta che lo si desidera. In particolare, questo clone virtuale dell'utente può continuare ad evolversi nel tempo di pari passo all'intelligenza artificiale, sfruttando i dati raccolti negli anni precedenti. Questo progetto si sposa perfettamente con la tecnologia della blockchain, che per sua natura garantisce completa trasparenza nella gestione di dati personali degli utenti.

Ciò che ha permesso la messa in atto di questa idea è il potenziale che si nasconde dietro la raccolta dati nella realtà virtuale. In uno studio dell'ottobre 2020 pubblicato su *Nature*, si afferma che dopo meno di cinque minuti di monitoraggio dei movimenti del corpo delle persone, la tecnologia della realtà virtuale potrebbe identificare qualcuno con una precisione del 95% su un gruppo di 500 persone [4].

Gli utenti che desiderano partecipare al progetto "Live Forever" devono avviare il processo di registrazione e memorizzazione dei dati che nella prima fase di progettazione si limita ai movimenti e ai suoni degli utenti all'interno dei loro appezzamenti di terra.

Per quel che riguarda la monetizzazione dei dati sensibili delle persone, il CEO sta cercando di costruire un modello di business responsabile che consenta agli utenti di sentirsi sicuri nel condividere i propri dati per l'analisi. La società afferma infatti che non raccoglierà dati su nessuno a meno che l'utente non decida di pagare per il servizio. Il prezzo addebitato ai primi utenti è di $50 per un anno di servizio.

Artur Sychov ha presentato questo progetto nel 2022 prevedendo che sarebbe stato disponibile entro cinque anni. A causa dei recenti progressi nell'intelligenza artificiale, potrebbe volerci meno tempo per far si che le persone possano conversare con un clone in realtà virtuale senza rendersi conto che non si tratta di una persona reale.

Capitolo 4

Conclusione

Come è noto, ad oggi, il Metaverso in senso stretto non esiste, ma sempre più aziende stanno investendo per far si che questo progetto diventi realtà.
In questo campo Somnium Space è una delle aziende più all'avanguardia grazie anche all'integrazione della tecnologia blockchain in un contesto di realtà virtuale e alla flessibilità nelle possibilità di utilizzo, con o senza VR.

Bibliografia

[1] *Cos'è e come funziona Somnium Space*. URL: https://osservatoriometaverso.it/cose-e-come-funziona-somnium-space/.

[2] *Founder: You'll Soon Be Able to Talk to Your Dead Mom In the Metaverse Thanks to ChatGPT*. URL: https://www.vice.com/en/article/bvmqbv/founder-youll-soon-be-able-to-talk-to-your-dead-mom-in-the-metaverse-thanks-to-chatgpt.

[3] *Metaverse Company to Offer Immortality Through 'Live Forever' Mode*. URL: https://www.vice.com/en/article/pkp47y/metaverse-company-to-offer-immortality-through-live-forever-mode.

[4] Mark Miller et al. "Personal identifiability of user tracking data during observation of 360-degree VR video". In: *Scientific Reports* 10 (ott. 2020). DOI: 10.1038/s41598-020-74486-y.

[5] *Somnium CUBE*. URL: https://coinmarketcap.com/it/currencies/somnium-space-cubes/.

[6] *Somnium Road Map*. URL: https://somnium-space.canny.io/.

[7] *Somnium Space Canny*. URL: https://somnium-space.canny.io/.

[8] *Somnium Space Economy Paper*. URL: https://somniumspace.com/files/Somnium%20Space%20Economy%20Paper.pdf.

[9] *Somnium Space Goes Multi-Chain to Launch NFT Land Offering*. URL: https://dappradar.com/blog/somnium-space-goes-multi-chain-to-launch-nft-land-offering.

[10] *Somnium Space Guida Completa*. URL: https://www.comprarebitcoin.com/somnium-space-guida-completa/.

[11] *Somnium Space Guide*. URL: https://somniumspace-guide.com/?page_id=54.

[12] *Somnium Space inserisce l'opzione "Vivi per Sempre"*. URL: https://cryptonomist.ch/2022/04/23/somnium-space-inserisce-opzione-vivi-per-sempre/.

[13] *Somnium Worlds*. URL: https://somniumspace.medium.com/announcing-somnium-worlds-somnium-web-blockchain-avatars-slo-details-prices-81ec741e2d3a.

PROPAGAZIONE DELL'INFORMAZIONE

CHAINLINK

Alessio Attanasi, Giorgia Buccelli, MariaCannistrà, RachidEl Amrani

POLITECNICO DI TORINO

TESINA BLOCKCHAIN E CRIPTOECONOMIA

CHAINLINK

Attanasi Alessio (319689)
Buccelli Giorgia (303492)
Cannistrà Maria (304632)
El Amrani Rachid (286847)

ANNO ACCADEMICO 2022/2023

Indice

1 Introduzione 3

2 Architettura 5
- 2.1 Architettura on-chain . . . 6
- 2.2 Architettura off-chain . . . 8

3 Sicurezza dell'oracolo 11
- 3.1 Oracolo ideale . . . 11

4 Approccio alla decentralizzazione di ChainLink 15
- 4.1 Fonti distributive . . . 16
- 4.2 Oracoli distributivi . . . 16

5 Servizi di Sicurezza ChainLink 19
- 5.1 Sistema di Validazione . . . 20
- 5.2 Sistema di Reputazione . . . 20
- 5.3 Servizio di certificazione . . . 21
- 5.4 Servizio di aggiornamento dei contratti . . . 21
- 5.5 Utilizzo del token LINK . . . 22

6 Off-Chain Reporting 23

7 Conclusione 25

Capitolo 1

Introduzione

Gli smart contracts sono applicazioni che vengono eseguite su un'infrastruttura decentralizzata, come una blockchain. Essi sono a prova di manomissione, ovvero nessuna parte (nemmeno il loro creatore) può alterare il loro codice o interferire con la loro esecuzione. Storicamente, i contratti incorporati nel codice venivano eseguiti in modo centralizzato, di conseguenza essi potevano essere soggetti ad alterazione, risoluzione e persino cancellazione da parte di una parte privilegiata (l'autorità centrale). Al contrario, le garanzie di esecuzione degli smart contracts, che vincolano tutte le parti a un accordo come scritto originariamente, creano un nuovo e potente tipo di relazione fiduciaria che non si basa sulla fiducia in nessuna delle parti coinvolte, bensì la fiducia è riposta nella tecnologia stessa. Poiché sono autoverificanti e autoeseguibili (ovvero, a prova di manomissione come spiegato sopra), gli smart contracts offrono quindi un veicolo superiore per realizzare e amministrare accordi digitali. Il nuovo potente modello di fiducia rappresentato dagli smart contracts, tuttavia, introduce una nuova sfida tecnica: la connettività.

La stragrande maggioranza delle interessanti applicazioni degli smart contracts si basa su dati sul mondo reale che provengono da risorse chiave, in particolare feed di dati e API, che sono esterne alla blockchain. A causa dei meccanismi di consenso alla base delle blockchain, una blockchain non può recuperare direttamente tali dati critici.

Viene proposta una soluzione al problema della connettività dello smart contract sotto forma di ChainLink, una rete di oracoli decentralizzata creata da Sergey Nazarov e Steve Ellis ed introdotta nel 2017, quando è stato presentato il whitepaper, ed è stata lanciata ufficialmente nel 2019. Chainlink fornisce transazioni sicure utilizzando fonti di dati e API esterne, consentendo a chiunque di unirsi alla rete e di fornire dati o di completare i "lavori" di Chainlink, come la gestione di nodi e oracoli affiliati.
Nel 2018, Chainlink ha integrato Town Crier, un oracolo blockchain basato su un ambiente di esecuzione affidabile che è stato co-sviluppato da Ari Juels della Cornell University. Questa integrazione ha permesso a Chainlink di collegare la blockchain di Ethereum con fonti web che utilizzano HTTPS.
Nel 2019 Chainlink ha lanciato ufficialmente il proprio protocollo, seguito dalla registrazione del marchio Chainlink nelle Isole Cayman. Nel 2020 Chainlink ha integrato DECO, un altro progetto co-creato da Juels. DECO è un protocollo che utilizza prove a conoscenza zero (zero-knowledge proofs) per consentire agli utenti di dimostrare la veridicità delle informazioni a un oracolo blockchain senza rivelare informazioni sensibili.
Chainlink ha pubblicato nel 2021 un secondo whitepaper che introduce Chainlink 2.0. Il documento espande le capacità delle reti oracolo decentralizzate e introduce smart contract ibridi che utilizzano il codice on-chain e i servizi off-chain forniti dalle reti oracolo.

Ciò che differenzia ChainLink da altre soluzioni Oracle è la sua capacità di operare come una rete completamente decentralizzata. Questo approccio decentralizzato limita la fiducia in ogni

singola parte, consentendo di estendere la qualità a prova di manomissione apprezzata negli smart contracts all'operazione end-to-end tra gli smart contracts e le API su cui si basano.
Rendere gli smart contracts capaci di interagire con le risorse off-chain è necessario se si intende sostituire gli accordi digitali oggi in uso. Esempi di potenziali smart contracts di nuova generazione e relativi requisiti di dati includono:

- Gli smart contracts su titoli come obbligazioni, derivati su tassi di interesse e molti altri richiederanno l'accesso alle API che riportano i prezzi di mercato e i dati di riferimento del mercato, ad es. tassi di interesse.
- Gli smart contracts assicurativi avranno bisogno di feed di dati sui dati IoT relativi all'evento assicurabile in questione, ad esempio: la porta magnetica del magazzino era chiusa al momento della violazione, il firewall dell'azienda era online o il volo per cui avevi l'assicurazione è arrivato in tempo.
- Gli smart contracts di trade finance avranno bisogno di dati GPS sulle spedizioni, dati dai sistemi ERP della catena di approvvigionamento e dati doganali sulle merci spedite per confermare l'adempimento degli obblighi contrattuali.

Un altro problema comune a questi esempi è l'impossibilità per gli smart contracts di inviare dati a sistemi off-chain. Tale output assume spesso la forma di un messaggio di pagamento indirizzato all'infrastruttura centralizzata tradizionale in cui gli utenti hanno già un account, ad esempio per pagamenti bancari, PayPal e altri circuiti di pagamento. La capacità di ChainLink di inviare in modo sicuro i dati alle API e a vari sistemi legacy per conto di uno smart contract consente la creazione di contratti a prova di manomissione esterni.

Dopo questa breve introduzione, verrà esaminata l'architettura della rete, presentando sia un semplice sistema di aggregazione dei dati dei contratti on-chain, sia un meccanismo di consenso off-chain più efficiente. Viene descritto anche il supporto dei servizi di monitoraggio della reputazione e della sicurezza per ChainLink che aiutano gli utenti ad effettuare selezioni informate del provider e ottenere un servizio solido. Viene illustrato, in seguito, l'approccio di ChainLink alla decentralizzazione, distribuzione e sicurezza degli oracoli, con una discussione dei quattro servizi di sicurezza proposti da ChainLink, nonché del ruolo svolto dai token LINK. Concludendo, viene presentato il protocollo di off-chain reporting, che comporta una maggiore decentralizzazione e scalabilità della rete Chainlink.

Capitolo 2

Architettura

L'architettura di Chainlink è suddivisa in due componenti che fanno da collegamento tra il mondo interno della blockchain e il mondo esterno da cui ricevere le informazioni:

- architettura on-chain, la parte della piattaforma che è eseguita direttamente sulla blockchain;
- architettura off-chain, costituita da nodi esterni alla blockchain.

La parte on-chain del sistema riguarda quegli smart contracts relativi alla richiesta di dati esterni alla blockchain e l'utilizzo di tali dati per automatizzare gli accordi e le transazioni. La parte off-chain del sistema è costituita da nodi oracolari, responsabili della raccolta, della verifica e della trasmissione di dati provenienti da diverse fonti agli smart contracts su blockchain. Ogni parte del sistema può essere migliorato utilizzando tecniche più aggiornate e implementazioni competitive.

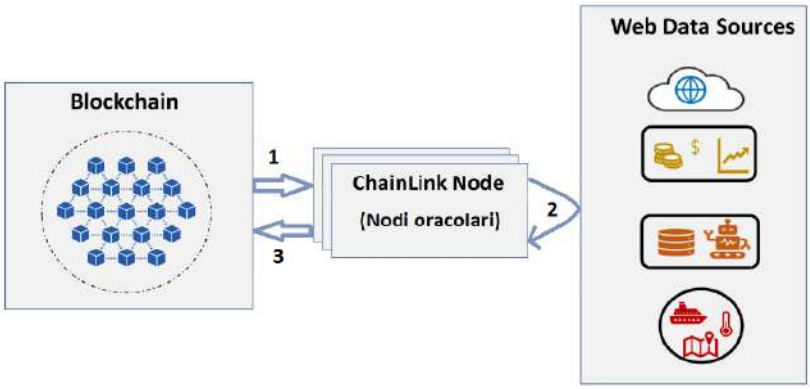


Figura 2.1. Esecuzione del flusso di lavoro

L'esecuzione del flusso di lavoro di Chainlink, rappresentata nella Figura 2.1, è:

1. Uno smart contract all'interno della blockchain richiede dati esterni alla rete,
2. I nodi oracolari, ricevuta la richiesta, interrogano le risorse esterne (API),
3. I nodi oracolari trasmettono i dati ricevuti dalle API alla blockchain, dove verranno aggregati e utilizzati dallo smart contract che ne ha fatto richiesta.

Ciascuna parte del processo è a sua volta costituita da sottoprocessi, ciascuno svolto da una componente specifica dei sistemi on-chain e off-chain.

2.1 Architettura on-chain

L'architettura on-chain di Chainlink si compone di due tipologie di smart contract:

- USER-SC rappresenta un contratto utente. Esso è responsabile dei requesting contracts, ovvero quei contratti che richiedono dati da fonti esterne alla blockchain, in cui viene specificato il tipo di dati richiesti e le condizioni che devono essere soddisfatte affinché i dati siano considerati validi. Nello specifico, USER-SC deve creare una richiesta indicando l'indirizzo dell'oracolo, l'ID del lavoro in modo che l'oracolo sappia quali compiti eseguire e la funzione di callback a cui l'oracolo invia la risposta.

- CHAINLINK-SC rappresenta un contratto on-chain relativo all'interfaccia per la richiesta di contratti. Esso è responsabile di tre tipi di contratto:

  - *reputation contract*,
  - *order-matching contract*,
  - *aggregating contract*.

  Il primo tipo di contratto è progettato per misurare e tracciare la reputazione di un particolare utente o entità su una rete blockchain sulla base del loro comportamento. Nello specifico, viene assegnato a ciascun fornitore di servizi oracolo un valore sulla base di diversi fattori, come il tempo di risposta medio, il rapporto di completamento, il deposito di sicurezza medio e altro. Le prestazioni storiche degli oracoli di Chainlink sono pubblicamente disponibili tramite dati firmati sulla catena, consentendo agli utenti di selezionare gli oracoli in base a tali metriche, garantendo fiducia e credibilità di tale fornitore. Gli operatori dei nodi hanno anche la possibilità di fornire dati aggiuntivi come la loro identità, la posizione geografica e le certificazioni di terze parti.

  Il secondo tipo di contratto è progettato per prendere e registrare una proposta di accordo sul livello di servizio (*service level agreement*, con acronimo SLA) e relativi parametri, raccogliere le offerte dei fornitori di oracolo, selezionare le offerte utilizzando il *reputation contract* e finalizzare lo SLA.

  Il terzo tipo di contratto è progettato per raccogliere le risposte dei fornitori di oracoli e calcolare il risultato collettivo finale della query. Esso, inoltre, è responsabile dell'alimentazione delle metriche dei fornitori di oracoli nel *reputation contract*.

I contratti di ChainLink sono progettati in modo modulare, in modo da permettere agli utenti di configurarli o sostituirli a seconda delle necessità. Ciò che avviene all'interno dell'architettura on-chain si articola in tre fasi:

1. appena risulta necessario richiedere dati esterni alla blockchain, viene selezionato l'oracolo (o rete di oracoli) a cui affidare il compito,

2. trasmissione dei dati all'interno della rete da parte di ciascun oracolo,

3. aggregazione dei risultati.

Durante la prima fase, un acquirente di servizi oracolo specifica i requisiti che costituiscono una proposta SLA, includendo dettagli quali i parametri della query e il numero di oracoli necessari. Inoltre, l'acquirente specifica il *reputation contract* e l'*aggregation contract* da utilizzare per il resto dell'accordo [1]. In tal modo, Chainlink consente agli utenti di definire i termini del lavoro di oracolo richiesto negli on-chain smart contracts. È anche possibile richiedere che i nodi oracolo versino un deposito di sicurezza che viene restituito al nodo solo se esegue il lavoro secondo i

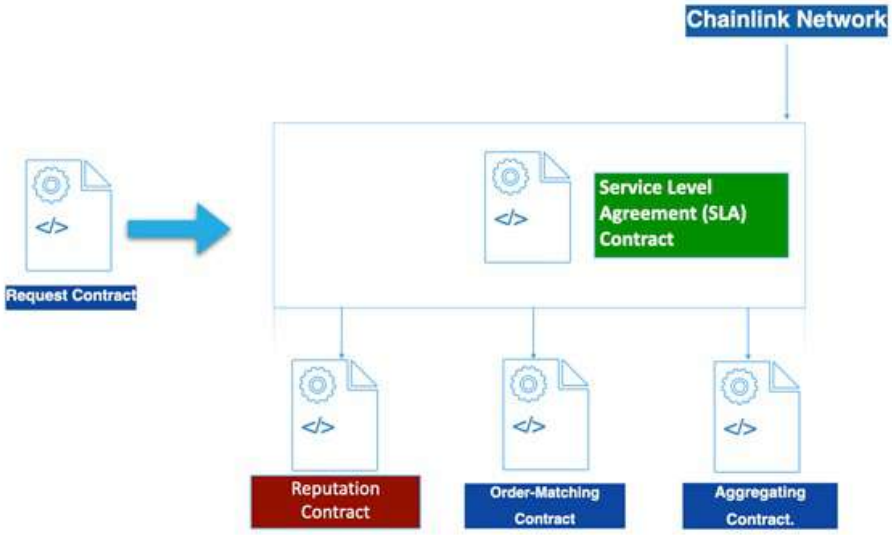


Figura 2.2. Smart contracts

termini preconcordati (ad esempio, i dati vengono consegnati in tempo). La penale depositata è in LINK, il token nativo della piattaforma Chainlink, e incentiva gli oracoli a fornire dati accurati e affidabili.

Utilizzando i registri dei contratti passati e le prestazioni presenti nella catena vengono generati elenchi off-chain, da cui gli acquirenti possono ordinare, filtrare e selezionare manualmente gli oracoli. Quando la selezione manuale è possibile, agli oracoli selezionati viene presentata la proposta SLA e viene raggiunto un accordo tra acquirente e oracoli prima di finalizzare lo SLA sulla catena. Quando invece c'è dinamicità nelle richieste da un contratto ai nodi oracolari, invece di contattare direttamente gli oracoli, l'acquirente sottopone la propria proposta SLA a un *order-matching contract*. Viene generato un registro che i fornitori di oracoli possono monitorare e filtrare in base alle loro capacità e ai loro obiettivi di servizio. Se un oracolo sceglie di fare un'offerta per la proposta, si impegna a rispettare il contratto in quanto allega la penale che andrebbe persa nel caso di un suo comportamento scorretto, come definito nello SLA.

Tra le offerte effettuate, il contratto accetta solo quelle relative ai nodi che soddisfano i requisiti dello SLA per tutta la durata del periodo di offerta. Al termine di tale periodo e se il numero di offerte che soddisfano i requisiti ha raggiunto il numero di oracoli richiesto dall'acquirente, i nodi oracolari vengono selezionati tra tutti quelli validi. Agli oracoli non selezionati viene restituita la penale e viene registrato nella catena lo SLA definitivo. Si attiva un registro che notifica gli oracoli selezionati e quest'ultimi eseguono l'incarico.

Gli oracoli raccolgono e selezionano i dati richiesti dal mondo esterno alla blockchain e li trasmettono nuovamente all'interno dell'architettura on-chain. Questo passaggio di dati costituisce la seconda fase del flusso di lavoro all'interno della catena.

Durante la terza fase, invece, i dati ricevuti dagli oracoli vengono confrontati dall'*aggregating contract*, il quale calcola una risposta ponderata che viene restituita al contratto specifico in USER-SC. Inoltre, la validità di ogni risposta dell'oracolo viene comunicata al *reputation contract*. Non esiste un unico *aggregating contract*, ma un insieme standard di tali contratti, in quando la scelta del contratto e l'identificazione di outliers o valori errati dipendono dall'applicazione e dal tipo di dati con cui si ha a che fare (ad esempio dati numerici o booleani). Dunque, l'acquirente specifica l'indirizzo di contratto configurabile tra quelli esistenti. Inoltre, è possibile specificare anche contratti personalizzati, purché conformi all'interfaccia di calcolo standard.

2.2 Architettura off-chain

L'architettura off-chain di Chainlink è composta da nodi oracolari connessi alla blockchain. Ciascun oracolo opera senza alcuna dipendenza da altri oracoli, ovvero raccoglie le risposte dalle richieste off-chain in modo indipendente. Inoltre, può liberamente far parte contemporaneamente di diverse reti di oracoli.

Il tipo di lavoro più comune per un nodo consiste nell'effettuare una richiesta GET a un'API (ovvero un metodo di richiesta HTTP per prelevare dati da una fonte), recuperare alcuni dati da essa, analizzare la risposta, convertire il risultato in dati compatibili con la blockchain e quindi inviarlo in una transazione al contratto oracolo. Le singole risposte pervenute dai diversi nodi oracolari vengono combinate on-chain tramite uno dei diversi meccanismi di consenso disponibili, per produrre una risposta globale che viene restituita a un *requesting contract* USER-SC.

Ciascun nodo oracolo è caratterizzato dalla massima flessibilità per quanto riguarda i tipi di dati che possono essere recuperati e il modo in cui tali dati possono essere forniti. Infatti, ogni nodo dispone di una serie di *core adapters* precostruiti, che gli consentono di connettersi a qualsiasi API aperta e di fornire i dati sulla catena. Questi adattatori forniscono ai nodi Chainlink alcune funzionalità, ma è possibile aggiungere estensioni software, note come *external adapters*, che offrono ulteriori servizi specializzati off-chain e permettono di accedere a qualunque risorsa esterna. Tali servizi riguardano principalmente la varietà di dati a cui accedere e il tipo di calcoli che possono essere eseguiti. Gli *external adapters* possono, ad esempio, eseguire calcoli off-chain sui dati (producendo una media delle risposte dei nodi) o accedere ad API autenticate che richiedono credenziali.

La differenza sostanziale tra le due tipologie di nodi oracolari è la seguente:

- i nodi *Core* si interfacciano con gli smart contracts della blockchain e si occupano di pianificare e bilanciare il lavoro tra i vari servizi esterni,
- i nodi *External Adapters* comunicano con le API esterne con una semplice specifica JSON e sono la rappresentazione off-chain di servizi REST-API.

Il lavoro eseguito dai nodi Chainlink viene suddiviso in incarichi. Ciascun incarico è costituito da un insieme di sotto-attività più piccole, che vengono elaborate come una pipeline. Infatti, ogni sotto-attività è responsabile di eseguire un'operazione specifica e trasmettere il risultato alla sotto-attività successiva, e così via fino a raggiungere un risultato finale. Alcune sotto-attività sono integrate nel software del nodo di ChainLink, tra cui le richieste HTTP, JSON *pairing* e la conversione in vari formati di blockchain.

Oltre alle sotto-attività integrate, è possibile definire sotto-attività personalizzate creando gli *adapters*. Modellando tali adattatori in modo orientato ai servizi, è possibile implementare con facilità i programmi in qualsiasi linguaggio di programmazione aggiungendo una piccola API intermedia nella parte iniziale del programma. Allo stesso modo, è possibile semplificare l'interazione con complicate API multi-step utilizzando singole sotto-attività parametrizzate. Le informazioni sugli adattatori esterni sono suddivise in tre categorie principali:

- creatori di contratti, responsabili di specificare la richiesta di dati esterni;
- sviluppatori, responsabili di implementare un adattatore esterno per un'API;
- operatori di nodi, responsabili di aggiungere un adattatore esterno al proprio nodo, in modo da poter fornire servizi specializzati agli smart contracts.

Per via degli *external adapters*, la rete Chainlink può espandersi continuamente per supportare nuove funzionalità, come la comunicazione bidirezionale, i pagamenti bancari off-chain, l'interoperabilità con altre blockchain e molto altro, senza mettere a rischio le funzioni principali della rete.

La maggior parte degli *adapters* sono open source, per cui vari membri della comunità possono verificare ed eseguire i diversi servizi. Poiché ci sono molti tipi di adattatori creati da numerosi sviluppatori diversi, è fondamentale assicurarsi che gli adattatori siano compatibili tra loro. L'idea iniziale dei creatori di Chainlink è quella di utilizzare un sistema di schemi basato sullo schema JSON, un linguaggio dichiarativo che consente di annotare e convalidare documenti JSON. In tal modo è possibile specificare quali sono gli input di cui ogni adattatore ha bisogno e come devono essere formattati. Allo stesso modo, gli adattatori specificano uno schema di output per descrivere il formato dell'output di ogni sotto-attività.

Dopo aver specificato tutti i componenti dell'architettura di Chainlink, il flusso di lavoro più dettagliato, descritto dalla Figura 6.1, è il seguente:

1. USER-SC effettua una richiesta on-chain,
2. CHAINLINK-SC registra un evento per gli oracoli,
3. il nodo *Core* di ChainLink raccoglie l'evento e instrada l'assegnazione a un *adapter*,
4. l'*adapter* di ChainLink esegue una richiesta a un'API esterna
5. l'*adapter* elabora la risposta e la passa di nuovo al *Core*,
6. il *Core* riporta i dati a CHAINLINK-System,
7. CHAINLINK-SC aggrega le risposte e trasmette la singola risposta a USER-SC.

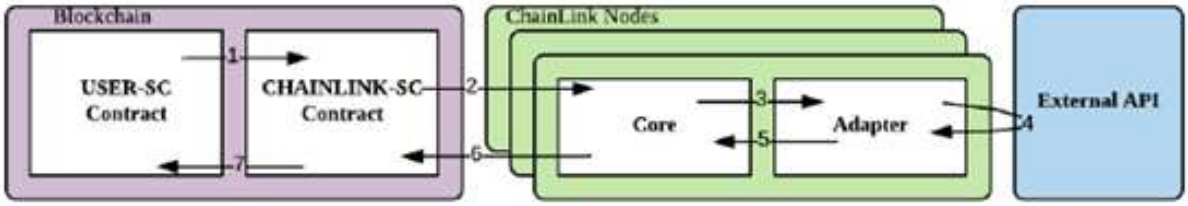


Figura 2.3. Flusso di lavoro ad alto livello

Capitolo 3

Sicurezza dell'oracolo

La sicurezza degli oracoli è un aspetto fondamentale per garantire l'affidabilità e l'integrità delle informazioni fornite agli smart contract basati sulla tecnologia blockchain. Prima di spiegare l'architettura di sicurezza di ChainLink, ovvero i meccanismi che mette in atto, verrà spiegato più nel dettaglio il motivo per cui la sicurezza è importante e cosa significa.

Perché gli oracoli devono essere sicuri?
Per ciascuno dei tre esempi presentati nell'introduzione si possono considerare le seguenti carenze in ambito di sicurezza:

- se un titolo di smart contract riceve un feed di dati falso, potrebbe pagare la parte errata,
- se i feed di dati dell'assicurazione di smart contract possono essere manomessi dalla parte assicurata, potrebbe esserci una frode assicurativa,
- se i dati GPS relativi a una spedizione forniti a un contratto di finanziamento commerciale possono essere modificati dopo che lasciano il provider, il pagamento può essere erogato per le merci che non sono arrivate.

Più in generale, una blockchain ben funzionante offre proprietà di sicurezza molto forti. Gli utenti si affidano alla blockchain come una funzionalità che convalida correttamente le transazioni e impedisce ai dati di essere alterato. Lo trattano a tutti gli effetti come una terza parte fidata. Un servizio di oracoli di supporto alla blockchain deve offrire un livello di sicurezza adeguato con quello della blockchain stessa. Anche un oracolo deve quindi servire gli utenti come un'efficace terza parte fidata, fornendo risposte corrette e tempestive con altissima probabilità. La sicurezza di qualsiasi sistema è forte solo quanto lo è il suo anello più debole, quindi è necessario un oracolo altamente affidabile per preservare l'affidabilità di una blockchain ben progettata.

3.1 Oracolo ideale

Per ragionare sulla sicurezza dell'oracolo, è necessario prima definirla. Un modo istruttivo e basato sui principi di ragionare sulla sicurezza dell'oracolo deriva dal seguente esperimento mentale. Si può immaginare che una terza parte fidata (TTP), che sia un'entità o una funzionalità ideale che esegue sempre le istruzioni fedelmente alla lettera, abbia il compito di gestire un oracolo. Tale oracolo verrà indicato con ORACLE (utilizzando tutte le maiuscole in generale per indicare un'entità completamente fidata dagli utenti) e si suppone che TTP ottenga i dati da una fonte di dati perfettamente affidabile *Src*. Dato questo servizio magico ORACLE, quali istruzioni è

possibile chiedergli di eseguire? Per ottenere la proprietà di **integrità**, nota anche come proprietà di **autenticità**, verrà chiesto semplicemente all'ORACLE di eseguire i seguenti passaggi:

1. *Accettare la richiesta*: importare da uno smart contract USER-SC una richiesta $Req = (Src, \tau, q)$ che specifica un'origine dati di destinazione Src, un'ora o un intervallo di volte τ e una richiesta q;
2. *Ottenere i dati*: inviare la richiesta q a Src all'istante τ;
3. *Restituire i dati*: alla ricezione della risposta a, restituire a allo smart contract.

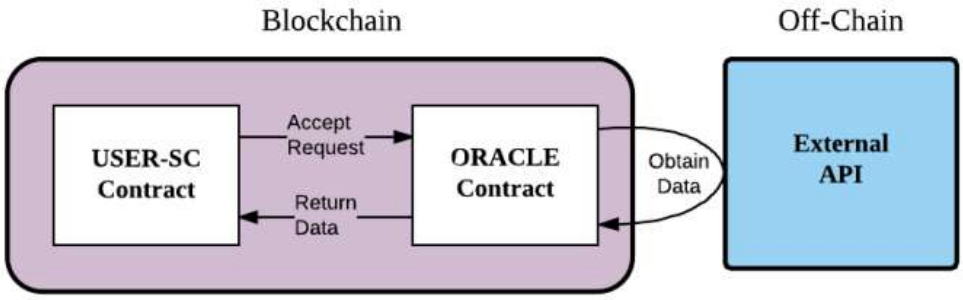


Figura 3.1. Comportamento di un oracolo ideale

Queste semplici istruzioni, eseguite correttamente, definiscono una nozione di sicurezza forte, significativa, ma semplice. Intuitivamente, impongono che ORACLE agisca come un ponte affidabile tra Src e USER-SC. Ad esempio, se Src è il sito web "$https://www.FountOfKnowledge.com$", τ corrisponde alle 16:00 e q = "prezzo per ticker INTC", l'integrità dell'ORACLE garantisce che fornirà a USER-SC esattamente il prezzo di INTC come richiesto alle 16:00 al sito web "$https://www.FountOfKnowledge.com$".

La **riservatezza** è un'altra proprietà desiderabile per gli oracoli. Poiché USER-SC invia Req all'ORACLE in chiaro sulla blockchain, Req è pubblico. Ci sono molte situazioni in cui Req è sensibile e la sua pubblicazione potrebbe essere dannosa. Se USER-SC è un contratto di assicurazione per voli aerei, ad esempio, e invia all'ORACLE una richiesta Req riguardante un volo di un particolare utente (q = "Ether Air Flight 338"), il risultato sarebbe che i piani di volo di un utente vengono rivelati al mondo intero. Se, invece, USER-SC è un contratto per il trading finanziario, Req potrebbe far trapelare informazioni sulle operazioni e sul portafoglio di un utente. Ci sono molti altri esempi, ovviamente. Per proteggere la riservatezza di Req, possiamo richiedere che i dati in Req siano crittografati sotto una (chiave pubblica) appartenente all'ORACLE. Continuando a sfruttare la natura TTP dell'ORACLE, si può quindi semplicemente assegnare all'ORACLE il vincolo del flusso di informazioni. Inoltre, una volta decifrato Req, non bisogna rivelare o utilizzare mai i dati in Req se non per interrogare Src.

Ci sono altre importanti proprietà dell'ORACLE, come la **disponibilità**, l'ultima delle classica triade CIA (*Confidentiality-Integrity-Availability*, ovvero Riservatezza-Integrità-Disponibilità). Un servizio davvero ideale dell'ORACLE, ovviamente, non andrebbe mai in crisi. La disponibilità comprende anche proprietà più sottili come la resistenza alla censura: un oracolo onesto non individuerà particolari contratti intelligenti e negherà le loro richieste. Il concetto di una terza parte fidata è simile alla nozione di una funzionalità ideale utilizzata per dimostrare la sicurezza dei

protocolli crittografici in alcuni modelli. Si può anche modellare una blockchain in termini simili, concettualizzandola in termini di TTP che mantiene una bacheca ideale. Le sue istruzioni sono di accettare transazioni, convalidarli, serializzarli e mantenerli permanentemente sulla bacheca, una struttura di dati di sola aggiunta.

Perché l'oracolo ideale è difficile da raggiungere.
Ovviamente non esiste una fonte di dati Src perfettamente affidabile. I dati possono essere danneggiati in modo benigno o dannoso a causa di siti web difettosi, fornitori di servizi imbroglioni o errori onesti. Se Src non è affidabile, anche se ORACLE funziona esattamente come un TTP come indicato sopra, non soddisfa ancora completamente la nozione di sicurezza necessaria. Data una sorgente errata Src, la proprietà di integrità definita sopra non significa più che la risposta a di un oracolo è corretta. Se il vero prezzo di Intel è 40 e "$https://www.FountOfKnowledge.com$" lo riporta erroneamente come 50, ad esempio, l'oracolo invierà il valore errato a = 50 a USER-SC. Questo problema è inevitabile quando si utilizza un'unica sorgente Src. L'oracolo semplicemente non ha modo di sapere se le risposte che Src fornisce alle sue domande sono corrette. Un problema più grande, ovviamente, è il fatto che il nostro TTP per ORACLE è solo un'astrazione. Nessun fornitore di servizi è incondizionatamente affidabile. Anche il più intenzionato potrebbe essere difettoso o violato. Quindi non c'è modo per un utente o un contratto intelligente di avere l'assoluta certezza che un servizio ORACLE eseguirà fedelmente le sue istruzioni.

ChainLink ragiona sui suoi protocolli di sicurezza in termini di questa funzionalità ideale ORACLE. L'obiettivo in ChainLink è realizzare un sistema del mondo reale con proprietà il più vicino possibile a quelli di ORACLE sotto ipotesi realistiche di fiducia. Verrà spiegato successivamente come questo sia possibile. Per semplicità in quanto segue, verrà indicato con CHAINLINK-SC l'insieme completo di contratti ChainLink, ovvero la sua piena funzionalità on-chain (non solo la sua interfaccia per la richiesta di contratti). In questo modo vengono estratti i molteplici contratti individuali effettivamente utilizzati nell'architettura del sistema.

Capitolo 4

Approccio alla decentralizzazione di ChainLink

Si possono proporre tre soluzioni complementari che garantiscono la sicurezza e l'affidabilità della rete Chainlink contro i nodi difettosi:

1. distribuzione delle fonti di dati;

2. distribuzione di oracoli;

3. utilizzo di hardware affidabile.

Tali soluzioni possono essere applicati singolarmente o combinati tra loro, aumentando in tal modo l'attendibilità dei dati. In particolare, i primi due approcci sono degli esempi di decentralizzazione della rete. Pertanto, verranno discussi in questa sezione. Nella figura 4.1 viene mostrato un esempio in cui questi due approcci vengono usati in modo combinato.

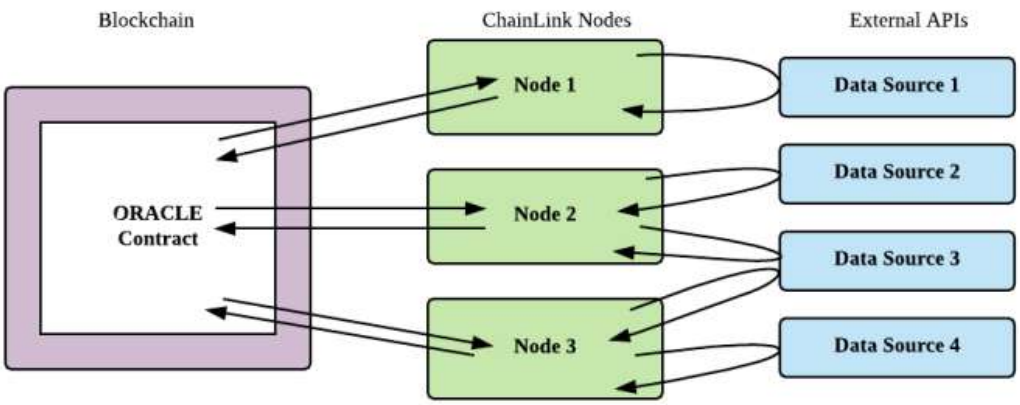


Figura 4.1. Decentralizzazione del Chainlink

4.1 Fonti distributive

Un modo semplice per gestire una singola fonte di dati difettosa Src consiste nell'ottenere dati da più fonti, ovvero distribuire l'origine dati. Un ORACLE affidabile può interrogare una raccolta delle sorgenti $Src_1, Src_2, ..., Src_k$, ottenere le risposte $a_1, a_2, ..., a_k$, e infine aggregarle in un'unica risposta $A = agg(a_1, a_2, ..., a_k)$.

L'aggregazione dei risultati potrebbe essere effettuata in una miriade di modi diversi. Uno dei modi più comuni, ad esempio, è il voto a maggioranza. Se la maggior parte delle fonti restituisce lo stesso valore a, la funzione agg restituisce tale valore; altrimenti restituisce un errore. In questo caso, a condizione che la maggioranza ($> k/2$) delle fonti funzioni correttamente, ORACLE restituirà sempre un valore corretto A.

Molte funzioni alternative agg possono garantire robustezza contro dati errati o gestire le fluttuazioni dei valori dei dati nel tempo (ad esempio, i prezzi delle azioni). In tal caso, agg potrebbe, ad esempio, scartare valori anomali (come i valori più grandi e più piccoli a_i) e produrre la media di quelli rimanenti.

Tuttavia, si può presentare un ulteriore problema. Gli errori possono essere correlati tra le fonti di dati e ciò comporta l'indebolimento delle garanzie fornite dall'aggregazione. Se il sito $Src_1 = EchoEcho.com$ ottiene i suoi dati da $Src_2 = TheHorsesMouth.com$, un errore in Src_2 implicherà sempre un errore in Src_1. Possono verificarsi anche correlazioni più sottili tra le fonti di dati. Chainlink propone inoltre di proseguire la ricerca sulla mappatura e la segnalazione dell'indipendenza delle fonti di dati in un modo facilmente digeribile in modo che gli oracoli e gli utenti possano evitare correlazioni indesiderate.

4.2 Oracoli distributivi

Proprio come le fonti possono essere distribuite, anche il servizio di oracolo ideale può essere approssimato come un sistema distribuito. Questo equivale a dire che invece di un singolo nodo oracolo monolitico O, si possono invece avere una raccolta di n diversi nodi oracolo $O_1, O_2, ..., O_n$. Ogni oracolo O_i contatta il proprio insieme distinto di fonti di dati che possono o meno sovrapporsi a quelle di altri oracoli. O_i aggrega le risposte dalle sue origini dati e restituisce la propria risposta distinta A_i a una query Req.

Alcuni di questi oracoli potrebbero essere errati. Quindi, chiaramente, l'insieme di tutte le risposte degli oracoli $A_1, A_2, ..., A_n$ dovrà essere aggregato in modo affidabile in un singolo valore autorevole A. Ma data la possibilità di oracoli difettosi, dove e come avverrà questa aggregazione in ChainLink?

Soluzione iniziale: aggregazione in-contract. La soluzione iniziale proposta in ChainLink è stata chiamata *aggregazione in-contract*. CHAINLINK-SC che, ancora una volta, denota la parte sulla catena di ChainLink, aggregherà a sua volta le risposte dell'oracolo. (In alternativa, CHAINLINK-SC può chiamare un altro contratto di aggregazione, ma per semplicità concettuale viene assunto che le due componenti formino un unico contratto.) In altre parole, CHAINLINK-SC calcolerà $A = Agg(A_1, A_2, ..., A_n)$ per qualche funzione Agg (simile a agg, come descritto sopra) e invierà il risultato A a USER-SC. Questo approccio è pratico per n piccoli e presenta diversi vantaggi distinti:

- *Semplicità computazionale*: Nonostante il fatto che l'oracolo sia distribuito, una singola entità, CHAINLINK-SC, esegue l'aggregazione eseguendo Agg.

- *Affidabilità*: Poiché il codice di CHAINLINK-SC può essere ispezionato pubblicamente, è possibile verificarne il corretto comportamento. (CHAINLINK-SC sarà un pezzo di codice relativamente piccolo e semplice.) Inoltre, l'esecuzione di CHAINLINK-SC è completamente visibile on-chain. Così gli utenti, cioè i creatori di USER-SC, possono raggiungere un alto grado di fiducia in CHAINLINK-SC.

- *Flessibilità*: CHAINLINK-SC può implementare le funzioni aggregate *Agg* più desiderate, come la funzione di maggioranza, la media, ecc.

Per quanto semplice, questo approccio presenta una nuova e interessante sfida tecnica, vale a dire il problema del freeloading. Un oracolo imbroglione O_z può osservare la risposta A_i di un altro oracolo O_i e copiarla. In questo modo, l'oracolo O_z evita la spesa di interrogare le fonti di dati, che possono addebitare tariffe per query. Dunque, il freeloading indebolisce la sicurezza minando la diversità delle query sull'origine dei dati e inoltre disincentiva gli oracoli dal rispondere rapidamente: rispondere lentamente combinata con il freeloading è una strategia più economica.

Una soluzione a questo problema corrisponde all'uso di uno schema *commit/reveal*. In un primo round, gli oracoli inviano a CHAINLINK-SC impegni crittografici alle loro risposte. Dopo che CHAINLINK-SC ha ricevuto un quorum di risposte, avvia un secondo round in cui gli oracoli rivelano le loro risposte. In [1] è stato proposto un algoritmo, che mostra un semplice protocollo sequenziale che garantisce la disponibilità data $3f + 1$ nodi. Utilizza uno schema di commit/rivelazione per impedire il freeload. Le risposte degli oracoli vengono disattivate e quindi esposte a un potenziale freeloader solo dopo che tutti gli impegni sono stati presi, escludendo così il freeloader dalla copia di altre risposte degli oracoli. I protocolli on-chain possono sfruttare i tempi di blocco per supportare progetti di protocolli sincroni. In ChainLink, tuttavia, i nodi oracolari ottengono dati da fonti che possono avere tempi di risposta molto variabili e i tempi di disattivazione dei nodi possono variare a causa di, ad esempio, utilizzo di diversi prezzi del gas in Ethereum. Per garantire la reattività del protocollo più veloce possibile, quindi, l'algoritmo proposto è progettato come protocollo asincrono. Il protocollo presuppone canali autenticati tra tutti i giocatori. Inoltre, viene garantito con tale algoritmo che la risposta finale aggregata sarà corretta, se si suppone che i nodi difettosi siano al massimo f. Dati $3f + 1$ nodi in totale, almeno $2f + 1$ invieranno impegni. Di quegli impegni, al massimo f provengono da nodi difettosi, quindi almeno $f + 1$ provengono da nodi onesti. Tutti questi impegni saranno infine disimpegnati. Dei $f + 1$ disimpegni sul singolo valore A, almeno uno deve provenire da un nodo onesto.

L'*aggregazione in-contract* sarà l'approccio principale supportato da ChainLink a breve termine. L'implementazione iniziale proposta comporterà una variante più sofisticata e simultanea dell'algoritmo. La proposta a più lungo termine si riflette nel protocollo OCA (Off-Chain Aggregation) piuttosto complicato. OCA è un protocollo di aggregazione off-chain che riduce al minimo i costi di transazione on-chain. Tale protocollo include anche il pagamento ai nodi oracolari e garantisce contro i pagamenti ai freeloader.

Strategia a medio termine: aggregazione off-chain. L'*aggregazione in-contract* ha uno svantaggio chiave: il costo. Sostiene il costo della trasmissione e dell'elaborazione dei messaggi Oracle sulla catena $O(n)$ (commit e rivelazioni per $A_1, A_2, ..., A_n$). In blockchain permissioned, questo sovraccarico può essere accettabile. Nelle blockchain permissionless con commissioni di transazione on-chain come Ethereum, se n è grande, i costi possono essere proibitivi. Un un approccio più conveniente consiste nell'aggregare le risposte degli oracoli off-chain e trasmettere un singolo messaggio A a CHAINLINK-SC. Questo approccio è chiamato *aggregazione off-chain* e viene proposto nel medio-lungo termine. Il problema di raggiungere un valore di consenso A di fronte a nodi potenzialmente difettosi è molto simile al problema del consenso che è alla base

delle stesse blockchain. Dato un insieme predeterminato di oracoli, si potrebbe considerare l'utilizzo di un algoritmo di consenso classico Byzantine Fault Tolerant (BFT) per calcolare A. I protocolli BFT classici, tuttavia, mirano a garantire che alla fine di un'invocazione di protocollo, tutti i nodi onesti memorizzino lo stesso valore, ovvero che tutti i nodi memorizzano lo stesso nuovo bloccoin una blockchain. In questa impostazione dell'oracolo, l'obiettivo è leggermente diverso. Si vuole assicurare che CHAINLINK-SC (e quindi USER-SC) ottiene la risposta aggregata $A = Agg(A_1, A_2, ..., A_n)$ senza partecipare al protocollo di consenso e senza bisogno di ricevere risposte da più oracoli. Il problema del freeloading, inoltre, deve ancora essere affrontato.

ChainLink propone l'uso di un semplice protocollo che coinvolge le firme di soglia. Tali firme possono essere realizzate utilizzando uno qualsiasi di un certo numero di schemi di firma, ma sono particolarmente semplici da implementare utilizzando le firme di Schnorr. In questo approccio, gli oracoli hanno una chiave pubblica collettiva pk e una corrispondente chiave privata sk condivisa tra $O_1, O_2, ..., O_n$ in modo (t, n)-soglia. Tale condivisione significa che ogni nodo O_i ha una distinta coppia di chiavi privata/pubblica (sk_i, pk_i). O_i può generare una firma parziale $\sigma_i = Sig_{sk_i}[A_i]$ verificabile rispetto a pk_i. La caratteristica chiave di questa configurazione è che le firme parziali sullo stesso valore A possono essere aggregate attraverso qualsiasi insieme di oracoli per produrre un'unica firma collettiva valida $\Sigma = Sig_{sk}[A]$ su una risposta A. Nessun insieme di $t - 1$ oracoli, tuttavia, può produrre una firma valida su qualsiasi valore. La firma singola Σ incorpora quindi implicitamente le firme parziali di almeno t oracoli. Le firme di soglia possono essere realizzate in modo ingenuo lasciando che Σ consista esplicitamente di un insieme di t firme indipendenti valide dai singoli nodi. Le firme di soglia hanno proprietà di sicurezza simili a questo approccio ingenuo, ma forniscono un significativo miglioramento delle prestazioni on-chain: riducono le dimensioni e il costo della verifica di Σ di un fattore di t. Con questa configurazione, sembrerebbe che gli oracoli possano solo generare e trasmettere firme parziali finchè t di tali firme parziali consentono il calcolo di Σ.

Di nuovo, però, si pone il problema del freeloading. Bisogna quindi garantire che gli oracoli ottengano realmente i dati dalle loro fonti designate, piuttosto che barare e copiare A_i da un altro oracolo. La soluzione proposta prevede un meccanismo finanziario: un'entità FORNITORE (realizzabile come smart contract) premia solo gli oracoli che hanno fornito dati originali per le loro firme parziali. In un ambiente distribuito, determinare quali oracoli si qualificano per il pagamento risulta complicato. Gli oracoli possono intercomunicare off-chain e, non essendoci più un'unica entità autorevole (CHAINLINK-SC) che riceve risposte, pertanto non si è più in grado di identificare i beneficiari idonei direttamente tra gli oracoli partecipanti. Di conseguenza, il FORNITORE deve ottenere prove di comportamento scorretto dagli stessi oracoli, alcuni dei quali potrebbero essere inaffidabili. Viene proposto l'uso di meccanismi simili al consenso al fine di garantire che il FORNITORE non paghi gli oracoli che applicano il freeloading. Nello specifico, l'algoritmo proposto fa uso di un protocollo distribuito basato su firme di soglia che fornisce resistenza al freeloading da parte di $f < n/3$ oracoli.

Capitolo 5

Servizi di Sicurezza ChainLink

Grazie ai protocolli descritti nella sezione precedente, ChainLink si propone di garantire disponibilità e correttezza fino al caso in cui ci siano **f** oracoli difettosi. Inoltre, l'hardware fidato viene considerato attivamente come approccio sicuro alla protezione da oracoli corrotti che forniscono risposte errate. L'hardware affidabile, tuttavia, potrebbe non fornire una protezione definitiva per tre motivi. Innanzitutto, non verrà distribuito nelle versioni iniziali della rete ChainLink. In secondo luogo, alcuni utenti potrebbero non fidarsi dell'hardware affidabile. Infine, l'hardware affidabile non può proteggere dai tempi di inattività del nodo, ma solo dal comportamento scorretto del nodo. Gli utenti vorranno quindi assicurarsi di poter scegliere gli oracoli più affidabili e ridurre al minimo la probabilità che USER-SC faccia affidamento su oltre f oracoli difettosi. A tal fine, è stato proposto l'utilizzo di quattro servizi di sicurezza chiave: un sistema di convalida, un sistema di reputazione, un servizio di certificazione e un servizio di aggiornamento del contratto. I primi tre servizi forniscono solo valutazioni o indicazioni agli utenti, mentre il servizio di aggiornamento dei contratti è del tutto facoltativo per gli utenti. Tutti questi servizi possono inizialmente essere gestiti da un'azienda o da un gruppo interessato a lanciare la rete ChainLink, ma sono progettati per operare rigorosamente in conformità con gli obiettivi di ChainLink. Inoltre, essi non possono bloccare la partecipazione dei nodi oracolo o alterarne le risposte.

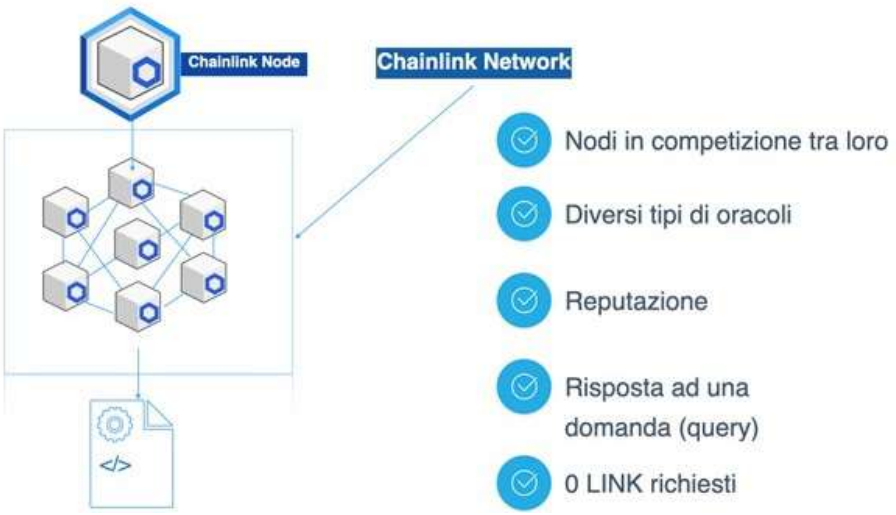


Figura 5.1. Come Chainlink garantisce la sicurezza

5.1 Sistema di Validazione

Il sistema di convalida ChainLink monitora il comportamento degli oracoli sulla catena, fornendo una metrica oggettiva delle prestazioni che può guidare la selezione degli oracoli da parte dell'utente. Cercherà di monitorare gli oracoli per:

- *Disponibilità*: Il sistema di convalida dovrebbe registrare gli errori di un oracolo per rispondere in modo tempestivo alle domande. Compila statistiche di uptime in corso.
- *Correttezza*: Il sistema di convalida dovrebbe registrare risposte errate apparenti da parte di un oracolo misurate in base alle deviazioni dalle risposte fornite dai colleghi.

Nel sistema iniziale di aggregazione on-chain in ChainLink, tale monitoraggio è semplice, poiché tutta l'attività dell'oracolo è visibile a CHAINLINK-SC. Tuttavia, nel sistema di aggregazione off-chain previsto per ChainLink, sono gli oracoli stessi che eseguono l'aggregazione. Di conseguenza, CHAINLINK-SC non ha visibilità diretta sulle risposte degli oracoli e non può monitorare la disponibilità e la correttezza. Fortunatamente, gli oracoli firmano digitalmente le loro risposte e quindi, come effetto collaterale, generano prove non ripudiabili delle loro risposte. L'approccio proposto sarà quindi quello di realizzare il servizio di convalida come un contratto intelligente che premierebbe gli oracoli per la presentazione di prove di risposte divergenti. In altre parole, gli oracoli sarebbero incentivati a segnalare comportamenti apparentemente errati. La disponibilità è in qualche modo più complicata da monitorare, poiché gli oracoli ovviamente non firmano mancate risposte. Invece, un miglioramento del protocollo proposto richiederebbe agli oracoli di firmare digitalmente le attestazioni per l'insieme di risposte che hanno ricevuto da altri oracoli. Il contratto di convalida accetterebbe quindi (e ricompenserebbe nuovamente) l'invio di insiemi di attestazioni che dimostrano una costante non reattività da parte di un oracolo con prestazioni insufficienti nei confronti dei suoi pari. In entrambi i casi on-chain e off-chain, le statistiche di disponibilità e correttezza per gli oracoli saranno visibili sulla catena. Gli utenti/sviluppatori potranno così visualizzarli in tempo reale attraverso un front end appropriato, come una Dapp in Ethereum o un'applicazione equivalente per una blockchain permissioned.

5.2 Sistema di Reputazione

Il sistema di reputazione proposto per ChainLink registrerebbe e pubblicherebbe le valutazioni degli utenti di provider e nodi Oracle, offrendo agli utenti un mezzo per valutare le prestazioni di Oracle olistico. È probabile che i rapporti del sistema di convalida siano un fattore importante nella determinazione delle reputazioni oracolari e che ponngano queste reputazioni su una solida base di fiducia. Fattori al di là della cronologia on-chain, tuttavia, possono fornire informazioni essenziali sui profili di sicurezza del nodo oracolo. Questi possono includere la familiarità degli utenti con i marchi degli oracoli, entità operative e architetture. Viene previsto che il sistema di reputazione ChainLink includa un componente on-chain di base in cui le valutazioni degli utenti sarebbero disponibili per altri smart contracts a cui fare riferimento. Inoltre, le metriche sulla reputazione dovrebbero essere facilmente accessibili off-chain, dove è possibile elaborare in modo efficiente e più flessibile grandi quantità di dati.
Per un dato operatore Oracle, il sistema di reputazione viene inizialmente proposto per supportare le seguenti metriche:

- *Numero totale di richieste assegnate*: Il numero totale di richieste passate accettate da un oracolo, sia soddisfatte che non soddisfatte.

- *Numero totale di richieste completate*: Il numero totale di richieste passate soddisfatte da un oracolo. Questo può essere calcolato in media sul numero di richieste assegnate per calcolare il tasso di completamento.
- *Numero totale di richieste accettate*: Il numero totale di richieste che sono state ritenute accettabili calcolando i contratti rispetto alle risposte dei pari. Questo può essere calcolato in media rispetto al totale delle richieste assegnate o completate da ottenere comprensione dei tassi di accuratezza.
- *Tempo medio di risposta*: Sebbene possa essere necessario dare alle risposte dell'oracolo il tempo per la conferma, la tempestività delle loro risposte sarà utile per determinare la tempestività futura. Il tempo medio di risposta viene calcolato in base al completamento richieste.
- *Importo delle penalità*: Se i pagamenti di penalità fossero bloccati per garantire le prestazioni di un operatore di nodo, il risultato sarebbe una metrica finanziaria dell'impegno di un fornitore di oracoli a non impegnarsi in un attacco "exit scam", in cui il fornitore prende i soldi degli utenti e non fornisce servizi. Questa metrica lo farebbe coinvolgere sia una dimensione temporale che finanziaria.

I servizi di alta reputazione sono fortemente incentivati in qualsiasi mercato a comportarsi correttamente e garantire disponibilità e prestazioni elevate. Il feedback negativo degli utenti rappresenterà un rischio significativo per il valore del marchio, così come le sanzioni associate al comportamento scorretto. Di conseguenza, si prevede un circolo virtuoso in cui oracoli ben funzionanti sviluppano una buona reputazione e una buona reputazione genera incentivi per continuare a ottenere alte prestazioni.

5.3 Servizio di certificazione

Mentre i sistemi di convalida e reputazione hanno lo scopo di affrontare un'ampia gamma di comportamenti errati da parte degli oracoli e sono proposti come un modo per garantire l'integrità del sistema nella stragrande maggioranza dei casi, ChainLink può includere anche un meccanismo aggiuntivo chiamato servizio di certificazione. Il suo obiettivo è prevenire e/o rimediare a eventi rari ma catastrofici, in particolare imbrogli in blocco sotto forma di attacchi Sybil e di mirroring.

In particolare, il servizio di certificazione ChainLink cerca di fornire una garanzia generale di integrità e disponibilità, rilevando e aiutando a prevenire mirroring e colludendo i quorum degli oracoli nel breve e medio termine. Il servizio di certificazione rilascia approvazioni di fornitori di oracoli di alta qualità. Come notato sopra, il servizio valuta solo i fornitori a vantaggio degli utenti; non ha lo scopo di dettare la partecipazione o la non partecipazione del nodo oracolo al sistema.

5.4 Servizio di aggiornamento dei contratti

La codifica di smart contracts a prova di bomba è un'attività molto complessa e richiede un'attenta pianificazione e attenzione ai dettagli. Tuttavia, anche se un contratto intelligente è stato programmato in modo corretto, cambiamenti ambientali o errori di codifica possono ancora causare vulnerabilità. Per mitigare questi rischi, si propone un servizio di aggiornamento dei contratti opzionale e sotto il controllo degli utenti. Il Contract-Upgrade Service è stato sviluppato per fornire un ulteriore livello di sicurezza e affidabilità agli smart contract basati sulla tecnologia ChainLink.

In caso di scoperta di vulnerabilità, il Contract-Upgrade Service rende disponibile un nuovo set di contratti oracolo di supporto, che gli smart contract richiedenti appena creati potrebbero migrare. Ciò garantiresce che gli smart contract continuino a funzionare in modo affidabile e sicuro, anche in presenza di cambiamenti ambientali o di altri fattori che potrebbero influenzare il loro funzionamento. Tuttavia, l'uso del Contract-Upgrade Service è completamente facoltativo e sotto il controllo degli utenti. Gli utenti possono scegliere di utilizzare il servizio o di continuare a utilizzare i loro contratti originali, se lo desiderano. Inoltre, il servizio viene fornito con una serie di controlli e bilanciamenti per garantire la massima sicurezza possibile, tra cui l'audit indipendente dei nuovi contratti oracolo e l'utilizzo di meccanismi di incentivazione per premiare gli sviluppatori per l'aderenza alle linee guida stabiliti.

5.5 Utilizzo del token LINK

La rete ChainLink utilizza il token LINK per pagare gli operatori del nodo ChainLink per il recupero di dati da feed di dati off-chain, la formattazione dei dati in formati leggibili da blockchain, il calcolo off-chain e le garanzie di uptime che forniscono come operatori. Affinché uno smart contract su reti come Ethereum utilizzi un nodo ChainLink, dovrà pagare l'operatore del nodo ChainLink scelto utilizzando i token LINK, con i prezzi fissati dall'operatore del nodo in base alla domanda per la risorsa off-chain fornita da ChainLink e la fornitura di altre risorse simili. Il token LINK è un token ERC20, con la funzionalità aggiuntiva di "transfer and call" ERC223 di trasferimento (indirizzo, uint256, byte), che consente ai token di essere ricevuti ed elaborati dai contratti all'interno di una singola transazione.

Capitolo 6

Off-Chain Reporting

Il protocollo di Off-Chain Reporting (OCR) presentato in [3] rappresenta un miglioramento della decentralizzazione e della scalabilità delle reti Chainlink. Come presentato in precedenza, periodicamente, viene effettuata off-chain l'aggregazione delle risposte di una rete di oracoli in un unico report, utilizzando l'OCR, e trasmesso quest'ultimo a uno smart contract nella blockchain. Il contratto verifica la validità del report, paga ogni oracolo che ha contribuito con un'osservazione alla redazione del report e pubblica la mediana dei valori riportati ai contratti di consumo sulla catena. Questo comporta una maggiore efficienza dei costi, in quanto viene trasmessa una singola transazione aggregata con un notevole risparmio di gas, ma anche comitati più ampi di nodi (maggiore scalabilità) e una maggiore affidabilità durante i periodi di estrema congestione della rete blockchain. Ne consegue una maggiore decentralizzazione delle reti di oracoli, maggiore accuratezza, disponibilità e antimanomissione per gli utenti di Chainlink e una riduzione del carico di lavoro on-chain. Viene utilizzata una rete peer-to-peer sicura per la comunicazione tra i vari nodi *aggregators* e un algoritmo di consenso alleggerito in cui ogni nodo riporta la propria osservazione dei dati e la firma. Queste firme sono poi verificate nella catena.

Ciò che si vuole raggiungere con questo protocollo è resilienza a diversi tipi di fallimento, semplicità, basse tasse per le transazioni e una bassa latenza, ovvero si vuole ridurre al minimo il tempo che intercorre tra l'avvio del protocollo di firma e l'inclusione della transazione risultante nella blockchain da parte dello smart contract, in modo da avere dati aggiornati e più precisi, condizione fondamentale ad esempio per quelle applicazioni degli smart contract più sensibili ai piccoli movimenti di prezzo.
Il modo in cui il protocollo funziona è il seguente e si ripete per ogni *epoca*:

1. I nodi eleggono un nuovo nodo leader che guida il resto del protocollo per quella determinata epoca.

2. Ogni oracolo fa partire un timer di durata massima in cui il leader deve produrre un report valido da inviare. In tal modo vengono controllate le performance del leader. Se tale nodo non riesce a concludere il suo lavoro entro il tempo stabilito, inizia una nuova epoca con un leader diverso.

3. Una volta eletto, il leader chiede ai nodi di fornire osservazioni aggiornate e firmate che aggrega in un rapporto. Questo report viene inviato ai follower per verificarne la validità. Se il leader riceve una copia firmata del report da un quorum di nodi, allora tale rapporto è stato approvato. Di conseguenza, il leader assembla un report finale con le firme del quorum e lo trasmette a tutti i follower.

4. I nodi cercano di trasmettere il rapporto finale all'*aggregation contract* secondo un programma randomizzato. L'aggregatore verifica che un quorum di nodi abbia firmato il report ed

espone il valore mediano ai consumatori come risposta, insieme a un timestamp del blocco e un ID del round.

5. Tutti i nodi controllano la blockchain per il report finale al fine di eliminare qualsiasi possibile punto di errore durante la trasmissione. Nel caso in cui il nodo designato non riesca a confermare la sua trasmissione entro un determinato periodo di tempo, entra in funzione un protocollo che consente agli altri nodi di trasmettere il report finale finché uno di essi non viene confermato.

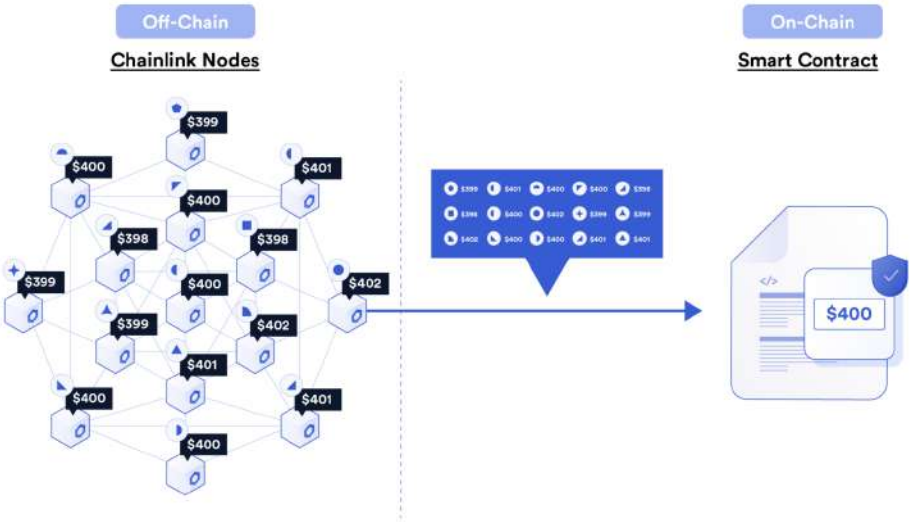


Figura 6.1. Chainlink off-chain reporting

Grazie all'introduzione dell'OCR, si è verificato un notevole aumento della quantità di dati del mondo reale disponibili per le applicazioni degli smart contracts. Ciò comporta un'ulteriore innovazione in molti settori, come la DeFi, le assicurazioni decentralizzate e i giochi basati su blockchain. Gli sviluppatori di contratti intelligenti potranno utilizzare queste nuove fonti di dati per creare una vasta gamma di prodotti e mercati finanziari. Ad esempio, in ambito DeFi è possibile aumentare sicurezza e affidabilità grazie a una maggiore precisione della valutazione del rischio. Le assicurazioni decentralizzate possono anch'esse beneficiare di tale precisione della valutazione del rischio al fine di offrire polizze personalizzate. Mentre i giochi basati su blockchain possono utilizzare i dati del mondo reale per creare esperienze di gioco più realistiche e coinvolgenti, come ad esempio giochi di ruolo basati sulla posizione geografica o giochi di simulazione basati sulle condizioni meteorologiche in tempo reale.

Capitolo 7

Conclusione

Riassumendo, in questa tesina è stata introdotta ChainLink, una rete di oracoli decentralizzata per gli smart contracts, la quale permette di interagire in modo sicuro con risorse esterne alla blockchain.
In particolare, è stata inizialmente delineata l'architettura di ChainLink, descrivendo sia i componenti on-chain che off-chain. Dopo aver definito la sicurezza nell'ambito degli oracoli, è stato prima presentato l'approccio a più livelli (multistrato) di ChainLink alla decentralizzazione ed in seguito è stato proposto un nuovo protocollo con nuove funzionalità come la protezione, con alcuni protocolli aggiuntivi, contro il freeloading. Oltre a tali protocolli, è stato citato come ChainLink può sfruttare i progressi tecnologici e infrastrutturali per migliorare la qualità dei dati forniti alle reti blockchain, ovvero utilizzando hardware affidabili e la firma digitale dei dati da parte delle fonti. Infine, è stato descritto il funzionamento dell'off-chain reporting, che ha comportato il vantaggio di ridurre il carico sulla blockchain e migliorare l'efficienza e la scalabilità.

I principi fondamentali che guidano lo sviluppo di ChainLink sono i seguenti:

- **Decentralizzazione per sistemi aperti e sicuri**. Il decentramento non è solo il fondamento delle proprietà a prova di manomissione delle blockchain, ma anche la base della loro natura senza autorizzazione. Continuando a creare sistemi decentralizzati, l'obiettivo a cui si mira è quello di consentire ulteriormente lo sviluppo senza autorizzazione all'interno dell'ecosistema. La decentralizzazione è infatti una componente cruciale per un ecosistema prospero a livello globale con sostenibilità a lungo termine.

- **Modularità per un design di sistema semplice e flessibile**. È possibile ragionare facilmente su componenti semplici e quindi combinarli in modo sicuro in sistemi più grandi. La modularità consente l'aggiornamento dei sistemi e facilita anche il decentramento. La piattaforma Chainlink si impegna a garantire che non ci sia una dipendenza eccessiva da un numero limitato di soggetti e che sia possibile utilizzare diverse implementazioni concorrenti della tecnologia.

- **Open source per sistemi estensibili e sicuri**. ChainLink è reso possibile grazie al supporto di molti progetti open source. Inoltre, la piattaforma si impegna a collaborare costantemente con sviluppatori, accademici ed esperti di sicurezza per garantire solidità e sicurezza. La piattaforma incoraggia test, audit e prove formali di sicurezza per garantire che Chainlink sia sempre all'avanguardia e in grado di soddisfare le esigenze in continua evoluzione del settore blockchain.

Forti di questi principi, gli sviluppatori di Chainlink cercano dunque di estendere la portata e l'impatto delle blockchain e degli smart contracts, rendendo gli oracoli un porto sicuro dell'ecosistema delle criptovalute.

Bibliografia

[1] S. Ellis, A. Juelsy, S. Nazarov, *ChainLink: A Decentralized Oracle Network*, September 4, 2017, [Online] https://link.smartcontract.com/whitepaper

[2] H. Al-Breiki, M. Habib Ur Rehman, K. Salah, D. Svetinovic, *Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges*, May 19, 2020, [Online] https://www.researchgate.net/publication/

[3] *Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks*, April 15, 2021, [Online] https://research.chain.link/whitepaper-v2.pdf

[4] *Cos'è Chainlink (LINK) e come funziona*, [Online] https://cryptofacili.com/chainlink/

[5] *Chainlink: cos'è e come funziona, LINK crypto*, [Online] https://www.webeconomia.it/chainlink/#Il_Token_LINK

[6] *Chainlink: Guida definitiva su LINK Coin*, [Online] https://www.criptovaluta.it/chainlink

[7] *Basic Request Model*, [Online] https://docs.chain.link/architecture-overview/architecture-request-model/

[8] *What Is a Chainlink Node Operator?*, [Online] https://blog.chain.link/what-is-a-chainlink-node-operator

[9] *External Adapters Introduction*, [Online] https://docs.chain.link/architecture-overview/off-chain-reporting?parent=gettingStarted

[10] *Off-Chain Reporting*, [Online] https://docs.chain.link/chainlink-nodes/external-adapters/external-adapters

[11] *Chainlink Achieves Major Scalability Upgrade With Mainnet Launch of Off-Chain Reporting (OCR)*, [Online] https://blog.chain.link/off-chain-reporting-live-on-mainnet/

[12] *Video introduttivo 1: Parliamo di Chainlink (LINK): che cos'é e come funziona* https://www.youtube.com/watch?v=T8tmn3t6c5g&ab_channel=cripto51

[13] *Video introduttivo 2: Chainlink (LINK): un progetto crypto utile che devi conoscere* https://www.youtube.com/watch?v=OrLsRfHoUmw

[14] *Video introduttivo 3: Chainlink (LINK) spiegato in maniera semplice (a cosa serve, tokenomics)* https://www.youtube.com/watch?v=uTJPXcBlVaQ

INTRODUZIONE E FUNZIONAMENTO DI RGB

Gianluca Cappiello, Matilde Carnevale, Nadia Giolito, Salvatore Scorsone

POLITECNICO DI TORINO

Blockchain e Criptoeconomia

Introduzione e funzionamento di RGB

Gianluca Cappiello s304649, Matilde Carnevale s317049,
Nadia Giolito s316121, Salvatore Scorsone s294854

Contents

1 Introduzione **2**
1.1 Tokenizzazione: perché RGB? 2
1.2 Alla scoperta di RGB 4

2 Funzionamento di RGB **6**
2.1 Sigilli monouso 6
2.2 Contratti RGB e transizioni di stato 6
2.3 Trasferimenti off-chain 7
2.3.1 Validazione lato client 9
2.3.2 Commitment su Bitcoin 10
2.3.3 Batching 12
2.4 Privacy 12
2.5 Comunicazione client-to-client 13

3 Compatibilità con LN **14**
3.1 Vantaggi 14
3.2 Commitment su LN 14

4 Conclusioni **19**

Chapter 1

Introduzione

Il concetto di *smart contract* è precedente all'invenzione della blockchain e dello stesso Bitcoin: la sua prima menzione si trova in un articolo del 1994 di Nick Szabo, che definiva gli smart contract come un "*protocollo di transazione computerizzato che esegue i termini di un contratto*", anche se il termine è stato reso popolare solo in seguito dai promotori di Ethereum, che hanno stravolto la definizione originale come "codice che viene eseguito in modo ridondante da tutti i nodi in una rete di consenso globale".
Se da un lato delegare l'esecuzione del codice a una rete di consenso globale presenta dei vantaggi, dall'altro questo design ha un grande difetto: la mancanza di scalabilità (e di privacy). Se ogni nodo di una rete deve eseguire in modo ridondante lo stesso codice, la quantità di codice che può essere effettivamente eseguita senza aumentare eccessivamente il costo di gestione di un nodo (e quindi preservare la decentralizzazione) rimane scarsa, il che significa che solo un piccolo numero di contratti può essere eseguito.
Ma cosa succederebbe se potessimo progettare un sistema in cui i termini del contratto sono eseguiti e convalidati solo dalle parti coinvolte, anziché da tutti i membri della rete?
Nell'ultimo decennio il lavoro congiunto di diversi ricercatori ha portato nuove basi che possono essere utilizzate per raggiungere l'obiettivo. Tra questi spiccano i concetti di *client-side validation* e di *sigilli monouso* di Peter Todd e le "colored coin" con la convalida client-side di Giacomo Zucco, in grado di operare come strato scalabile in cima a Bitcoin e alla rete Lightning.

1.1 Tokenizzazione: perché RGB?

Di recente è cresciuto l'interesse per i token su Bitcoin e Lightning Network. L'idea di creare token che rappresentino beni che possono essere trasferiti e conservati con la stessa sicurezza e convenienza che il protocollo Bitcoin offre non è nuova, anzi è stata pionieristicamente introdotta già nel 2013 da protocolli come Counterparty ed OmniLayer (ex Mastercoin), e successivamente adottata da Ethereum e altre altcoin, dove si svolge la maggior parte dell'attività dei token blockchain.
Tuttavia, l'uso delle altcoin per proteggere gli asset finanziari non è ideale, poiché non sono in grado di offrire lo stesso livello di sicurezza e decentralizzazione di Bitcoin. Per questo motivo, nel corso degli anni sono emersi alcuni progetti che cercano di modernizzare i protocolli dei *token-on-Bitcoin* e di renderli compatibili con Lightning Network, in particolare questo elaborato si concentrerà su **RGB** (**Red-Green-Blue**), con l'obiettivo di fornire una panoramica completa del suo funziona-

mento e della sua proposta di valore.

La *tokenizzazione* degli asset è diventata un importante strumento per rappresentare e scambiare valori digitali sulla blockchain: è il processo di trasformare un asset in un token digitale su una blockchain, consentendone lo scambio, il trasferimento e l'utilizzo in modo sicuro e trasparente. I token possono essere fungibili, che sono intercambiabili tra loro, o non fungibili (NFT), che rappresentano oggetti digitali unici.
La tokenizzazione offre diversi vantaggi:

- la rappresentazione di asset tradizionalmente illiquidi (oltre a quelli digitali nativi della blockchain), come proprietà immobiliari o opere d'arte, sotto forma di token digitali, facilitandone lo scambio e la divisione in frazioni più piccole;
- favorisce la trasparenza e la tracciabilità, poiché le transazioni avvengono sulla blockchain ed è possibile seguire il flusso di proprietà e verificare la provenienza e la storia dei token;
- semplifica e automatizza processi complessi utilizzando smart contracts, eliminando la necessità di intermediari tradizionali e riducendo i costi operativi.

Tuttavia, la tokenizzazione presenta anche sfide da affrontare, come la standardizzazione dei protocolli, la sicurezza, l'interoperabilità tra diverse blockchain e la conformità alle normative legali e regolamentari. La scelta del protocollo di tokenizzazione e la gestione dei token richiedono quindi una valutazione attenta delle esigenze specifiche del progetto e una comprensione dei rischi e delle opportunità associati.
Esistono diversi protocolli di tokenizzazione, ognuno dei quali ha le sue caratteristiche uniche e può variare in termini di efficienza, scalabilità e funzionalità. Di seguito sono elencati alcuni esempi:

1. **ERC-20 su Ethereum**: L'ERC-20 è uno standard di tokenizzazione utilizzato sulla blockchain di Ethereum. Mentre è stato ampiamente adottato e ha alimentato il boom dei token ICO (Initial Coin Offering), può essere soggetto a problemi di scalabilità a causa della congestione della rete Ethereum durante periodi di elevata attività.
2. **Omni Layer su Bitcoin**: L'Omni Layer è un protocollo di tokenizzazione costruito sopra la blockchain di Bitcoin. Tuttavia, a differenza del protocollo RGB, richiede la creazione di transazioni aggiuntive sulla blockchain di Bitcoin per gestire i token, il che può avere un impatto sulla scalabilità e l'efficienza complessiva.
3. **EOS Token Standard**: EOS è una piattaforma blockchain che supporta la creazione di token. Anche se offre funzionalità avanzate come il consenso delegato e l'elaborazione dei contratti intelligenti, la sua architettura decentralizzata potrebbe avere limitazioni in termini di scalabilità e prestazioni.
4. **TRC-20 su TRON**: TRC-20 è uno standard di tokenizzazione utilizzato sulla blockchain di TRON. Mentre TRON ha una latenza inferiore e tariffe di transazione più basse rispetto ad Ethereum, potrebbe ancora avere problemi di scalabilità a causa del suo protocollo di consenso delegato.

È importante notare che le prestazioni di un protocollo possono essere influenzate da vari fattori, tra cui la dimensione della rete, il carico di lavoro e la progettazione del protocollo stesso. La scelta del protocollo di tokenizzazione dipenderà dalle esigenze specifiche dell'applicazione e dal bilanciamento tra performance, sicurezza e funzionalità desiderate.

In questo contesto, il protocollo RGB su Bitcoin si rivela una soluzione innovativa e promettente.

1.2 Alla scoperta di RGB

Il protocollo RGB è stato sviluppato per consentire la creazione, la gestione e lo scambio di token digitali sulla blockchain di Bitcoin. Sfruttando la solida infrastruttura di Bitcoin, offre un approccio decentralizzato e sicuro per la tokenizzazione di una vasta gamma di asset digitali.
L'obiettivo principale del protocollo è migliorare la fungibilità sulla blockchain di Bitcoin, consentendo la rappresentazione di asset digitali diversi come token standardizzati e permettendo agli utenti di scambiare i token senza preoccuparsi della loro storia o provenienza, creando quindi un ambiente di scambio efficiente.

Il processo di creazione dei token utilizzando il protocollo RGB è flessibile e personalizzabile: gli utenti possono specificare le caratteristiche del token, come il nome, la descrizione e altre proprietà personalizzate. Inoltre, i *token RGB* possono includere metadati che forniscono ulteriori informazioni sull'asset rappresentato, aumentandone trasparenza e tracciabilità.
In realtà RGB viene anche definito come un *sistema di smart contracts* scalabili e riservati per Bitcoin e Lightning Network. Infatti, non è solamente un protocollo per emettere token: sebbene l'emissione e la gestione di beni altamente scalabili, programmabili e privati di vario tipo siano possibili con RGB, esso può essere applicato in molti settori oltre a quello finanziario.
Fondamentalmente RGB è una piattaforma decentralizzata di *notarizzazione di contratti tra peers*.

Il protocollo abbraccia il modello di *client-side validation*, che consiste nel mantenere tutti i dati specifici della transazione fuori dalla catena, farli scambiare solo tra il mittente e il destinatario della transazione ed utilizzare la blockchain di Bitcoin solo come *sigillo*. La blockchain Bitcoin viene utilizzata come livello di impegno dello stato, mentre l'evoluzione dello smart contract è definita da uno schema al di fuori della catena. Ciò offre vantaggi in termini di scalabilità, privacy ed estensibilità rispetto ad altri protocolli che mantengono tutte le informazioni sulla catena.
Un altro aspetto importante del protocollo è la sua interoperabilità: i token RGB possono essere scambiati e utilizzati su diverse piattaforme blockchain compatibili, consentendo l'integrazione e l'interazione con altri ecosistemi digitali.
I casi d'uso più immediati di RGB sono l'emissione di beni fungibili e collezionabili, ma il protocollo è sufficientemente generalizzato per supportare anche altri casi d'uso, come le identità decentralizzate, il DNS decentralizzato e la proof-of-publication.
Come sistema di smart contract, RGB è molto diverso dagli approcci precedenti, sia basati su Bitcoin (Colored coins, Counterparty, OMNI) sia basati su altri ecosistemi (Ethereum, EOS e altri):

- RGB separa il concetto di emittente dello smart contract, di proprietario dello stato e di evoluzione dello stato.
- RGB mantiene il codice e i dati dello smart contract fuori dalla catena
- RGB utilizza la blockchain come livello di impegno dello stato e lo script Bitcoin come sistema di controllo della proprietà, mentre l'evoluzione dello smart contract è definita da uno schema fuori dalla catena.

Il sistema di smart contract proposto da RGB è stato progettato secondo i seguenti criteri:

- **Scalabilità, ottenuta a più livelli**: capacità di scalare in termini di dimensione dei dati grazie alle client-side validation; capacità di scalare in termini di throughput delle transazioni grazie alla compatibilità con la rete lightning.
- **Forte proprietà**: lo smart contract opera in "stati di proprietà" che hanno un proprietario ben definito. Nessuno, tranne questo proprietario, può aggiornare lo stato del contratto. I contratti definiscono sempre i tipi di diritti come un insieme di operazioni che possono essere eseguite sul contratto e questi diritti sono assegnati come "pubblici" o "di proprietà", utilizzando una logica di validazione specifica.
- **Riservatezza**: i dati devono essere noti solo ai partecipanti al contratto, cioè ai proprietari degli stati, a meno che non decidano di renderli pubblici. Tutte le parti del protocollo devono essere protette da strumenti come l'analisi della catena e il protocollo non deve memorizzare alcuna informazione in blockchain.
- **Separazione dei compiti**: i protocolli devono essere progettati in modo modulare e stratificato, dove ogni modulo risolve uno e un solo compito. I livelli devono essere ben astratti, il che significa che i livelli sottostanti non devono essere a conoscenza della struttura dei livelli superiori. Questa separazione dei compiti fornisce una base per l'interoperabilità del protocollo, la sicurezza, la componibilità e la compatibilità futura.
- **Estensibilità**: deve essere possibile creare forme avanzate di smart contract senza dover modificare il nucleo del protocollo o aggiungere codice e ricompilare le librerie RGB.
- **Determinismo**: la logica di validazione di RGB deve essere deterministica, nel senso che, dato l'insieme di input forniti e lo stato del livello di impegno (blockchain o lightning channel), produce sempre lo stesso risultato, indipendentemente dalla piattaforma utilizzata o dalle librerie collegate.
- **Interoperabilità LNP/BP**: RGB deve funzionare bene con tutte le tecnologie bitcoin e lightning esistenti ed essere compatibile con eventuali aggiornamenti futuri.

Il protocollo RGB su Bitcoin rappresenta un importante passo avanti nell'ambito della tokenizzazione e della fungibilità sulla blockchain. La sua capacità di creare e gestire token digitali su Bitcoin offre nuove opportunità per la rappresentazione di asset e l'interazione con il mondo decentralizzato.
Esplorare il potenziale di questo protocollo ci consente di comprendere meglio come l'innovazione continua a trasformare il modo in cui gestiamo e scambiamo valore digitale.

Chapter 2

Funzionamento di RGB

2.1 Sigilli monouso

L'idea dei sigilli digitali monouso è comparabile con l'idea delle fascette monouso di plastica numerate utilizzate per rilevare tentativi di manomissione e apertura dei container durante il trasporto di beni.

Figure 2.1: Fascette monouso

Allo stesso modo, i sigilli digitali monouso sono usati per garantire che un messaggio venga utilizzato una sola volta. Se il messaggio certifica il possesso di un token, applicando il sigillo monouso, non è possibile mostrarlo a più persone ed effettuare un double-spending.
Il protocollo RGB sfrutta gli UTXO (Unspent Transaction Outputs, ovvero gli output delle transazioni di Bitcoin ancora non spesi) come sigilli.
Il protocollo di Bitcoin prevede che, quando si vuole effettuare un pagamento, l'UTXO venga completamente svuotato e che non sia possibile eseguire questa operazione due volte. Quindi, un UTXO può essere visto come un sigillo che viene chiuso quando viene creato e aperto quando viene speso.

2.2 Contratti RGB e transizioni di stato

Con RGB è possibile creare uno smart contract la cui struttura dati definisce:

- i diritti associati al contratto (es. diritto di spostare un asset)
- la proprietà dei diritti di uno o più UTXO

- le regole di trasferimento di tali diritti ad altri UTXO
- i metadati del contratto (ad esempio il nome dell'asset)

Il contratto può essere creato a partire da un modello, chiamato "schema", in cui il creatore del contratto si limita a modificare i parametri e i diritti di proprietà, come avviene nei contratti legali tradizionali.
Il contratto appena creato viene detto *contratto Genesi*, in cui è definito il primo proprietario di ciascun diritto disponibile.

Alcuni esempi di schema RGB sono:

- RGB20 emissione di asset fungibili.
- RGB21 emissione di collectible asset.
- RGB22 identità digitali decentralizzate.
- RGB23 registro cronologico univoco verificabile per dati.
- RGB24 domain name system decentralizzato.

Chiunque è libero di sviluppare il proprio schema senza dover chiedere il permesso agli sviluppatori RGB, tuttavia gli schemi indicati sopra coprono la maggior parte dei casi d'uso.

Quando si verifica una transazione RGB, il mittente crea una *state transition* del contratto, che definisce quale nuovo UTXO sarà proprietario dei diritti trasferiti e/o eventuali modifiche su alcune caratteristiche del token (metadati).
A differenza di altri sistemi di smart contract, le regole con cui avvengono le transazioni sono definite esclusivamente nel contratto di genesi e non possono essere modificate dai successivi proprietari. Questa caratteristica differisce da Bitcoin, in cui chiunque può bloccare i propri bitcoin all'interno di uno script personalizzato. L'approccio di RGB aiuta a mantenere i costi di validazione e la complessità più bassi.

2.3 Trasferimenti off-chain

Il progetto RGB ha lo scopo di migliorare il design della blockchain attraverso una soluzione più scalabile, più rispettosa della privacy e più adatta al futuro. L'idea di base è di utilizzare la blockchain di Bitcoin solo per ciò che è strettamente necessario, ovvero per la protezione dal double spending e per il decentramento della rete, sfruttando il protocollo di consenso proof-of-work. Tutto il lavoro di convalida del trasferimento dei token viene invece effettuato off-chain, delegando questa responsabilità al client che riceve il pagamento.

Esaminiamo più nel dettaglio come avviene una transazione RGB. Per rendere più chiara la trattazione specifichiamo la distinzione tra

- transazione Bitcoin: transazione on-chain utilizzata per il solo trasferimento di bitcoin UTXO
- transazione RGB: transazione off-chain utilizzata per l'effettivo trasferimento del contratto.

Come è già stato detto, per spostare i diritti di proprietà di un asset, è necessario

1. effettuare la transazione Bitcoin spendendo l'UTXO controllato dalla stessa persona che possiede la proprietà in questione

2. inserire all'interno della transazione Bitcoin sia l'output (uno o più) della transazione Bitcoin, sia l'informazione sull'indirizzo UTXO controllato dal nuovo proprietario dell'asset. Questi due indirizzi non devono per forza coincidere.

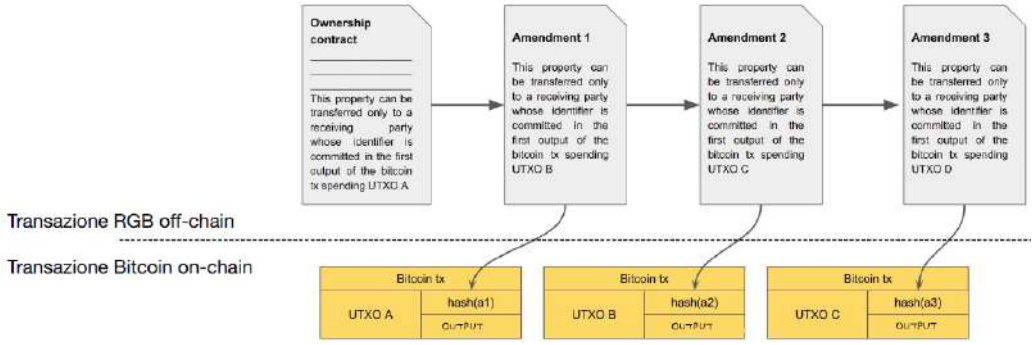


Figure 2.2: Transazioni on-chain e off-chain

Utilizzando soltanto il protocollo Bitcoin, sarebbe necessario codificare tutte le informazioni sul nuovo proprietario direttamente all'interno della transazione Bitcoin. Tuttavia, questo è un approccio limitante dal momento che vi sono vincoli sulla dimensione delle transazioni. Inoltre, ció potrebbe compromettere la privacy delle parti coinvolte.
Pertanto, un approccio migliore consiste nell'aggiungere alla transazione Bitcoin solo un commit crittografico che rappresenta il destinatario. Ad esempio, potremmo includere l'hash del contratto aggiornato (Figura 2.7). In questo modo, ogni volta che la proprietà viene trasferita, viene effettivamente creato un emendamento al contratto originale che specifica quale nuovo UTXO Bitcoin detiene ora il controllo sulla proprietà.

La trasmissione off-chain dei contratti avviene attraverso un canale di comunicazione diretto crittografato peer-to-peer, tra il pagatore e il destinatario. È quest'ultimo a verificare che le regole del protocollo RGB siano state rispettate. Approfondiremo successivamente questo aspetto.

Si noti che le transazioni Bitcoin in Figura 2.2 non sono collegate tra loro. È come se la proprietà venisse "teletrasportata" da un UTXO all'altro senza lasciare traccia nel grafo delle transazioni Bitcoin. Ciò significa che un osservatore blockchain non può estrarre informazioni sull'attività degli utenti RGB.

Al fine di riassumere quanto spiegato, proponiamo l'esempio mostrato in Figura 2.7.
Alice dispone di token assegnati all'output 1 e vuole mandarli a Carl. Per spostarli deve effettuare una transazione on-chain "Bitcoin TX A" per spendere i suoi UTXO, sia una transazione RGB off-chain "RGB TX M" in cui invia la proprietà dei token ad un altro indirizzo UTXO "Bitcoin TX C: output 2" di proprietà di Carl. Come si vede dalla figura, la transazione RGB non lascia

traccia all'interno della blockchain. Nella maggior parte dei casi, possiamo aspettarci che Alice usi la transazione on-chain solo per provare di essere proprietaria dei token, inviando i bitcoin ad un altro indirizzo UTXO di sua proprietà.

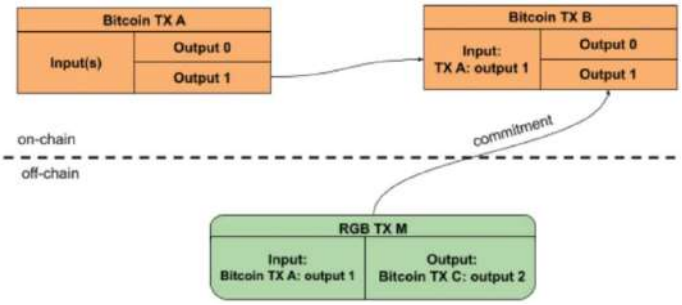


Figure 2.3: transazione di token

2.3.1 Validazione lato client

La procedura di convalida dei trasferimenti in entrata in RGB è notevolmente diversa da quella applicata ai pagamenti standard in Bitcoin.
Nel caso di Bitcoin, un nodo connesso alla rete scarica e convalida continuamente i blocchi e le transazioni presenti nella mempool. In questo modo, il nodo è sempre in grado di visualizzare una copia aggiornata dell'UTXO set, che raccoglie tutti gli UTXO nella blockchain. Questo è utile perché, nel momento in cui viene inserita una nuova transazione, è sufficiente controllare che tutti gli input siano presenti nell'ultimo stato dell'UTXO set per verificarne la validità.

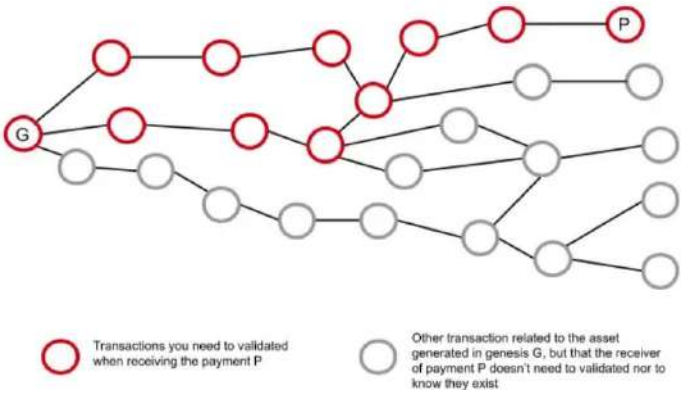


Figure 2.4: convalida lato client

In RGB non esiste una rete globale in cui vengono trasmesse tutte le transazioni, pertanto non è possibile creare un UTXO set equivalente a quello di Bitcoin. Quando un client RGB riceve un pagamento in entrata, deve quindi non solo verificare che l'ultima transizione di stato sia valida, ma anche eseguire la stessa operazione di convalida per tutte le transizioni di stato precedenti, fino

al momento di genesi del contratto di emissione.
Allo stesso tempo, questo significa anche che, a differenza di Bitcoin e di qualsiasi altro sistema di consenso globale, in RGB un client non ha bisogno di vedere e convalidare tutte le transazioni che avvengono a livello globale, ma solo quelle pertinenti al suo wallet (Figura 2.4). Di conseguenza, per ogni client la quantità di dati che deve convalidare è significativamente minore e ciò rende il sistema complessivamente più scalabile.
La necessità di convalidare molti dati nel momento in cui avviene la ricezione di un pagamento, può essere visto come un problema. Infatti, si potrebbe verificare un'esperienza di pagamento lenta a causa del tempo necessario per validare un trasferimento in entrata. Tuttavia, questo diventa un problema solo quando si ricevono asset con una cronologia di transazioni molto lunga.
Una possibile soluzione è permettere ai client di condividere volontariamente tra loro i dati di state transition relativi a contratti con cronologia lunga. In questo modo, i futuri riceventi possono iniziare a convalidare in anticipo parte dello storico delle transazioni.

2.3.2 Commitment su Bitcoin

Come detto precedentemente, RGB utilizza la blockchain di Bitcoin per proteggersi dal double spending. Questo viene fatto mediante un commitment crittografico per ogni transizione di stato RGB, inserito all'interno delle transazioni che spendono l'UTXO contenente i diritti di trasferimento.
Affinché il commitment crittografico sia versatile e sicuro, devono essere soddisfatte due condizioni:

- con una singola transazione Bitcoin si possono effettuare più transizioni di stato (garantisce la versatilità)
- la transazione Bitcoin può contenere un solo commitment per ogni transizione di stato (garantisce la sicurezza, evitando il double spending)

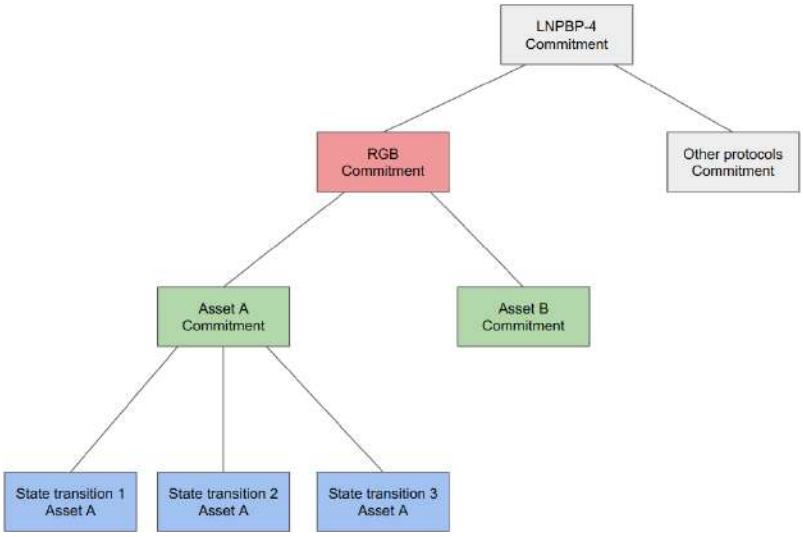


Figure 2.5: Deterministic Bitcoin Commitments

Per soddisfare la prima condizione, le transizioni di stato possono essere aggregate più volte in un merkle tree (Figura 2.5), nel modo seguente:

1. si aggregano tutte le state transitions relative ad un contratto specifico
2. si aggregano i commitment relativi a contratti diversi
3. si aggrega il commitment RGB risultante con i commitment di altri protocolli, al fine di garantire la compatibilità di RGB (come descritto da LNPBP4 standard)

L'hash risultante diventa la stringa inserita effettivamente nella transazione Bitcoin.
Una volta ottenuto il messaggio LNPBP-4 finale, ci sono due modalità per inserirlo all'interno della transazione Bitcoin:

- **Commitment Taproot**: viene aggiunto uno script OP_ RETURN, contenente il messaggio LNPBP-4, nel nodo foglia in alto a destra del TapTree del primo output Taprooot della transazione Bitcoin (Figura 2.7)
  Tale messaggio viene rivelato solo off-chain al destinatario del trasferimento RGB. In questo modo la transazione Bitcoin può contenere un solo output taproot che può essere utilizzato sia per rispedire la modifica bitcoin al mittente sia per contenere il commitment senza aggiungere alcun byte extra e senza lasciare alcuna traccia che la transazione Bitcoin possa essere legata a un trasferimento di asset RGB.

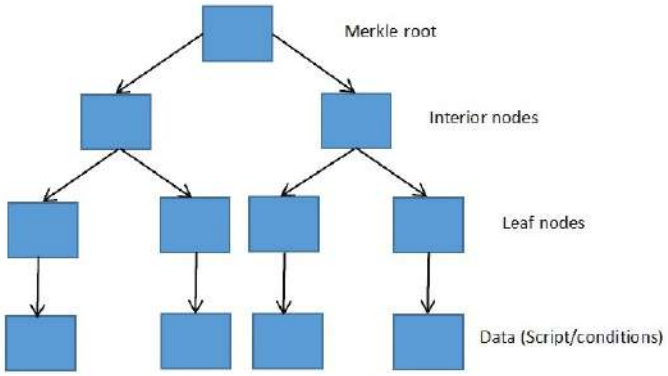


Figure 2.6: TapTree

- **Commitment OP_RETURN**: il messaggio LNPBP-4 viene inserito direttamente nel primo output OP_RETURN della transazione Bitcoin. Ciò si traduce in 46 byte extra nella transazione, ma non rivela alcuna informazione sul contenuto del trasferimento RGB poiché per l'osservatore blockchain è solo un OP_RETURN con un hash (esattamente come, ad esempio, le transazioni di open timestamp). Il vantaggio di questo schema rispetto a quello basato su Taproot è la sua semplicità e la più facile integrazione per gli sviluppatori dei wallet.

Qualsiasi tentativo di double spending è reso vano dal fatto che, nel caso in cui vengano inseriti più commitment nella transazione Bitcoin, solo il primo sarà rilevante per le regole di validazione RGB e gli altri verranno ignorati.

2.3.3 Batching

La possibilità di includere un numero arbitrario di state transation in un singolo commitment Bitcoin, permette di effettuare operazioni di batching di grandi dimensioni. Ad esempio, se qualcuno desidera effettuare pagamenti a più persone contemporaneamente, può semplicemente creare una state transaction per ogni destinatario e inserire i relativi commitment nella stessa transazione Bitcoin, senza aumentarne la dimensione e mantenendo invariato il costo della commissione on-chain. Questo permette di rendere molto basso il costo marginale di ogni pagamento RGB.
Tuttavia, queste operazioni di batching risultano efficaci solo quando si spende dallo stesso UTXO. Infatti, se un utente spende da più UTXO, ciascuno di questi output deve essere incluso come input nella transazione Bitcoin, aumentandone la dimensione e, conseguentemente, la commissione on-chain da pagare.

Il batching è notevolmente utile per i fornitori di servizi con UTXO consolidati, come gli exchange, che devono gestire molti clienti e hanno quindi la necessità di effettuare contemporaneamente un elevato numero di operazioni. Ad esempio, un exchange potrebbe aggregare tutte le richieste di prelievo ogni 30 minuti in un'unica transazione on-chain e, con il costo di quella singola transazione, pagare ciascun utente che ha inviato una richiesta di prelievo in quel periodo di tempo.

2.4 Privacy

RGB presenta già un grado elevato di privacy grazie al protocollo di validazione lato client. Un ulteriore miglioramento è stato apportato con l'aggiunta dei *blinded UTXO*.
Il nome è legato al fatto che vengono costruiti usando l'hash della concatenazione tra l'UTXO e un segreto random. Quando un utente vuole essere pagato, invece di condividere l'UTXO in cui ricevere l'asset, può aumentare la propria privacy condividendo l'UTXO in formato blinded.
In questo modo, il mittente non sa esattamente dove sono finiti gli asset e non può monitorare quando verranno spesi in futuro.

La segretezza dell'UTXO viene meno nel momento in cui si vuole trasferire nuovamente la proprietà dell'asset. Infatti, durante la fase di spesa, il mittente deve condividere con il ricevente il blinding secret utilizzato per generare l'UTXO blinded. In questo modo, durante la fase di validazione il ricevente può verificare che l'hash della concatenazione tra l'UTXO e il segreto coincide con il blinded UTXO, che aveva ricevuto l'asset.

```
UTXO: ad3ebdcda0f83b37fffab0439c89fd3ef7d99c41c353a45a98d5983d9ad00183:0

Outpoint blinding secret: 8114079862469528952

Blinded outpoint:
txob1kewrvnf8sjmarq65gv98lz2xrgxylpnlta8lc3p78fjxaw9qda4qkewlwr
```

Figure 2.7: Esempio di un UTXO blinded

2.5 Comunicazione client-to-client

Come già anticipato, i client coinvolti nella transazione RGB devono condividere tra loro alcuni dati in un canale di comunicazione dedicato. Nello specifico, il mittente deve condividere con il/i destinatari il *consignment* che è una struttura dati contenente le informazioni necessarie per permette la validazione del trasferimento, incluso tutto lo storico delle precedenti state transation fino a raggiungere il contratto di genesi. La condivisione dei dati in RGB può avvenire attraverso due canali principali:

- **Storm**: un sistema di messaggistica e storage peer-to-peer costruito su Lightning Network.
- **RGB proxy server**:un server HTTP JSON-RPC standardizzato in cui i client possono caricare e scaricare dati. Un utente può fare hosting del proprio server proxy o utilizzare il server di una terza parte. Affidarsi a un server di terze parti ha implicazioni sulla privacy e sulla censura, ma non sulla sicurezza.

Il coordinamento sulla scelta del canale di comunicazione da utilizzare avviene tramite un protocollo di invoice, tramite il quale il ricevente mette a disposizione uno o più endpoint dove il mittente può caricare i dati del consignment.

Chapter 3

Compatibilità con LN

Lightning Network è un layer 2 di Bitcoin, che permette di transare in maniera trustless al di fuori della blockchain, usando canali di pagamento chiamati "payment channels".
RGB è *disegnato* per essere compatibile con Lightning Network, astraendo in "asset generici" l'interno dei canali di pagamento. Gli asset di RGB possono essere quindi trasferiti con la stessa velocità e convenienza che caratterizza le transazioni bitcoin su lightning. Data però la natura di LN, è richiesta molta liquidità per *lavorare* in maniera efficace.

3.1 Vantaggi

Tra i vantaggi nell'utilizzare la tecnologia Lightning Network in comunione con RGB si ha:

- possibilità di tradare gli asset direttamente su lightning
- bassa latenza ed alta velocità di transazioni
- no "frontrunning"
- atomic-swap basati su liquidity pools
- costi di infrastruttura "condivisi"
- decentralizzazione del trading su Bitcoin
- maggiore volume per i "LN node operators"

3.2 Commitment su LN

In generale il commitment su Lightning Network può essere diviso in tre fasi:

1. invio degli asset al multisig UTXO di apertura del canale LN. Ovvero viene creata una "funding transaction". Nell'esempio riportato in figura 3.1, Alice apre un canale con Bob. Contestualmente all'apertura del canale LN (e quindi alla creazione del multisign 2/2 tra A e B), viene creato un RGB State Transition, e gli asset vengono *committati* ad un nuovo UTXO condiviso nel 2/2 di proprietà di Alice e Bob.

2. ad ogni update dello stato del canale, si crea un nuovo "RGB state transition" che aggiorna l'ownership degli asset all'interno dell'HTLC tra Alice e Bob (vedi figure 3.2, 3.3, 3.4, 3.5).

3. quando il canale viene chiuso, ogni rispettiva parte coinvolta muove gli asset dall'UTXO di commitment (il multisig), ad un UTXO esclusivamente controllato da loro (vedi figura 3.6)

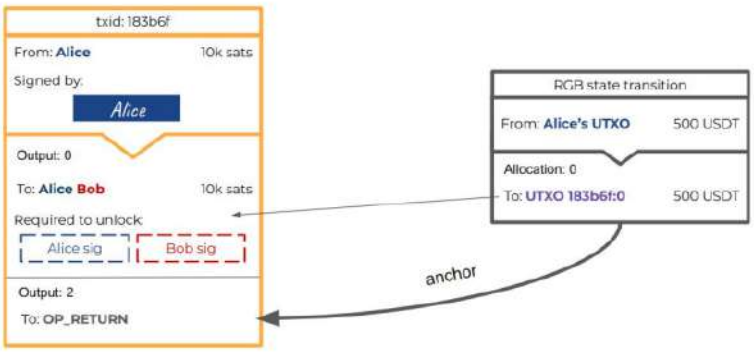


Figure 3.1: LN Bitcoin Commitments

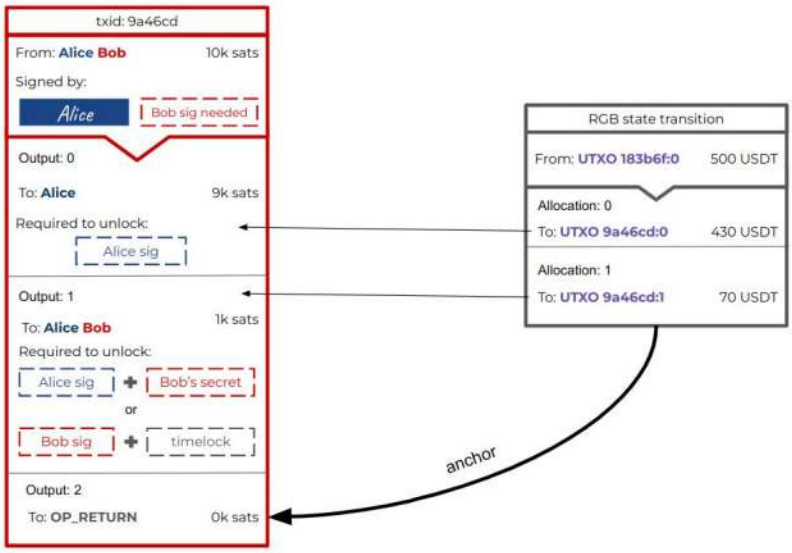


Figure 3.2: RGB State Transition on LN

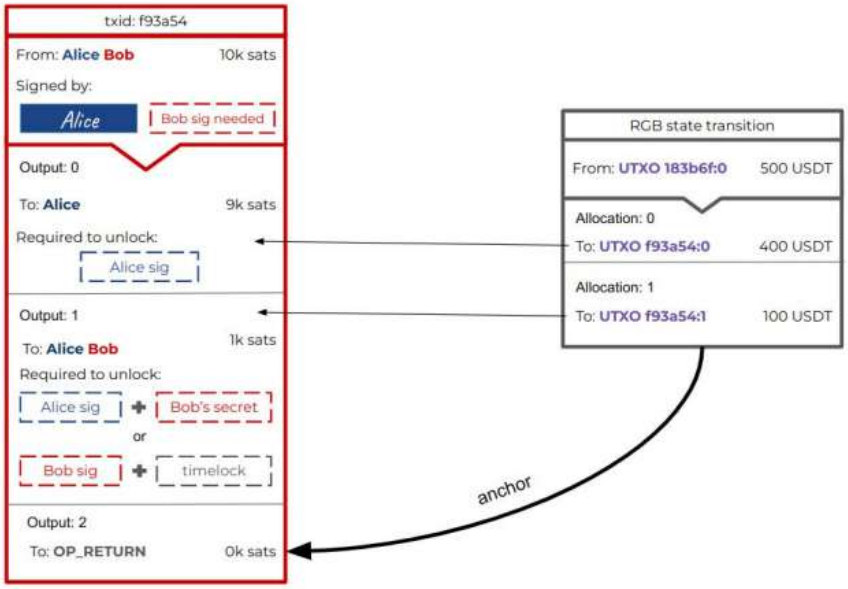


Figure 3.3: RGB State Transition on LN

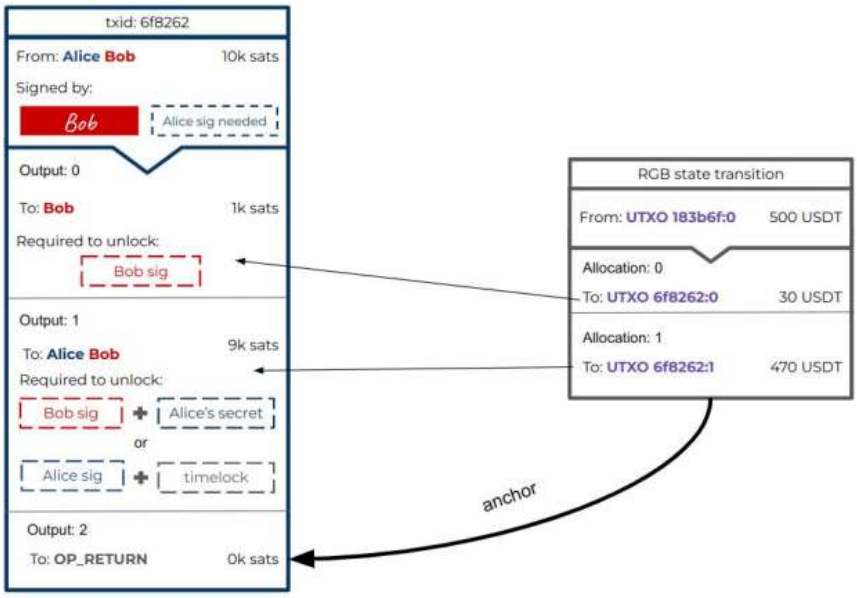


Figure 3.4: RGB State Transition on LN

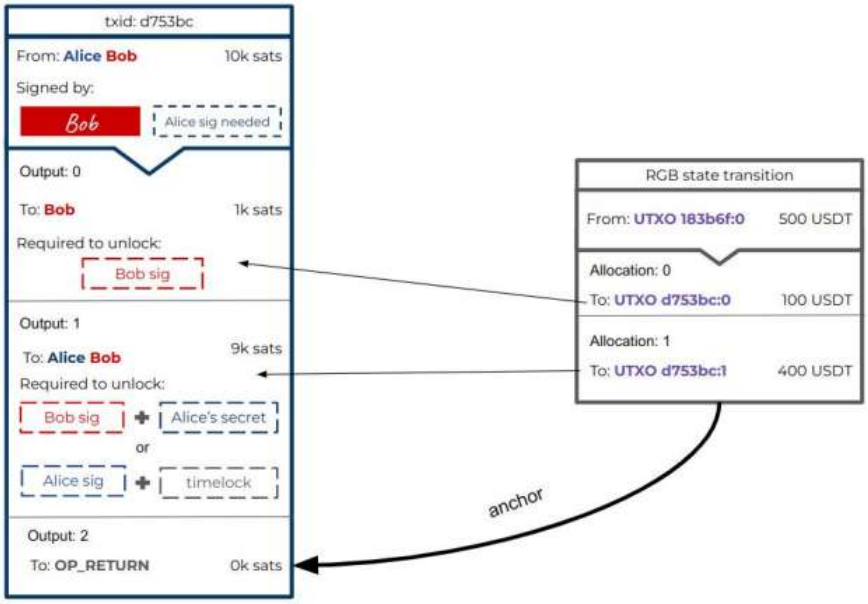


Figure 3.5: RGB State Transition on LN

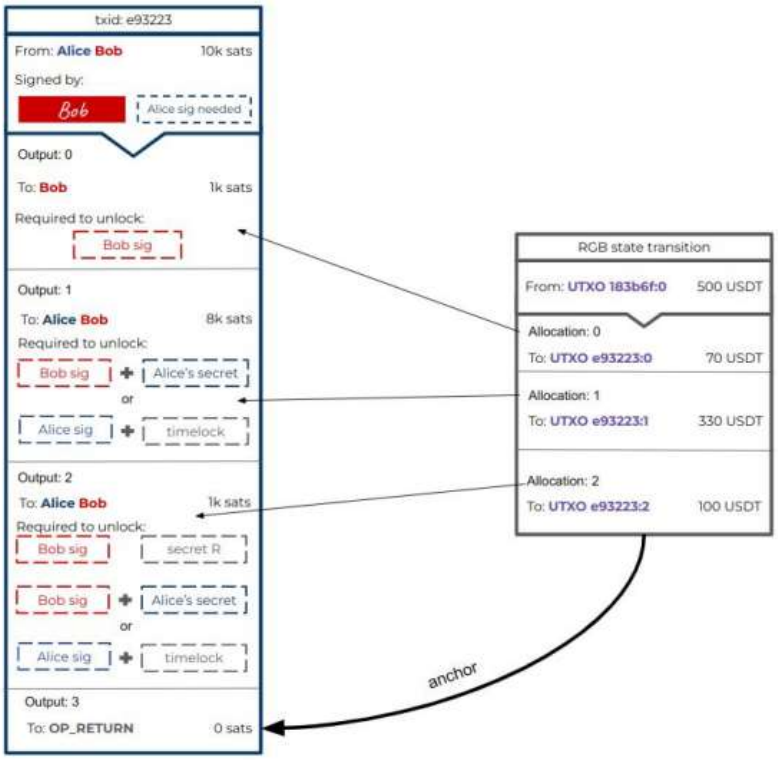


Figure 3.6: RGB State Transition on LN

Chapter 4

Conclusioni

RGB è un'innovazione rivoluzionaria che apre a nuovi casi d'uso, utilizzando un paradigma (Client Side Validation + "ancoraggio" onchain/LN) completamente nuovo nell'ecosistema "blockchain". Nonostante la tecnologia sia ancora in fase di sviluppo e produzione, riteniamo che possa nell'immediato futuro avere un notevole impatto nell'ecosistema.

Bibliography

[1] Bitcoin detox 9 - rgb: la tv a colori per bitcoin - giacomo zucco. https://www.youtube.com/watch?v=6JeULalSi3Y.

[2] Rgb blackpaper. https://blackpaper.rgb.tech/.

[3] Rgb magic: client-side contracts on bitcoin. https://bitcoinmagazine.com/technical/rgb-magic-client-contracts-on-bitcoin,.

[4] Rgb protocol: Asset issuance on bitcoin and lightning network — plan b forum 2022 — lugano. https://www.youtube.com/watch?v=WBnMiHQCt6g&list=PLNETuT4LKydJeNVFFR-aVLcFWLOURWnBC&index=47,.

[5] Rgb viareggio summit 2023. https://www.massmux.com/wp-content/uploads/2023/04/federico-tenga-viareggio.pdf,.

[6] Rgb.info. https://docs.rgb.info/.

[7] Understanding the rgb protocol. https://medium.com/@FedericoTenga/understanding-rgb-protocol-7dc7819d3059.

CORDA

UNA PIATTAFORMA BLOCKCHAIN PROGETTATA PER I SERVIZI FINANZIARI

Mahdi Beji, Martina Bonelli, Riccardo Kiefer, Sara Papapietro

POLITECNICO DI TORINO

Corso di Laurea Magistrale in Ingegneria Matematica

Blockchain e Criptoeconomia

Corda: una piattaforma blockchain progettata per i servizi finanziari

Supervisors

Prof. Danilo BAZZANELLA

Prof. Andrea GANGEMI

Candidate

Mahdi BEJI 304665

Martina BONELLI 299777

Riccardo KIEFER 301286

Sara PAPAPIETRO 305726

Giugno, 2023

Indice

1 Introduzione 1

2 Struttura e funzionamento di Corda 3
2.1 Data model 4
2.1.1 CordApp 5
2.1.2 Transazioni 9
2.2 Algoritmi di consenso 10
2.3 Business Logic: smart contracts 11
2.4 Nodi notarili 12
2.4.1 Servizi notarili integrati 12
2.4.2 La soluzione del modello GSL (Global Synchronisation Log) 13
2.4.3 Implementazione del modello GSL in Corda 14

3 Confronto con altre piattaforme 15
3.1 Corda: Blockchain o DLT? 15
3.2 Corda VS Bitcoin 16
3.3 Corda VS Ethereum 17

4 Conclusioni 18
4.1 Vantaggi di Corda 18
4.1.1 Sistema permissioned e privacy 18
4.1.2 Applicazioni 19
4.2 Svantaggi di Corda 19

Capitolo 1

Introduzione

In diverse aziende, uno sforzo notevole viene fatto per riuscire a mantenere diversi database sincronizzati gli uni con gli altri. Perchè non utilizzare un modello relazionale? Sicuramente risolverebbe molti problemi, impiegando soltanto le tecnologie esistenti, tuttavia darebbe luogo anche ad alcune domande:

- Come si può trovare un individuo incorruttibile a cui affidare la gestione del database?
- Cosa succederebbe in caso di manutenzione del database?
- Se venisse attaccato?
- Cosa fermerebbe i paesi che fanno da host dal non abusare dell'enorme quantità di informazioni sensibili in loro possesso?

Possiamo immaginare molte altre domande, a cui si cerca di dare una risposta, almeno in parte, attraverso la realizzazione di un database decentralizzato.
Corda s'inserisce nel gruppo delle piattaforme blockchain con ledger distributo.
Viene utilizzata per la registrazione, la gestione e la sincronizzazione di transazioni finanziarie, con scelte di design che la rendono in grado di soddisfare le esigenze delle istituzioni finanziarie regolarmente.
E' stata sviluppata a seguito della nascita nel 2015 del Consorzio R3, un'azienda che guida un network di 200 partecipanti tra istituti finanziari, banche, enti regolatori e aziende di tecnologia.
Viene pensata per superare le difficoltà di interoperabilità tra le diverse piattaforme che vengono utilizzate dai clienti dei diversi istituiti bancari.
Infatti, il problema che Corda cerca di risolvere riguarda la gestione degli accordi tra aziende e individui, specialmente quando tali parti si fidano l'una dell'altra

abbastanza da intrattenere rapporti commerciali, ma non abbastanza da far sì che la loro controparte mantenga tutti i record delle transazioni, potendo dunque negare il fatto di averne eseguita qualcuna.
Come viene riportato all'interno del White Paper *The corda Platform: An Introduction* di Richard Genadl Brown, CTO di R3, Corda è:

"il risultato di oltre due anni di intenso lavoro di ricerca e sviluppo da parte di R3 per soddisfare i più alti standard dei servizi finanziari ed è oggi applicabile a qualsiasi scenario commerciale".

Corda include i seguenti principi legati al business:

1. *inclusione*: essendo una rete aperta, i nodi si conoscono l'un l'altro;
2. *identità assicurata*: i nodi hanno garanzia dell'identità dei partecipanti della rete;
3. *privacy*: le uniche entità che hano accesso ai dettagli di una transazione sono coloro che ne prendono parte;
4. *logica condivisa*: la validità e consistenza degli accordi è garantita e condivisa;
5. *base giuridica*: ogni transazione registrata nel ledger è per contratto accettata come prova ammissibile e legalmente vincolante, da tutte le perti in qualsiasi controversia;
6. *immutabilità*: qualsiasi fatto registrato nel ledger è da considerarsi definitivo e immutabile.

Capitolo 2

Struttura e funzionamento di Corda

Corda è una piattaforma pensata a livello di mercato e di industrie, non a livello di singole aziende.
L'elemento principale è lo *state object*: un documento digitale che contiene i dettagli e lo stato di un accordo fra più parti. Esso rappresenta un'istanza specifica di un accordo, ovvero un contratto nel mondo reale. Viene condiviso soltanto tra chi è legittimato a consultarlo.
Qualsiasi operazione in Corda viene eseguita attraverso *transazioni*, le quali sono composte da più *state object* di input e di output, da un *command* che specifica l'azione che si sta svolgendo, e vengono validate attraverso controlli specificati nello *smart contract*.
Quest'ultimo consiste in un'unica funzione, il *verify()*, la cui responsabilità è quella di accettare (ritorna senza risultato) o rifiutare (lancia un'eccezione) una transazione proposta. Possiamo perciò dire che una transazione corrisponde al ciclo di vita di uno *state object*, il quale può essere *consumato* e *ricreato* ad ogni funzione eseguita.
Sono necessarie poi, le firme dei partecipanti alla transazione.
Inoltre, le transazioni sono atomiche: non possono presentarsi stadi intermedi. Esse possono andare a buon fine venendo considerate valide, oppure possono essere rifiutate. I contratti definiscono quindi la parte critica della business logic del ledger condiviso, essendo gli *state object* immutabili.
Corda è costruita su un'architettura *point to point* e i partecipanti possiedono una copia solo delle transazioni alle quali prendono parte. Ogni nodo di una rete Corda possiede un ledger univoco che tiene traccia di queste transazioni: il *vault*. Due partecipanti durante la visualizzazione del ledger (soggettiva per

ogni peer), hanno la certezza di vedere sempre la stessa versione degli state object che condividono.

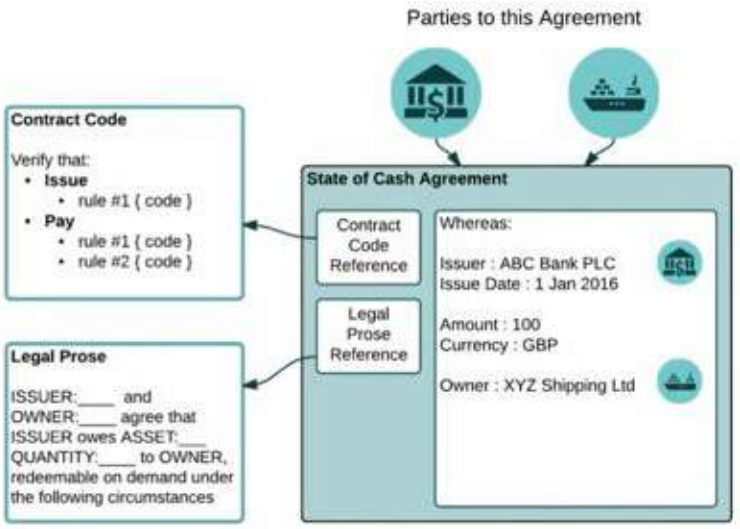


Figura 2.1: Nella figura viene rappresentato uno state object rappresentante un pagamento di £100 con emittente una banca commerciale.

2.1 Data model

La rete globale Corda ha lo scopo di abilitare un gran numero di reti aziendali in competizione e collaborative, accomunate dall'idea di facilitare l'interoperabilità dei nodi.
I componenti principali della Corda network sono:

1. i nodi Corda che devono eseguire *CordApp*;
2. specifici parametri di rete che indicano i nodi critici per il consenso, ovvero quelli che devono essere d'accordo per garantire la stabilità della rete;
3. *identity framework* che permettono alle imprese di avere garanzia di fiducia nello stipulare contratti nel mondo reali;
4. *pool notarile* che sono gruppi di consenso e forniscono servizi di consenso univoco e trasparente;

2.1.1 CordApp

Una CorDapp è un'applicazione decentralizzata che basa il suo funzionamento su tre elementi essenziali:

1. lo *state*, che rappresenta un'azione condivisa tra i nodi della rete. Definisce i partecipanti, il riferimento al contratto di gestione della compravendita che regola l'uso dello *state object* e le proprietà della transazione.
   Nelle blockchain tradizionali, ogni fatto deve essere consultabile da tutti, mentre in Corda, ogni partecipante vede solo un sottoinsieme dei fatti presenti nel registro, ovvero un sottoinsieme di state. Uno state può essere corrente (*'unspent'*) oppure consumato (*'spent'*) e dunque non più valido. Uno state viene consumato e creato da una transazione.

2. il *contract*, che ha due scopi:

   - essere il riferimento alla documentazione legale generale che le due parti hanno concordato, nella quale viene gestita la situazione nel caso di controversie (come un contratto reale);
   - verificare che la proposta di transazione sia valida: accedendo ai dettagli della transazione, viene controllato che il numero di input state e output state sia quello stabilito e che i dati specifici all'interno di questi state siano corretti;

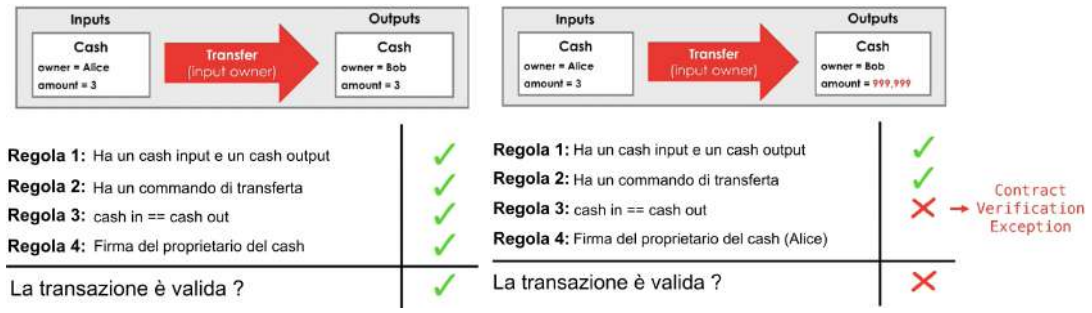
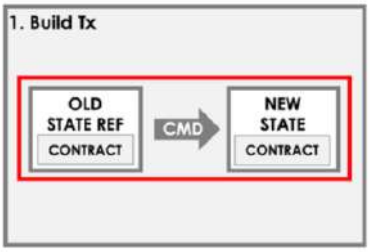


Figura 2.2: esempi di verifica di una transazione

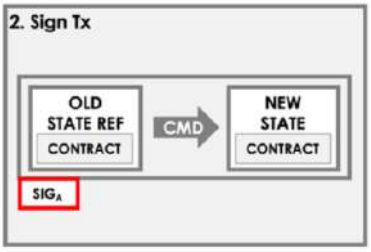
3. il *flow*, che è la comunicazione tra i nodi della rete, in cui un nodo costruisce una transazione (*initiator*) e la invia alla controparte (*responder*). Uno strumento utilizzato e gestito da ogni nodo in questo processo è il *vault*, cioè un database in cui si tiene traccia di tutti gli state attuali (non consumati) e di quelli storici (marcati come historic o consumati) di cui è a conoscenza

e che considera rilevanti per se stesso.
Il flow di una transazione è composto a livello implementativo dai seguenti passi:

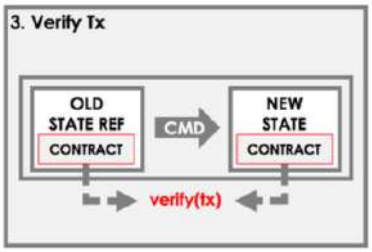
(a) costruzione della transazione: viene creato un *builder* per la futura transazione, si sceglie il nodo notarile, vengono raccolti dal *vault* dell'*initiator* gli input state necessari alla transazione e vengono creati gli output state;



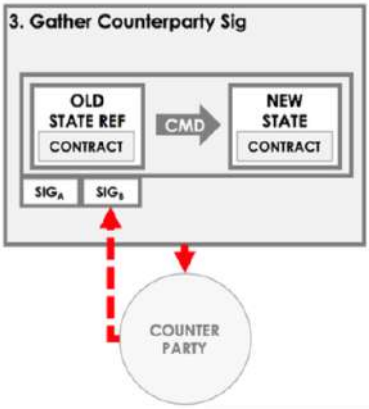
(b) firma da parte dell'*initiator* del *builder* della transazione, che viene convertito in una *signed transaction* (parzialmente firmata) ;



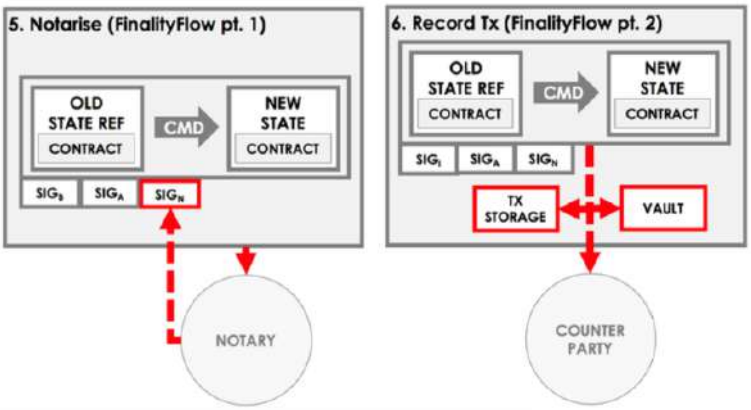
(c) verifica della transazione: vengono eseguiti i contratti associati per verificare la transazione. Solo il metodo *verify()*, come menzionato, sarà indicato al fine di determinare la validità della transazione;



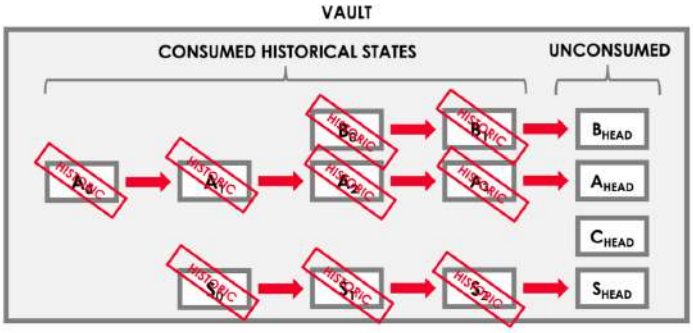
(d) ottenimento della firma della controparte: viene inviata la transazione al *responder* che verifica la presenza della firma dell'*initiator*, esegue i contratti, genera la sua firma sulla transazione e invia nuovamente al mittente il tutto;



(e) finalizzazione della transazione: l'*initiator* verifica le firme della transazione appena ricevuta e la invia al *pool* notarile. Quando quest'ultimo la *notarizza*, l'*initiator* la registra localmente salvando gli opportuni *state object* nel proprio *vault* e invia la transazione alla controparte che farà lo stesso.



Nella seguente figura è riportato un esempio di *vault* di un nodo in Corda.



Dal punto di vista di ogni nodo possiamo pensare al ledger come l'insieme di tutti gli state attuali (cioè non storici) di cui è a conoscenza. Di conseguenza, ciascun peer ha la possibilità di vedere solo un sottoinsieme di state del libro mastro e nessun peer è a conoscenza della sua interezza.

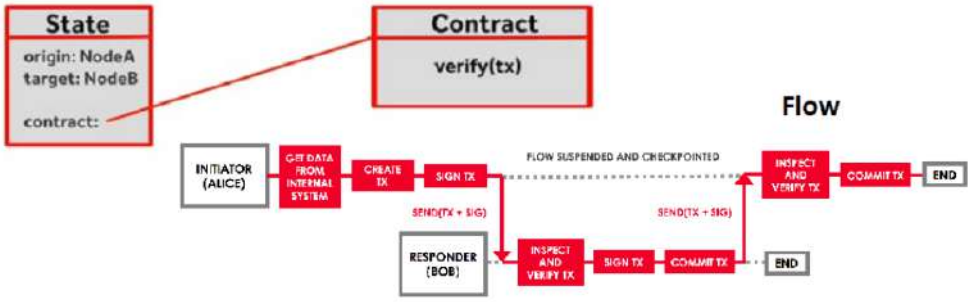


Figura 2.3: Funzionamento di una CorDapp.

2.1.2 Transazioni

Una transazione è una proposta di modifica del registro e funziona come segue: consuma zero o più states e ne crea zero o più nuovi.
Grazie a questo funzionamento, ogni stato può essere identificato dalla transazione che l'ha creato.
In particolare una transazione è composta da:

1. **Consuming input references**: puntano agli stati che una transazione sta consumando.

2. **Output states**: sono gli stati prodotti dalla transazione.

3. **Non-consuming input references**: 'reference-states' che non vengono consumati. Possono servire per l'importazione di dati che sono utili a verificare lo smart contract. Devono essere 'unspent'.

4. **Attachments**: non hanno un concetto di consumo (spentness) e sono rappresentati nelle transazioni come una lista ordinata di file zip. Ogni zip può contenere dati che servono alla transazione a cui il contratto ha accesso per verificarne la validità.

5. **Commands**: un asset può essere spostato nel registro ad un altro utente, creato o cancellato dal registro. Un command è un parametro che contiene più informazioni di quelle presenti negli state.

6. **Signatures**: sono richieste N firme nella transazione quando i commands hanno N chiavi pubbliche. Una signature può usare una varietà di suite di cifratura.

7. **Timestamp**: quando c'è, contiene un intervallo di tempo in cui la transazione è avvenuta. Specifica [start, end].

8. **Network parameters**: sono le hash dei parametri della rete presenti quando è avvenuta la transazione.

Di seguito viene riportato un esempio di una transazione tra il nodo 1 (Bob)e il nodo 2 (Alice) su Corda.

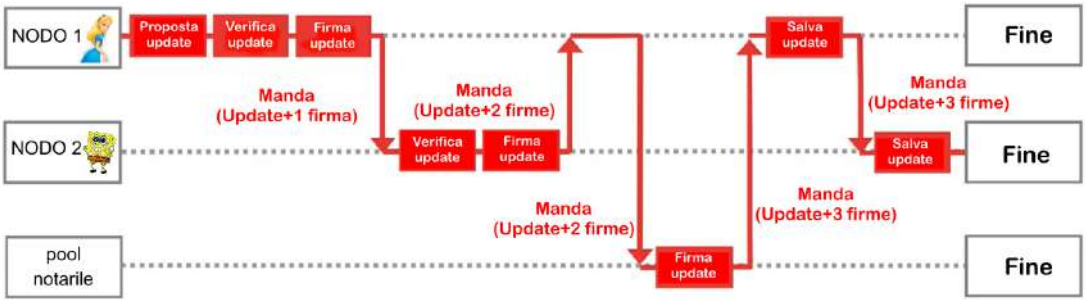


Figura 2.4: Transazione tra Alice e Bob: per esempio Alice che chiede soldi a Bob.

2.2 Algoritmi di consenso

Uno degli algoritmi nati per il consenso delle transazioni e dei blocchi in un sistema basato su blockchain è la Proof of Work. Non sempre però viene ritenuto il più vantaggioso, infatti Corda ne implementa uno nuovo attraverso 3 step:

1. Approvazione delle transazioni da parte dei partecipanti;
2. Approvazione della posizione in cui la transazione verrà inserita nel ledger.
3. Validazione, in cui viene preso un blocco di transazioni approvate e ordinate e viene convalidata la correttezza dei risultati. In particolare ci sono due aspetti fondamentali che riguardano la validazione.
   - Validità della transazione: è riposta interamente nelle mani degli smart contract che sono implementati nella rete. Ogni contratto ha infatti dei vincoli che devono essere rispettati nel momento in cui avviene una transazione.
   - Unicità della transazione: si deve controllare che gli stati consumati da una transazione non siano già stati consumati da un'altra.

Corda ha un consenso *pluggable*, ovvero non esiste un algoritmo preimpostato e può implementare diversi modelli di approvazione e validazione in base alle proprie esigenze. Quindi, come detto nei punti precedenti, il consenso viene ottenuto controllando se gli stati consumati da una transazione sono già stati consumati da un'altra e se le transazioni rispettano i vincoli degli smart contract.

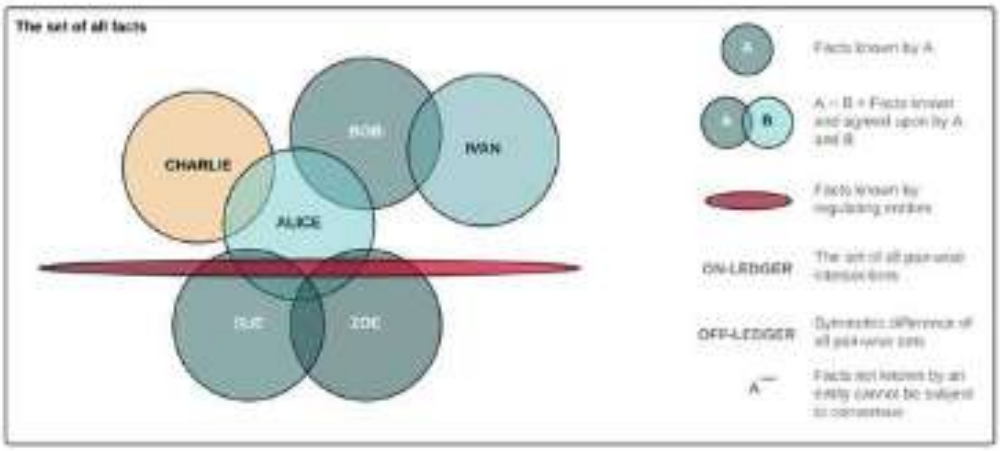


Figura 2.5: Il consenso sulla validità della transazione è dato solamente dalle parti che la eseguono. Ogni attore in Corda vede quindi solo un sottoinsieme di tutti i dati gestiti dal sistema. Diciamo che un dato è "on-ledger" se almeno due attori nel sistema concordano su di esso. Dati posseduti solo da un attore sono detti "off-ledger".

Nella rete troveremo un notaio o un gruppo notarile che autentica le transazioni con una firma che approva la scrittura nel ledger. Nel caso in cui si abbia un gruppo di notai a disposizone, ogni utente può decidere a quale affidarsi.
Come verrà meglio approfondito di seguito, i notai sono dei nodi all'interno della rete che offrono dei servizi notarili per l'organizzazione delle transazioni e, hanno come obiettivo quello di finalizzare una transazione tra due parti, nel caso ci fosse assenza di double spend. La presenza della firma di un notaio su una transazione indica la finalità della stessa.

2.3 Business Logic: smart contracts

Per eseguire le transazioni viene utilizzata la sandbox di *Java Virtual Machine*. Il nucleo di Corda è scritto in in linguaggio Kotlin, un linguaggio simile a Java ma molto più sintetico. Infatti, è possibile riassumere interi blocchi di linee di codice in Java con una singola riga in Kotlin. Nonostante il nucleo abbia questo linguaggio è possbile comunque implementare contratti e stati in Java visto che sono compatibili.
Ogni smart contract di Corda è composto da tre parti principali:

- il codice eseguibile (la logica di validazione): giudica la validità degli state object della transazione e degli altri suoi dati;

- lo *state object*: dati contenuti, o che saranno registrati, nel ledger che identificano gli input e gli output di una transazione;

- il *command*: dati aggiuntivi compresi nella transazione. Descrive l'azione che deve compiersi e istruisce il codice del metodo **verify()**.

2.4 Nodi notarili

Uno dei punti chiave di Corda è la separazione della verifica di una transazione tramite i contratti dalla questione di conflitto tra due transazioni che hanno superato la validazione, ma che si trovano in conflitto ad esempio, per l'assenza di qualche firma.
È necessaria la presenza di un'entità della quale tutti i nodi si fidano per scegliere tra due transazioni ugualmente valide ma in conflitto. All'interno del consorzio R3 è utilizzato il nominativo di *nodo notarile* per questa entità che rappresenta il ruolo svolto dai miners in una blockchain tradizionale.
I notai sono quindi dei nodi all'interno della rete che offrono dei servizi notarili per l'organizzazione delle transazioni e hanno come scopo principale quello di finalizzare una transazione tra due parti, in assenza di double spend. I notai vengono identificati e firmano con delle chiavi pubbliche composte.

2.4.1 Servizi notarili integrati

Corda include diverse implementazioni notarili integrate:

1. *Single-node*: un semplice servizio notarile che mantiene le richieste di notarizzazione nel database del nodo. È facile da configurare ed è consigliato per i test e le reti di produzione che non hanno requisiti di disponibilità rigorosi.

2. *Crash fault-tolerant*: un servizio notarile altamente disponibile gestito da un solo nodo.

3. *Byzantine fault-tolerant:* un servizio notarile altamente disponibile, decentralizzato e gestito da un gruppo di nodi.

L'implementazione notarile più in uso è la *single-node*. Le implementazioni rimanenti, attualmente, sono utilizzate solo a livello sperimentale.
Per usufruire del servizio notarile *single-node* è sufficiente impostare i valori di configurazione appropriati del nodo notarile prima di avviarlo. Settando il parametro validating come *false* la transazione non verrà verificata per validità (nodo notarile non convalidante): crea il rischio di attacchi "denial of state". Nel caso contrario settando il valore a *true* la transazione viene verificata per la validità (nodo notarile convalidante): il nodo notarile avrà accesso all'intero contenuto della transazione e alle sue dipendenze (come il miner per la blockchain tradizionale). Ciò fornisce dati potenzialmente privati al nodo notarile.

2.4.2 La soluzione del modello GSL (Global Synchronisation Log)

La piattaforma Corda implementa attraverso il nodo notarile, il modello GSL (Global Synchronisation Log) di Digital Asset in grado di gestire il rischio di attacco di tipo denial of state. Questo comporta la possibilità di utilizzo di un nodo notarile non convalidante, in cui non si viene a conoscenza di tutti i dettagli della transazione ma solamente dei dati necessari al fine di determinare l'ordine e l'unicità della transazione. Questo approccio però può portare sfiducia nei partecipanti della transazione: essi non vengono informati della conferma della stessa nel medesimo momento in cui il mittente riceve la conferma della transazione. Per risolvere quest'ultimo problema si adotta il seguente metodo:

- Vengono salvate in una lista, esterna alla transazione, le identità di tutti i partecipanti e il nodo notarile viene a conoscenza di questa lista.
- Questo elenco, però, potrebbe non essere corretto e il nodo notarile non avrebbe modo di verificarlo. Dunque si aggiunge una regola: se la transazione non "etichetta" il giusto insieme di destinatari previsti, allora non è considerata valida. Un possibile truffatore si troverebbe di fronte a una transazione dalla quale non riesce ad ottenere le identità necessarie alla sua validità perché quest'ultime sono autenticate dal nodo notarile. Quindi ci troviamo di fronte alla situazione migliore possibile: viene usato un nodo notarile non convalidante, e allo stesso tempo, l'attaccante non riesce ad ottenere una transazione valida, grazie alla regola imposta.
- D'altra parte se viene costruita una transazione valida secondo i contratti associati, allora il nodo notarile dovrà irreversibilmente informare tutte le parti interessate. Quindi un attaccante non ha la possibilità di ottenere transazioni valide e confermate allo stesso tempo.

Questo approccio lega il caso della validità della transazione al problema della notifica delle parti interessate, secondo una logica di tipo: "Non si può avere uno senza l'altro".
In questo modo si ottiene qualcosa di utile: i contenuti della transazione rimangono visibili solo a chi ha bisogno di vederli e la verifica delle transazioni è responsabilità di quelli che ne hanno preso parte; i notai non vedono ciò che non dovrebbero e se una transazione viene eseguita, tutte le parti pertinenti ne vengono a conoscenza. Per un buon numero di casi d'uso, questa è una serie discreta di compromessi.

2.4.3 Implementazione del modello GSL in Corda

Il modello GSL viene implementato in Corda attraverso i seguenti aspetti della piattaforma:

- Il problema del denial of state viene risolto grazie ai nodi notarili di Corda che registrano da subito i mittenti delle transazioni quando operano in modalità non convalidante.
- Corda supporta i transaction tear-offs, ossia il meccanismo in base al quale solo le informazioni pertinenti vengono condivise con terze parti, quali i nodi notarili, utilizzando la struttura merkle tree.
- Corda supporta il concetto di partecipanti/tag, ovvero una lista allegata a ciascuna transazione (grazie al metodo getPartecipant() definito nello state) che identifica le parti interessate.
- Il motore di verifica (metodo *verify()*) delle transazioni di Corda consente già ai contratti di verificare che l'elenco dei partecipanti sia correttamente compilato.

Il seguente modello si discosta leggermente da una blockchain: non è possibile per i partecipanti, "sfogliare" un ledger alla ricerca delle transazioni di interesse. Viene invece usato un modello molto più simile a una rete di messaggistica point-to-point. Sarà dunque il nodo notarile a informare direttamente le parti interessate dalla transazione.

Capitolo 3

Confronto con altre piattaforme

3.1 Corda: Blockchain o DLT?

All'interno di alcuni ambiti tra i quali quello finanziario, il termine blockchain è accompagnato dalla sigla DLT (Distributed Ledger Technology).
Essa indica la presenza di un "libro mastro", aggiornato, gestito, controllato e coordinato da tutti i nodi partecipanti alla rete.
Il "libro mastro" registra su record le transazioni tra due o più nodi in modo verificabile e permanente. I record permettono il collegamento di tutte le transazioni tra di loro e ogni transazione si collega alle precedenti che hanno determinato un output sul quale è stata effettuata quella corrente.
Sorge dunque spontanea la domanda sulla differenza tra blockchain e DLT. La differenza più importante tra le due è che la blockchain è un tipo di DLT: la blockchain impiega una catena di blocchi collegati tra loro e protetti da crittografia, per fornire il consenso al registro distribuito. La tecnologia a ledger distribuito, invece, non richiede l'utilizzo di una catena di blocchi. Inoltre, la DLT, offre migliori opzioni di scalabilità. La DLT è semplicemente un tipo di database distribuito su più siti, regioni o partecipanti. Si può dunque definire la blockchain come una particolare forma di DLT, in cui è possibile solo aggiungere dati al database distribuito. Importante è ricordare che tutte le blockchain sono DLT ma non tutti i DLT sono blockchain.
Solitamente Corda è descritta come una blockchain, ma alcune caratteristiche di questa piattaforma mostrano una maggiore somiglianza con una DLT:

- Le transazioni possono avvenire in parallelo, su nodi differenti, senza che

nessun nodo venga a conoscenza delle transazioni dell'altro.

- i nodi sono organizzati in una rete peer-to-peer autentica. Tutta la comunicazione è diretta all'interno di una rete.
- Corda non organizza il tempo in blocchi; dettaglio fondamentale che discosta la piattaforma dal basarsi su una blockchain. L'organizzazione dei blocchi è fornita da servizi notarili (pool) che astraggono il ruolo dei minatori in sistemi basati su blockchain.
- Non vi è alcuna trasmissione globale (broadcast) delle transazioni.

3.2 Corda VS Bitcoin

Corda ha alcune significative somiglianze con Bitcoin:

- Gli stati immutabili che vengono consumati e creati dalle transazioni sono gli stessi.
- Le transazioni hanno input e output multipli.
- Un contratto è una funzione pura; i contratti non hanno storage o la capacità di interagire con qualcosa. Dato lo stesso tipo di transazione, la funzione *verify()* di un contratto produce sempre esattamente lo stesso risultato.

Tuttavia, una transazione di Bitcoin ha un unico formato dati rigido e può contenere pochi dati oltre alle quantità di bitcoin e alle regole di spesa associate (script). Sono stati fatti dei tentativi per aggirare questa limitazione incorporando dati in posizioni semi-standardizzate nel codice del contratto, ma questa è un'approccio inefficace. Al contrario, gli stati in Corda possono includere dati di tipo arbitrario.
Inoltre, le transazioni fanno riferimento non solo ai contratti di input, ma anche ai contratti di output. In Bitcoin l'accettazione di una transazione è controllata solo dal codice del contratto negli stati di input. Il termine "contratto" fa riferimento a un insieme di logiche aziendali che possono gestire varie attività diverse, oltre alla verifica delle transazioni.
Attualmente i contratti in Corda includono anche il codice per la creazione di transazioni valide (questo è spesso chiamato "*Wallet Code*" in Bitcoin).

Uno script di Bitcoin può solo ricevere un insieme fisso di matrici di byte come input. Ciò significa che non c'è modo per un contratto di rappresentare la

struttura dell'intera transazione, il che ne limita l'uso che se ne può fare. I contratti in Corda possono essere scritti in qualsiasi linguaggio di programmazione ordinario che fa uso della JVM (Java Virtual Machine).
Corda consente di specificare limiti di tempo arbitrari per le transazioni (attestati da un timestamp fidato) anziché fare affidamento sul momento in cui un blocco viene estratto. Questo è importante dato che molti tipi di contratto che prevede di supportare richiedono precisione temporale e le implementazioni di consenso primarie utilizzano algoritmi di risoluzione dei conflitti senza blocco. È importante notare che Corda non utilizza la *Proof of Work* e non ha un concetto di "mining".

3.3 Corda VS Ethereum

Corda ed Ethereum sono due piattaforme blockchain con obiettivi e caratteristiche differenti.
Corda è progettata per applicazioni aziendali che richiedono la condivisione sicura di dati e l'esecuzione di transazioni tra parti identificate. Essa mira a consentire alle organizzazioni di collaborare in modo efficiente e sicuro riducendo gli intermediari e automatizzando i processi aziendali complessi. Inoltre in Corda solo le parti coinvolte direttamente nelle transazioni hanno accesso alle informazioni specifiche di quella transazione.
Ethereum, invece, è una piattaforma di sviluppo decentralizzata che consente la creazione e l'esecuzione di smart contract su una blockchain pubblica. L'obiettivo principale di Ethereum è fornire un'infrastruttura per la creazione di applicazioni decentralizzate (DApp) che possono eseguire codice personalizzato su una blockchain. Inoltre, consente a chiunque di partecipare alla rete come nodo e interagire con gli smart contract. Tutte le transazioni e i dati su Ethereum sono visibili a tutti i partecipanti della rete.
In conclusione, in entrambe il codice viene eseguito all'interno di una macchina virtuale e può contenere logiche complesse. Entrambi sono in grado di modellizzare diversi tipi di contratti finanziari, ma Ethereum è una piattaforma più ampia, non finalizzata solo a questo a differenza di Corda.

Capitolo 4

Conclusioni

4.1 Vantaggi di Corda

4.1.1 Sistema permissioned e privacy

Corda è un sistema permissioned, in cui solo una cerchia ristretta di utenti ha la possibilità di validare un blocco di transazioni. L'utente ha bisogno di essere sempre riconosciuto dal sistema, prima di procedere alla validazione. I vantaggi nell'utilizzo di questo sistema sono in termini di:

1. **privacy**: Corda sfrutta numerose tecniche per migliorare la privacy degli utenti, tra cui:

   - **Visibilità parziale dei dati:** le transazioni non sono trasmesse globalmente su tutta la rete
   - **Transaction tear-off:** le transazioni sono strutturate come Merkle trees quindi possono essere firmate senza che un nodo sia in grado di vederle completamente.
   - **Randomizzazione delle chiavi:** le chiavi utilizzate non sono collegabili in alcun modo all'identità del nodo.
   - **Cifratura:** lo sforzo primario per la gestione della privacy riguarda la gestione della cifratura dell'intero ledger, la quale deve prevedere i benefici della cifratura omomorfica e della zero-knowledge proof, ma senza sacrificare la scalabilità e le performance.

2. **scalabilità**: perché in grado di processare un gran numero di transazioni in parallelo.

3. **controllo di accesso** perché l'accesso ai dati all'interno del libro mastro è limitato in scrittura.

4.1.2 Applicazioni

Quanto descritto precedentemente rappresenta i punti di forza di Corda per cui ad oggi è una piattaforma molto utilizzata in settori come:

1. **Assistenza sanitaria**: questo campo si sta lentamente trasformando con l'uso di una soluzione DLT. È possibile utilizzare Corda per implementare le cartelle cliniche elettroniche (EHR), in cui la priorità è archiviare e facilitare i dati dei pazienti. Con la blockchain Corda per l'assistenza sanitaria, l'utente può interagire con l'EHR e conoscere i propri dati di rete decentralizzati. Anche altri membri, inclusi medici e professionisti, possono usufruire dei dati disponibili accedendovi con il permesso del paziente.

2. **Finanza**: il settore finanziario è stato il settore numero uno che utilizza la blockchain. Con Corda, si proteggono i dati dei clienti ed eseguono transazioni veloci. Migliora l'efficienza operativa dell'intera rete, con costi operativi ridotti e tempi di elaborazione migliori e aumenta la fiducia tra le istituzioni.

3. **Digital asset**: con l'aumento dei digital asset, è importante che le organizzazioni utilizzino una soluzione DLT in grado di gestire la trasformazione con un modo efficiente di archiviare, gestire ed elaborare tali risorse. Corda è un candidato perfetto perché garantisce scalabilità, sicurezza e controlli affidabili. Con Corda, è anche facile sviluppare sistemi di risorse digitali come le CBDC.

4. **Energia**: Corda sembra essere un'ottima scelta per il settore energetico considera l'energia come un digital asset, supportando il monitoraggio dei certificati energetici.

5. **Supply chain**: Corda può avere un monitoraggio accurato della posizione in tempo reale delle risorse nella catena di approvvigionamento offrendo a tutti gli stakeholder la trasparenza necessaria.

4.2 Svantaggi di Corda

Un primo svantaggio è rappresentato dal costo di un singolo nodo della rete; infatti Corda è stata ideata fin dal principio per gestire sistemi bancari e tutt'ora

mantiene le caratteristiche e i costi della rete originale.
Un altro motivo ma di minore importanza, è la conoscenza del linguaggio Kotlin. Non può essere considerata una vera e propria limitazione in quanto spesso è possibile applicare la controparte Java, come detto in precedenza. Essendo però Corda scritto in Kotlin, quest'ultimo risulta essere il linguaggio utilizzato maggiormente in molte repository di esempio, quindi non è considerato in termini di tempo l'apprendimento di un nuovo linguaggio.

Bibliografia

[1] Ian Grigg Mike Hearn Richard Gendal Brown James Carlyle. «Corda: An Introduction». In: (2016), pp. 1–15.

[2] Mike Hearn Richard Gendal Brown. «Corda: A Distributed Ledger». In: (2019), pp. 21–40, 50.

[3] Giacomo Greggio. «Blockchain per transazioni aziendali». In: (2018-2019).

[4] Corda. URL: https://corda.net/wp-content/uploads/2021/10/Corda_Overview_2021_R3.pdf.

RIPPLE

UNA PANORAMICA SULLA TECNOLOGIA E SUL SUO POTENZIALE

Cardellino Cecilia, D'Amico Lorenzo, Ferraro Luca, Gelsi Alessandro

Politecnico di Torino

Blockchain e criptoeconomia

Ripple: Una panoramica sulla tecnologia e sul suo potenziale

Cardellino Cecilia
D'Amico Lorenzo
Ferraro Luca
Gelsi Alessandro

Anno Accademico 2022–2023

Indice

1 Introduzione **3**

2 Il protocollo di consenso **5**
2.1 Deliberation 5
2.2 Validation 6
2.3 Preferred Branch 7
2.4 Analisi 9
2.4.1 Sicurezza 9
2.4.2 Liveness 10

3 XRP: Applicazioni e potenziale **13**
3.1 Ripple Inc. 13
3.2 XRP Ledger (XRPL) 13
3.3 XRP 14
3.3.1 Architettura della blockchain 14
3.3.2 Gli oggetti sul registro 16
3.3.3 Generazione e distribuzione XRP 17
3.4 Mitigazione dei possibili attacchi 18
3.5 I principali software 18
3.5.1 XCurrent 18
3.5.2 XVia 19
3.5.3 XRapid 20
3.5.4 Chi usa questo sistema? 20
3.6 XRP Ledger e Ethereum Virtual Machine 20

4 Ripple vs altre tecnologie **22**
4.1 Vantaggi e Svantaggi 22
4.1.1 Vantaggi 22
4.1.2 Svantaggi 22
4.2 Ripple/XRP vs Bitcoin 23
4.3 Ripple vs SWIFT 24

5 Limiti, controversie e vulnerabilità **25**
5.1 Contenziosi legali 25
5.2 Manipolazione del mercato: Pump and Dump 26

6 Conclusioni **28**

A Algoritmi **30**

Capitolo 1

Introduzione

La tecnologia Ripple è un insieme di protocolli, strumenti e soluzioni sviluppati da Ripple Labs Inc (società che si concentra sulla fornitura di soluzioni di pagamento e trasferimento di denaro basate su blockchain) per facilitare i pagamenti e i trasferimenti di denaro su scala globale. Ripple si basa su un approccio distribuito e utilizza una combinazione di tecnologie blockchain e di un sistema di consenso per raggiungere un accordo sulla validità delle transazioni. Ripple utilizza un protocollo di consenso, chiamato XRP Ledger Consensus Protocol. Questo protocollo consente ai partecipanti della rete di raggiungere un consenso sulla sequenza e l'integrità delle transazioni, senza richiedere un meccanismo di mining competitivo come nel caso del protocollo di consenso Proof-of-Work (PoW) utilizzato da Bitcoin. La tecnologia Ripple è stata sviluppata con l'intento di eliminare i ritardi e le inefficienze dei metodi convenzionali di pagamento, consentendo trasferimenti di denaro rapidi e economici. Ripple mira quindi a semplificare e velocizzare processi di liquidità e collaborazione fra istituzioni finanziarie per consentire ad esse di scambiarsi valute e effettuare pagamenti in tempo reale.

Ripple Labs Inc ha anche sviluppato la criptovaluta XRP. XRP È un token digitale che è possibile trasferire e scambiare attraverso la rete Ripple. Per facilitare i trasferimenti di valore tra valute, XRP funge da ponte di liquidità, serve come mezzo di scambio immediato per un trasferimento, evitando intermediari e velocizzando le transazioni. Grazie alla sua velocità e bassi costi di transazione e alla sua capacità di facilitare la liquidità in tempo reale, XRP è diventato piuttosto popolare nel settore finanziario. Tuttavia, è importante notare che la centralizzazione di Ripple e XRP e la questione della loro legalizzazione come titoli finanziari sono stati oggetto di controversie e contenziosi. Al momento della scrittura di questo studio, il valore Ripple XRP è 0.3942 €. Il volume di scambio a 24 ore di XRP è di 373,684,202 €. XRP è attualmente classificato sesto fra tutte le criptovalute per capitalizzazione di mercato totale, con una capitalizzazione di mercato di 22,902,774,491 €. Ha una fornitura circolante di XRP 51,837,820,505 e l'offerta massima è di 100 miliardi di XRP di cui solo circa 45 miliardi destinati al mercato libero, mentre la restante parte è posseduta da Ripple stesso.

In questo lavoro presentiamo una panoramica sulla tecnologia Ripple e sulla relativa criptomoneta XRP mettendone in luce potenziale, punti di forza, così come criticità e debolezze. Innanzitutto esponiamo una descrizione e un analisi del protocollo di consenso (capitolo 2), tale protocollo è il pilastro fondamentale per comprendere il funzionamento

del sistema Ripple. Nel capitolo 3 approfondiamo XRP evidenziando le sue applicazioni principali ed esaminiamo l'architettura della blockchain. Successivamente (capitolo 4) si propone un confronto fra Ripple e alcune tecnologie tradizionali con l'intento di studiare le potenzialità e le criticità di Ripple quando comparato con altri consolidati (SWIFT, bitcoin). Infine nel capitolo 5 sono descritti alcuni dei principali problemi che potrebbero rappresentare un limite per la diffusione di Ripple e XRP.

Capitolo 2

Il protocollo di consenso

Il protocollo di consenso Ripple è stato proposto per la prima volta nel white paper [1], tuttavia tale articolo non presenta lo stato attuale del protocollo, pertanto le prossime pagine descriveranno la versione aggiornata XRP Ledger Consesus Protocol (da ora in poi **XRP LCP**) descritta in [2]. XRP LCP è un protocollo di consenso bizantino a bassa latenza che opera su una rete distribuita peer-to-peer, in grado di raggiungere un consenso senza aver bisogno che tutti i nodi della rete diano l'approvazione. Nel protocollo, ogni nodo P_i è identificato univocamente da un indice i. Ogni nodo può scegliere di far parte di una lista unica di nodi chiamata **Unique node list** (UNL_i) che è l'insieme di nodi (incluso P_i) dei quali P_i si fida. Per ogni nodo P_i la cardinalità di UNL_i è $n_i = |\text{UNL}_i|$, mentre il **quorum** q_i è il minimo numero di conferme che P_i deve ricevere da UNL_i. in modo da raggiungere consenso. Un nodo può far parte di più UNL, il che gli garantisce più influenza nella rete. In figura 2.1 si possono osservare due UNL e la sovrapposizione tra di loro, vedremo successivamente che la sovrapposizione tra coppie di UNL è molto importante per garantire la sicurezza del protocollo. Inoltre, come si può anche osservare dalla figura 2.2, non è detto che la fiducia sia reciproca, ovvero può esserci un nodo $P_c \in \text{UNL}_i$ tale che $P_i \notin \text{UNL}_c$. Un nodo che si comporta seguendo il protocollo viene definito **onesto**, mentre un nodo che non lo fa prende il nome di **bizantino**. Ogni nodo P_i imposta $q_i = 0.8n_i$. Essendo la rete peer-to-peer, per poter considerare validi solamente i messaggi provenienti dal proprio UNL, tutti i messaggi sono crittograficamente firmati e verificati dal nodo ricevente. L'obiettivo del protocollo è quello di validare dei registri, ovvero i blocchi di una blockchain contenenti una serie di transazioni **ordinate** $T = [x_0, x_1, ...]$. Successivamente il termine blocco sarà usato in maniera interscambiabile con i termini registro e ledger. Ogni blocco ha un numero di sequenze $seq(L)$ che è il numero di sequenza del blocco genitore incrementato di 1, dove il numero di sequenza del blocco di genesi è 1. Il protocollo si compone di tre componenti principali che verranno ora descritte.

2.1 Deliberation

La **Deliberation** è la fase nella quale i nodi presentano le transazioni ad altri nodi, che le inviano in broadcast al resto della rete. I nodi mantengono un insieme di transazioni in sospeso che non sono state ancora incluse in un blocco. Un nodo inizia il processo

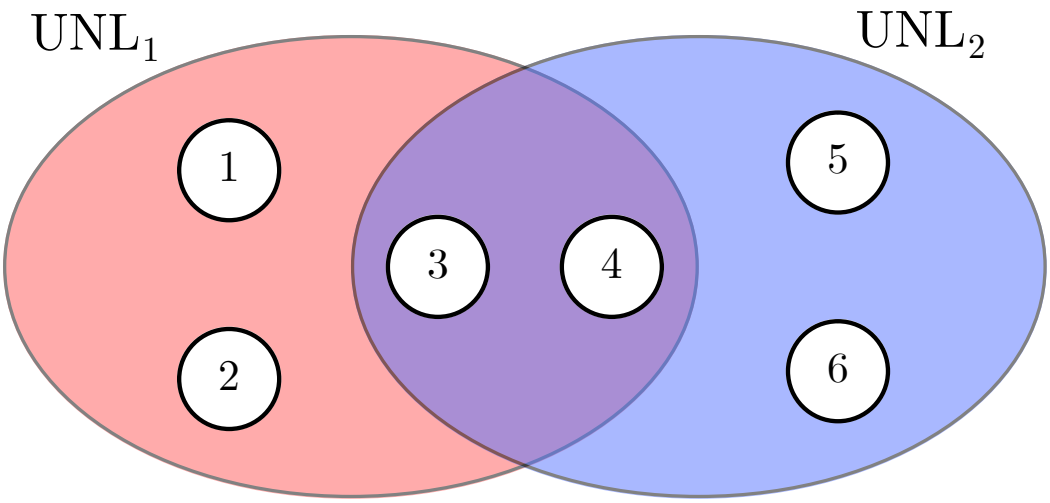


Figura 2.1: Esempio di due UNL con sei nodi. $UNL_1 = \{1,2,3,4\}$, $UNL_1 = \{3,4,5,6\}$. I nodi 1 e 2 si fidano della UNL_1, mentre i nodi 5 e 6 si fidano della UNL_2, 3 e 4 si fidano di entrambe le UNL. Da notare come 3 e 4, essendo in un'intersezione e facendo quindi parte di entrambe le UNL hanno più influenza del resto dei nodi.

di deliberazione e invia la sua lista di transazioni da applicare all'ultimo blocco L della catena. Il blocco riceve dalla sua UNL nuove proposte di transazioni e regolarmente aggiorna la sua proposta iniziale includendo le transazioni ricevute da almeno $threshold(r)$ insiemi di transazioni ricevute dai nodi di cui si fida, dove r è il round di aggiornamenti eseguiti fino a quel momento per il blocco L. La threshold aumenta con l'aumentare di r (0.5 -> 0.65 -> 0.70 -> 0.95) in modo da non compromettere la convergenza da parte di nodi lenti. Ogni nodo P_i dichiara che il consenso è stato raggiunto quando q_i nodi fidati concordano con l'insieme delle transazioni. A questo punto P_i genera il nuovo blocco, invia un messaggio di validazione, e parte con un nuovo round di deliberazione. Gli algoritmi sono stati riportati nell'appendice. L'algoritmo di Deliberazione è osservabile in 3.

2.2 Validation

La validazione è un processo molto semplice per il quale nodi restano in ascolto per ricevere messaggi di validazione da altri nodi fidati. Se un nodo P_i vede q_i validazioni per un blocco L, allora aggiunge un nuovo blocco $\hat{L}$ a L nella catena. L'algoritmo di validazione si può osservare in 1.
In altre parole, quello che accade in questi due passi (Deliberation e Validation) è che ogni nodo propone un insieme di transazioni che vuole includere nel prossimo blocco, i nodi aggiungono una transazione al loro insieme solo se una certa percentuale di altri nodi fidati invia tale transazione, al contrario elimina una transazione dal suo insieme se non viene proposta abbastanza dagli altri nodi. Quando il numero di nodi che concordano con l'insieme di transazioni è superiore al quorum, allora viene preparato il

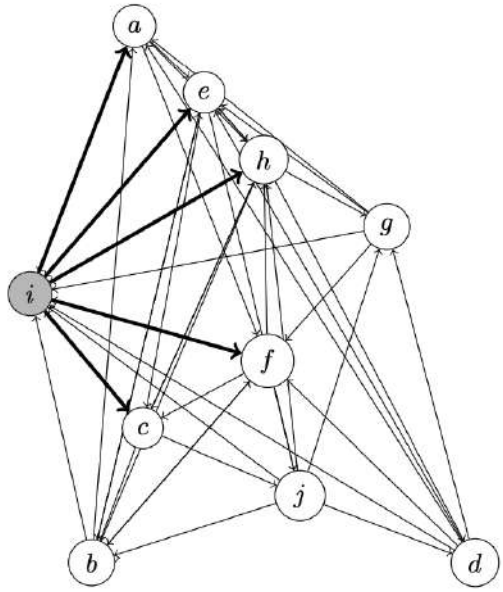


Figura 2.2: Rappresentazione grafo di diversi UNL. I vertici più spessi rappresentano l'UNL del nodo P_i

blocco e chiesta la validazione. Se un nodo vede arrivare per lo stesso blocco un numero di validazioni che supera l'80% del numero di nodi del suo UNL, allora valida il blocco e lo inserisce alla catena. Questo meccanismo garantisce il consenso fin quando meno del 20% dei nodi fidati fallisce.

2.3 Preferred Branch

Preferred Branch (Ramo preferito in italiano) è il meccanismo con il quale un nodo sceglie un blocco e continua la catena nel caso in cui ci siano blocchi che entrano in conflitto tra di loro, generando pertanto una "fork". Questo è dovuto alla natura asincrona della rete, ma anche da possibili fallimenti bizantini. Il metodo è basato sui seguenti valori:

1. Il **tip support** (supporto della punta in italiano) di un blocco L, che è il numero dei nodi fidati per i quali l'ultimo blocco validato è L, viene definito come:

$$supp_{tip}(L) = |\{V_{L',i} \in lastVals : L = L'\}| \tag{2.1}$$

   dove $lastVals$ è l'insieme degli ultimi blocchi validati.

2. Il **branch support** (supporto del ramo) di un blocco L, che è il numero dei nodi fidati per i quali l'ultimo blocco validato è L, oppure discende da L (cioè un blocco che è stato validato dopo di L nella catena), viene definito come:

$$supp_{branch}(L) = supp_{tip}(L) + |\{V_{L',i} \in lastVals : L = ancestors(L')\}| \tag{2.2}$$

   dove $ancestors(L')$ è l'insieme degli antenati di L', fino al blocco di genesi.

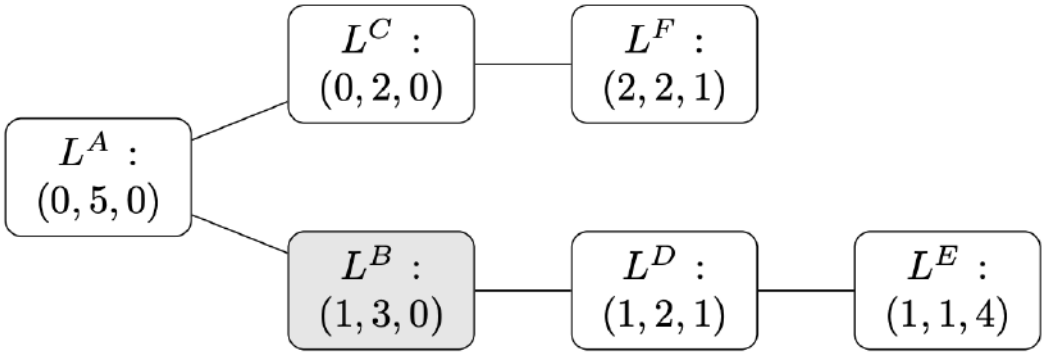


Figura 2.3: Esempio di una fork

3. L'**uncommited support** (supporto non legato in italiano) su un numero di sequenza s, che è il numero di nodi fidati per i quali il blocco validato più recentemente ha un numero di sequenza più piccolo di s oppure più piccolo del blocco con il numero di sequenza più grande per il quale abbiamo personalmente mandato la validazione in broadcast, viene definito come:

$$uncommited(s) = |\{V_{L',i} \in lastVals : seq(L') < max(s, seq(L))\}| \tag{2.3}$$

Il ramo preferito viene scelto a partire dal blocco che è l'antenato comune. Si seleziona poi il blocco $L' \in children(L)$ con il più alto supporto del ramo che avrebbe il maggior supporto anche se tutti i $uncommited(seq(L'))$ nodi scegliessero un blocco conflittuale. Se non fosse possibile trovare un blocco tra i figli di L con queste caratteristiche, allora L è il blocco preferito. Se invece è possibile, ripetiamo lo stesso processo con quest'ultimo. Per rompere eventuali situazioni di pareggio, il protocollo utilizza una funzione $\phi(L', L'')$ che restituisce 1 se l'hash di $L' > L''$, 0 altrimenti. Inoltre, se il blocco L trovato come preferred branch è un antenato del blocco corrente $\tilde{L}$ che un nodo sta considerando, questo mantiene $\tilde{L}$ come preferred dal momento che non c'è modo di sapere quale sia il ramo giusto. Intuitivamente, un nodo cambia ramo solamente quando sa che abbastanza nodi si sono impegnati a una catena di blocchi in modo che una catena alternativa non può avere più supporto. L'algoritmo di Preferred Branch è osservabile in 2. Per comprendere meglio l'algoritmo, supponiamo di trovarci nell'esempio in figura 2.3 e di essere un nodo che ha validato come ultimo blocco il blocco L^F. Ogni blocco ha associata una tupla di tre numeri, che sono rispettivamente $supp_{tip}$, $supp_{branch}$ e *uncommitted*. Ci sono 5 blocchi di cui il nodo si fida, di cui 2 hanno validato per ultimo L^F, mentre gli altri 3 hanno validato per ultimo rispettivamente L^B, L^D e L^E come si può osservare dal primo valore della tupla. Il nodo fa partire l'algoritmo di preferred branch e parte dal blocco da cui nasce la fork, ovvero L^A. I due blocchi figli di L^A sono L^B (1,3,0) e L^C (0,2,0). Tra questi vede quello che ha supporto di ramo maggiore in questo caso L^B perché $3-2+\phi(L^B, L^C) = 2$ (suppondendo $\phi(L^B, L^C) = 1$)

. Tuttavia si assicura che avrebbe supporto maggiore anche se tutti i nodi che non sono ancora arrivati a validare il blocco che stiamo considerando scegliessero l'altro ramo, cioè L^C. Come detto in precedenza questo numero è $uncommited(seq(L^B))$, che in questo caso è $max(0, 1)$ perché non ci sono nodi che hanno validato un blocco con numero di sequenza minore e $uncommited(seq(L^F)) = 1$. Quindi si ha che il blocco scelto è L^B (2>1). Si continua con il processo e si prendono i figli di L^B, ovvero solamente L^D (1,2,1). Seguendo il ragionamento di prima si prende il supporto di ramo di D, cioè 2, e si controlla se si ha supporto maggiore di $uncommited(seq(L^D))$, che è uguale a 1. Viene perciò scelto L^D e si procede nella catena con L^E (1,1,4). $uncommited(seq(L^E))$ = 4, ma $1 < 4$ quindi il nodo si ferma qui e, dal momento che l'ultimo blocco che lui ha validato (L^F) non è un antenato di L^D, il nodo abbandona L^F per scegliere L^D come preferred branch.

2.4 Analisi

Avendo descritto XRP LCP dal punto di vista del protocollo, ora si vogliono formalmente riportare dei risultati relativi alla sua sicurezza e liveness, cioè la proprietà che assicura che il sistema non si blocchi e che possa continuare a progredire nel raggiungimento di consenso.

2.4.1 Sicurezza

In questa sezione si dimostrano le condizioni di configurazione della rete che garantiscono che i diversi nodi che eseguono XRP LCP restino coerenti. Per tutta la fase di analisi risulta conveniente assumere che la convalida completa di un registro non convalidi completamente i suoi antenati. Per procedere poi con la fase iniziale della valutazione è necessario fare un'ulteriore ipotesi esemplificativa, denominata **Byzantine accountability**. Si assume che un nodo difettoso bizantino non può convincere due nodi onesti che ha convalidato ledger diversi. Questa viene giustificata dall'idea che tutta la comunicazione avviene tramite multicast generico su una rete peer-to-peer, così che gli "eco" di due messaggi contraddittori verrebbero notati in tempo per ignorare il messaggio, in quanto i messaggi sono firmati. Tuttavia questa ipotesi non regge in una rete completamente asincrona, poiché una partizione di rete potrebbe isolare i messaggi contraddittori per un periodo sufficientemente lungo da provocare danni. Per segregare si intende che questi messaggi possono essere divisi o separati in diverse parti della rete a causa di una partizione di rete. Una partizione di rete si verifica quando una rete viene divisa in più segmenti isolati a causa di problemi di connettività o guasti nella comunicazione tra i nodi. Due messaggi contraddittori vengono inviati contemporaneamente su segmenti diversi a causa di una partizione di rete, portando alcuni nodi potrebbero ricevere un messaggio che afferma una cosa, mentre altri nodi potrebbero ricevere un messaggio contrario. Questa situazione potrebbe indurre a comportamenti imprevisti e dannosi per il sistema. Pertanto, l'assunzione di base che tutti i nodi ricevano tutti i messaggi in modo tempestivo e che i messaggi contraddittori vengano rilevati e ignorati non è valida in una rete completamente asincrona, in cui le partizioni di rete possono isolare i messaggi e ritardare la loro consegna, consentendo potenziali danni o comportamenti indesiderati. Assumendo che l'ipotesi sia valida come accade nel white paper

originale [2], si procede analizzando quando è possibile per due nodi convalidare completamente registri diversi in un singolo round di consenso. Sia $O_{i,j} = |\text{UNL}_i \cap \text{UNL}_j|$ (ovvero la sovrapposizione tra i due UNL), si ha che P_i, P_j non possono convalidare completamente registri in conflitto se:

$$O_{i,j} \geq max\{n_i - q_i, n_j - q_j\} \tag{2.4}$$

Che, con un quorum di 0.8, può essere riscritta come:

$$O_{i,j} \geq 0.2max\{n_i, n_j\} \tag{2.5}$$

In altre parole, il protocollo non può generare fork nel caso in cui la sovrapposizione per ogni coppia di UNL nella rete sia superiore al 20%. In analisi successive Armknecht [3] propone che P_i, P_j non possono convalidare completamente due registri differenti *se e solo se*

$$O_{i,j} > 2max\{n_i - q_i, n_j - q_j\} \tag{2.6}$$

È vero che se la condizione sopra indicata è valida, allora P_i e P_j non possono convalidare completamente registri diversi. Il contrario non è tuttavia vero come dimostra la seguente proposizione: *Proposizione 1:* Assunta l'ipotesi di Byzantine accountability, due nodi onesti P_i e P_j non possono convalidare completamente registri diversi con lo stesso numero di sequenza se

$$O_{i,j} > n_i - q_i + n_j - q_j \tag{2.7}$$

Si noti che $2max\{n_i - q_i, n_j - q_j\} \geq n_i - q_i + n_j - q_j$, ma $n_i - q_i + n_j - q_j$ è strettamente minore ogni volta che $n_i - q_i \neq n_j - q_j$. Quindi, la condizione suggerita da Armknecht è sufficiente ma non necessaria. Assumendo un quorum dell'80%, la condizione di sovrapposizione può essere riassunta nel seguente modo: Ogni coppia di nodi necessita di una sovrapposizione del 41% rispetto alla dimensione media delle rispettive UNL.
Da questo punto in poi non viene più assunta l'ipotesi di Byzantine accountability. In una rete attiva infatti è preferibile avere una sicurezza assoluta anziché fare affidamento ad euristiche fragili che si basano sul fatto che è improbabile che un nodo bizantino possa inviare messaggi contrastanti a nodi diversi senza essere scoperto. Pertanto ora si assume che i nodi bizantini possano inviare messaggi arbitrari a nodi arbitrari. Per ogni coppia di nodi P_i e P_j, sia $t_{i,j} = min\{t_i, t_j, O_{i,j}\}$. $t_{i,j}$ è il massimo numero di fallimenti bizantini in $\text{UNL}_i \cap \text{UNL}_j$, assumendo al massimo t_i fallimenti in UNL_i e al massimo t_j in UNL_j.
È dimostrato che XRP LCP non può originare fork se $O_{i,j} > n_j/2 + n_i - q_i + t_{i,j}$ per ogni coppia di nodi P_i, P_j. Nella pratica, questo ci porta a richiedere circa una sovrapposizione per ogni coppia di UNL maggiore del 90% della dimensione massima dei rispettivi UNL assumendo sempre 0.8 di quorum. Questo valore è molto più alto di quelli che si era creduto originariamente nel white paper [1] (20%) e quello trovato nella successiva analisi [3] (41%).

2.4.2 Liveness

Ora che si ha una metrica concreta per capire quando è impossibile per la rete creare una fork, si va ad analizzare quando questa può fare progressi. Il fatto che una rete

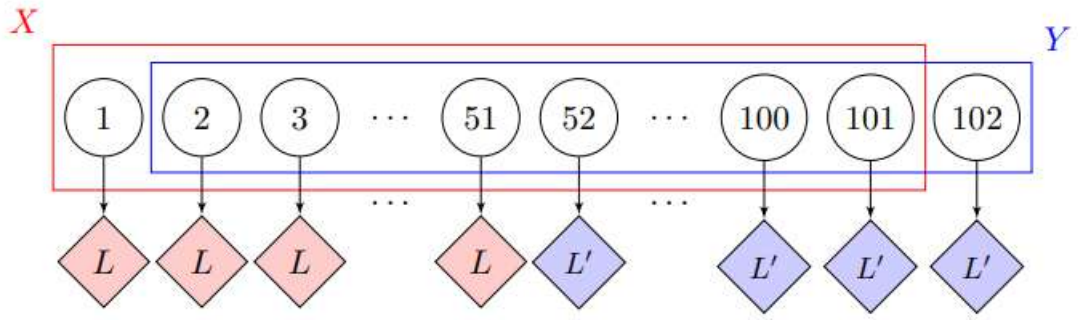


Figura 2.4: Esempio di una rete bloccata con una sovrapposizione dell'UNL del 99% e senza fallimenti bizantini.

attiva smetta di fare progressi rischia di essere ancora più dannoso della fork stessa, a causa della necessità delle aziende di effettuare trasferimenti in tempo. Purtroppo, come riportato da FLP [4], è impossibile garantire un progresso costante in una rete completamente asincrona.
Si vuole quindi almeno poter dimostrare che la rete non rischia di rimanere "bloccata", ovvero che la rete non può entrare in uno stato in cui alcuni nodi onesti non possono mai convalidare completamente un nuovo registro.
Complessivamente risulta molto difficile in generale garantire un progresso costante con XRP LCP. L'esempio seguente mostra che è possibile rimanere bloccati anche con sovrapposizioni delle UNL del 99% e senza fallimenti bizantini.

Esempio

Si consideri la rete di 102 partecipanti raffigurata in 2.4 Ci sono due UNL, il primo in rosso $X = \{P_1, P_2, ..., P_{101}\}$, il secondo in blu $Y = \{P_2, P_3, ..., P_{102}\}$. I partecipanti da 1 a 51 usano X mentre i partecipanti da 52 a 102 usano Y. Ci sono due registri, L e L'. I nodi che ascoltano X convalidano tutti un discendente di L, mentre i nodi che ascoltano Y convalidano tutti un discendente di L'. Dato che $51 > 0.5|Y|$ i nodi in X convalidano un discendente di L. Quindi, secondo il protocollo preferred branch, i nodi che ascoltano X non possono passare alla diramazione L'. Allo stesso modo, poiché $51 > 0.5|Y|$ i nodi in Y convalidano tutti un discendente di L, i nodi che ascoltano Y non possono passare al branch L'. La rete non può mai riunirsi senza un intervento manuale.
Il modello di fiducia raccomandato per XRP prevede che tutti i nodi ascoltino o una singola lista unica di nodi (UNL) composta da 5 nodi, oppure una UNL composta da questi 5 nodi più un nodo extra (tipicamente il nodo extra è se stesso; i nodi che ascoltano queste UNL estese vengono chiamati "foglie", poiché si diramano leggermente dalla rete principale). Il piano a breve termine per la decentralizzazione prevede l'ampliamento a una UNL più grande, ma ancora concordata e la diversificazione degli operatori di nodi. Perdere progressi mentre si passa a una nuova lista di nodi non è un grosso problema (poiché non appena tutti concordano nuovamente sulla lista dei nodi, il pro-

gresso riprenderà, e la sezione precedente garantisce che per "piccoli" cambiamenti non si verificherà una fork durante l'intervallo di tempo); pertanto, dimostrando che la rete non può rimanere bloccata in un grafo completo con le foglie, si può ottenere almeno un risultato positivo.

Capitolo 3

XRP: Applicazioni e potenziale

3.1 Ripple Inc.

La **Ripple Inc.** è l'azienda statunitense nata nel 2012 e fondata da Jed McCaleb, Chris Larsen, Ryan Fuggercon che elaborò il protocollo e la criptomoneta XRP. La **RippleNet** è la rete su cui si basa il servizio fornito da questa compagnia privata. Può costituire la spina dorsale di tutti i servizi e prodotti che può offrire un qualsiasi istituto di credito che utilizza questa tecnologia.

3.2 XRP Ledger (XRPL)

La **XRP Ledger (XRPL)** è una piattaforma open source che utilizza il XRP Ledger Consensus Protocol come metodo di convalida delle transazioni. Questo sistema si serve di qualche decina di validatori ufficiali delle transazioni, gestiti da università, exchange, imprese e privati in tutto il mondo. Grazie a questo meccanismo la rete può sopportare fino a 1500 transazioni al secondo con velocità di conferma compresa tra i 3 e i 5 secondi. Possiamo interpretare il XRPL come il "*libro mastro*" della moneta nativa **XRP**. Quindi le sue applicazioni sono:

- **Pagamenti:** Si possono spostare asset finanziari in tutto il mondo a prezzi irrisori, è anche possibile creare un wallet XRP (come Xumm) ed effettuare transazioni direttamente in XRP.
- **Tokenizzazione**: Qualsiasi tipo di asset può essere tokenizzato su XRP Ledger, compresi i token fungibili, le stablecoin e le Central Bank Digital Currency (CBDC). Ad oggi sono state emesse più di 5400 valute, che vengono scambiate su XRPL.
- **DeFi** : esiste la possibilità di fare trading direttamente su XRPL usando il suo exchange decentralizzato (DEX).
- **Stablecoin** : è inoltre possibile emettere dei token legati a delle attività di riserva stabili su XRPL. Infatti questi token possono essere supportati da valute fiat su un conto bancario con un tasso di cambio *stabile* a 1 : 1. In generale gli emittenti di

stablecoin sono aziende che collegano i token nel registro XRP ad asset nel mondo esterno, in modo da poter beneficiare di tutti i servizi Ripple essendo sicure di non perdere denaro durante il cambio.

3.3 XRP

La **XRP** è un asset digitale nativo di XRP Ledger che permette a tutto l'ecosistema digitale di Ripple di funzionare in modo organico e omogeneo. Basta possedere una connessione ad internet ed un wallet digitale per fare uso dei token XRP. Un XRP wallet è un asset bridge neutrale ottimizzato per pagamenti globali a commissioni ridotte.

- Uno dei principali usi è quello di permettere ***trasferimento di denaro*** tra privati, ma sopratutto tra istituti di credito a tempo praticamente nullo e a prezzi irrisori. Ripple converte qualsiasi valuta, anche quelle meno comuni, in un token XRP, che attraverso la RippleNet, viaggia in pochi secondi al destinatario, che a questo punto riceverà il denaro riconvertito nella sua valuta locale, con costi limitati e nel giro di qualche secondo. In pratica permette di effettuare pagamenti ***transfrontalieri***, ottimizzando problemi come cambio di valuta e lunghi tempi di conferma tipici delle tecnologie tradizionali.

- Questa criptomoneta non è usata solo dagli istituti di credito per gli spostamenti di denaro, ma si può comprare e usare come una vera e propria valuta. Ad oggi però questo uso non è rilevante, la compravendita avviene principalmente a scopo di ***investimento***.

- Un'altro uso è quello di effettuare transazioni sull'exchange decentralizzato (DEX) che permette di effettuare transazioni ***DeFi***, ciè tutte quelle transazioni fonite dalle tipiche banche fisiche ma in un ambiente sicuro e decentralizzato. Il DEX è nativo del protocollo e utilizza un modello a limit order book centralizzato per negoziare gli asset digitali.
  L'utilizzo principale di questa tecnologia è quello di fare trading.

- Con i token XRP è possibile ***acquistare NFT***. In pratica con i token XRP sarà possibile sbloccare tutte le funzionalità legate agli NFT, come il minting, il trading e il burning, le royalties automatiche per i creator e la comproprietà degli asset..

3.3.1 Architettura della blockchain

La XRPL processa le transazioni in blocchi chiamati **Ledger versions** o semplicemnete **Ledger** (registri), che contengono lo stato di tutti i conti e oggetti salvati nella ledger, l'insieme di transazioni aggiunte e alcuni metadati come un indice (numero di sequenza), e un hash crittografico basato sul contenuto della ledger e di quella precedente. A differenza di molte altre criptovalute, ogni blocco della ledger contiene completamente lo stato corrente, in modo che possa essere recuperato velocemente. Nella XRPL, una firma digitale autorizza una transazione a eseguire un insieme specifico di azioni. Solo le transazioni firmate possono essere inviate alla rete e incluse in un registro validato. Per firmare digitalmente, è necessaria una coppia di chiavi, una privata e una pubblica.

Una coppia di chiavi è ottenuta a partire da un **seed**, che deve essere random e segreto. Un seed può opzionalmente essere generato da una **passphrase**, il quale utilizzo è altamente sconsigliato per motivi di sicurezza ma è stato lasciato per casi d'uso di nicchia. XRPL è **Account-based**, cioè ogni partecipante possiede un account identificato da un **Accound ID** e può inviare e ricevere XRP tramite transazioni che coinvolgono gli account. L'Account ID è ottenuto a partire dalla chiave pubblica ed è lungo 20 byte. L'account può essere di due formati: **Classic address** che è semplicemente l'account ID codificato in base58 con un checksum, e l'**X-Address** che combina un Account ID e un **Destination Tag**, prima di fare la codifica base58 e aggiungere il checksum. Il checksum è molto importante dal momento che se viene fatto un errore di battitura sull'indirizzo non verrà eseguita una transazione su un indirizzo sbagliato. Il **Destination tag** è un identificatore numerico utilizzato per associare una transazione a un destinatario specifico. È un campo opzionale che può essere incluso quando si inviano XRP a determinati exchange o servizi che richiedono informazioni aggiuntive per accreditare i fondi al corretto conto utente. Questo è particolarmente utile per le piattaforme che utilizzano un singolo indirizzo del ledger XRP per ricevere fondi per conto di più utenti. Il destination tag non ha nessun uso diretto su XRPL, ma fornisce importanti informazioni sul come i sistemi al di fuori dovrebbero processare i pagamenti. Proprio come i destination tag, esistono anche i **Source tag**, che indicano la sorgente di un pagamento, cosi che un ricevente conosce l'indirizzo a cui inviare un eventuale rimborso. Questo metodo permette l'utlizzo di un singolo account per gestire diversi indirizzi in maniera leggera.
Le coppie di chiavi possono essere di due tipi:

- **Regular key pair**, ovvero una coppia di chiavi utilizzabile per autorizzare le transazioni normalmente (con alcune eccezioni che richiedono permessi maggiori). Questa coppia di chiavi può essere rimossa o rimpiazzata in qualsiasi momento senza ripercussioni sullo stato dell'account. È buona pratica cambiarla spesso.

- **Master key pair** dalla quale viene derivato l'indirizzo dell'account. Questa coppia non può essere eliminata e la sua conoscenza implica il pieno controllo sull'account ad essa collegato, per questo non andrebbe usata per eseguire transazioni (nonostante questo sia possibile) e andrebbe mantenuta offline. Inoltre può essere anche disattivata. La master key pair deve essere usata necessariamente per la prima transazione, in modo da inizializzare l'account. È l'unica che può disabilitaee l'account ed eseguire ulteriori operazioni speciali. Se un malintenzionato scoprisse la regular key pair, si può abilitare la master key pair e immediatamente cambiare la regular.

XRPL usa due algoritmi di firma, il primo è **ECDSA** sulla curva ellittica secp256k1, ovvero lo stesso meccanismo che utilizza Bitcoin. Il secondo è EdDSA con la curva ellittica Ed25519 [5], che è un algoritmo con performance e proprietà migliori. Dal momento che le chiavi pubbliche di Ed25519 sono un byte più corte, a queste viene prefisso il byte 0xED così da distinguerle e per fare in modo che entrambe siano di 33 byte.

3.3.2 Gli oggetti sul registro

Per evitare che la rete cresca eccessivamente e venga usata per scopi maliziosi e per poter mantenere tutto il registro in RAM, XRPL ha un **requisito di riserva** per poter permettere a un utente di mantenere un account, ovvero ogni account deve ricevere un minimo di XRP per poter avere un nuovo indirizzo utilizzabile nella rete. Questa riserva non può essere inviata a nessuno, ma cancellare un account permette di recuperarne alcuni. La riserva è composta da due parti, la **Base reserve** che è un minimo di XRP richiesti per ogni indirizzo, e la **Owner reserve**, che è un minimo di XRP per ogni oggetto che l'indirizzo possiede sul registro. I requisiti possono cambiare mediante una votazione da parte dei validatori, e al momento della scrittura di questo studio i requisiti di riserva sulla rete principale sono di 10 XRP per la **Base reserve**, e 2 XRP per oggetto per la **Owner reserve**. Gli oggetti che si possono essere presenti sul registro sono molteplici, tra queste troviamo:

- **NFT pages** ovvero le pagine che contengono NFT. Tali pagine possono contenere fino ad un massimo di 32 NFT.

- **NFT offers** XRPL offre la possibilità di fare offerte di vendita di NFT (NFTokenSellOffer) e offerte di acquisto (NFTokenBuyOffer), che contano come oggetti nel registro. Per creare una NFTokenSellOffer bisogna eseguire una transazione "NFTokenCreateOffer" con il tfSellToken flag. Si compone dell'ID del token che si vuole vendere e il prezzo, insieme a una data di scadenza e a un account di destinazione, che sarà l'unico a poter accettare l'offerta. Una NFTokenBuyOffer si crea allo stesso modo, ma omettendo il tfSellToken flag, e inserendo l'account del properitario, l'ID dell' NFT e il prezzo dell'offerta. Per accettare un offerta si deve usare la transazione "NFTokenAcceptOffer". L'acquisto di un NFT può avvenire direttamente tra venditore e acquirente (direct transaction), oppure può passare tramite un terzo (brokered transaction) che guadagna una quota sulla vendita. Il motivo delle brokered transaction sta nel fatto che questa terza entità può agire come agente di vendita per diversi venditori, occupandosi lui del processo di ricerca di un acquirente.

- **Offer** cioè un'offerta di scambio di valuta, che viene creata con una transazione "OfferCreate" e resta nel registro se non può essere soddisfatta da altre offerte esistenti. Le Offerte che non possono essere soddisfatte, per mancanza di fondi ad esempio, vengono eliminate dalla rete quando vengono elaborate le transazioni.

- **Checks** ovvero degli assegni, che permettono agli utenti di creare pagamenti differiti che possono essere cancellati o incassati dai riceventi. Esattamente come un vero assegno, gli XRP non venogno trasferiti finché l'assegno non viene incassato, e questa operazione può quindi fallire nel caso in cui il mittente non abbia abastanza liquidità. L'assegno può anche avere una data di scadenza, ma l'oggetto rimane finchè qualcuno non lo cancella.

- **Escrow** cioè depositi di garanzia. Sono pagamenti di XRP condizionali, mettono da parte degli XRP e li inviano quando sono soddisfatte alcune condizioni. Per inviare un escrow, bisogna creare una transazione del tipo "EscrowCreate" con

una data di scadenza per bloccare alcuni XRP, e definire delle condizioni che possono essere basate sul tempo oppure delle **crypto-condition**, cioè condizioni che devono essere valide perché lo sia anche la transazione. Dopo aver inviato questa transazione, il registro conterrà un oggetto escrow con gli XRP bloccati. Il ricevente invia quindi una transazione "EscrowFinish", che gli permette di ricevere gli XRP solo se tutte le condizioni sono soddisfatte, andando a distruggere l'oggetto dal registro. L'operazione restituisce errore se però l'escrow è già finito, e il mittente deve inviare una transazione "EscrowCancel" per poter riottenere gli XRP. XRLP quindi non usa smart contracts, ma gli escrow con le crypto-condition sono la cosa che vi si avvicina di più.

- **Ticket** cioè un modo per fare una transazione senza inviarla subito. Le transazioni infatti hanno un numero di sequenza unico, in modo da evitare il double spending. Il Ticket è una transazione con un numero di sequenza al di fuori del classico ordine, mettendolo da parte. Questo è molto utile soprattutto per firme multiple sulla stessa transazione, infatti non puoi usare numeri di sequenza successivi a una transazione finché tutti non hanno firmato quella prima. Un altro caso d'uso nasce quando più utenti condividono lo stesso account, se mandano una transazione insieme è probabile che usino lo stesso numero di sequenza, facendone fallire una. Ancora, i ticket sono utili nel caso in cui vuoi preparare e firmare una transazione prima e inviarla successivamente, continuando ad usare normalmente il tuo account numerando le transazioni sequenzialmente. Il ticket risolve tutti questi problemi mettendo da parte dei numeri di sequenza da usare dopo, al di fuori dell'ordinamento classico.

- **Signer list** cioè un insieme degli indirizzi che possono autorizzare una transazione dal proprio indirizzo. Queste liste vengono create mediante la transazione "SignerListSet" e può avere dagli 1 ai 32 indirizzi, che sono unici e diversi dal proprio. Si può impostare di quante firme c'è bisogno, e anche in che ordine. Inoltre gli indirizzi in una lista possono avere più o meno peso e può essere definito un **quorum**, cioè il minimo peso totale per autorizzare la transazione. Ogni elemento della lista inoltre può avere 256 bit di dati in più, che può essere usato arbitrariamente

- **Owner Directory** che è un cas speciale di oggetto, perché non contribuisce ai requisiti di risorsa. È una lista di tutti gli oggetti relativi a un account, insieme a tutti gli oggetti che l'account possiede.

3.3.3 Generazione e distribuzione XRP

Come affermato in precedenza, la quantità totale di XRP è fissa ed è pari a 100 miliardi. Per come è stato concepito, il sistema non è in grado di generare nuovi token come avviene invece per altre criptovalute come Bitcoin. 80 dei 100 miliardi di XRP sono stati donati alla società Ripple Labs. Secondo quanto riportato in [6] Questi XRP vengono concessi ai consumatori con i seguenti programmi:

- Utenti: I nuovi utenti vengono ricompensati con degli XRP quando entrano a far parte della rete Ripple.

- Sviluppatori: Gli sviluppatori vengono ricompensati con XRP quando trovano bug nel codice open source o forniscono delle patch a bug già noti.
- Mercanti: Degli XRP vengono regalati agli utenti in base al numero di transazioni che questi eseguono sulla rete.
- Gateways: Gli ideatori stanno cercando di incentivare l'esecuzione del sistema creando partner strategici e concedendo Ripples come ricompense ai propri partner.
- Market Makers: Le istituzioni finanziarie e gli agenti Forex vengono compensati appositamente per portare liquidità al modello.

3.4 Mitigazione dei possibili attacchi

In questa sezione, come riportato in [6], si trattano alcuni degli attacchi più comuni nel campo delle criptovalute e come Ripple sfrutta il proprio protocollo di consenso per contrastare queste minacce.

- **Attacco del 51%**: L'attacco in questione è molto temuto nel campo delle criptovalute, viene respinto dal Ripple Consensus Protocol attraverso l'introduzione di UNL. Un server si affida solo alle transazioni che sono fidate dai nodi nella sua UNL, limitando così la possibilità per un attaccante di prendere il controllo di nodi già presenti nell'UNL. Questa attacco risulta molto complesso, in quanto la transazione di double spending risultante verrebbe infinitamente considerata non affidabile dal server. Sono inoltre presenti controlli di latenza per assicurarsi che tutti i nodi stiano funzionando correttamente e sono previsti meccanismi per aggiornare l'UNL se i nodi mostrano comportamenti sospetti.
- **Attacco di Denial of Service (DoS)**: Ripple dispone di un meccanismo per prevenire possibili attacchi di Denial of Service. Per ogni transazione che avviene nel sistema, vengono distrutti 0,00001 XPR. Inoltre, un utente deve mantenere un saldo minimo di 20 XPR per creare una transazione nel registro. L'idea di questi meccanismi è di mandare in bancarotta l'attaccante in caso di attacco DoS, bruciando Ripple e rendendo costosa l'esecuzione di un elevato numero di transazioni, mantenendole al tempo stesso convenienti per gli utenti comuni.

3.5 I principali software

3.5.1 XCurrent

XCurrent è la soluzione software di Ripple che permette il processo di pagamenti internazionali senza usare direttamente la criptovaluta XRP, ma piuttosto regolandoli con un monitoraggio end-to-end. Si tratta di un software interbancario implementato nell'infrastruttura stessa delle banche che utilizza il protocollo **Interledger (ILP)**, che quindi si adatta ai diversi registri di pagamento di tutti i membri della RippleNet. Inoltre soddisfa tutti i requisiti di rischio, privacy e conformità che richiede ogni banca

partner.
Le quattro componenti di base di xCurrent sono:

- **xCurrent Messenger** fornisce una via di comunicazione peer-to-peer tra istituzioni finanziarie connesse attraverso la RippleNet. Viene usato per scambiare informazioni relative a rischio e conformità, tariffe, tassi di cambio, dettagli di pagamento e tempi previsti per l'erogazione di fondi.

- **Validator** viene usato per confermare crittograficamente il successo o il fallimento di una transazione, oltre che per coordinare il movimento di fondi nell'Interledger. Le istituzioni finanziarie possono gestire un proprio validatore o fare affidamento su uno di terzi.

- **ILP Ledger** funge da sotto-registro e viene usato per tracciare crediti, debiti e liquidità attraverso le parti che effettuano operazioni. I fondi vengono regolati automaticamente, o istantaneamente o per niente.

- **FX Ticker** viene usato per definire i tassi di cambio tra le parti delle transazioni. Monitora lo stato attuale di ciascun ILP Ledger configurato.

Questa tecnologia quindi aumenta l'efficienza della comunicazione interbancaria consentendo alle banche di liquidare transazioni (sopratutto multi-valuta) con trasparenza e integrità. Nota inoltre che Sebbene xCurrent sia stato progettato principalmente per valute fiat, supporta anche transazioni di criptovalute.
Se per esempio devo inviare 100 euro in Nuova Zelanda, invece di usare il sistema internazionale SWIFT, uso il mio sistema xCurrent su ledger distribuito, che è trasparente, immutabile e dunque sicuro. In questo modo il mio denaro in euro "viaggia sulla RippleNet", arriva alla banca del destinatario e viene convertito in dollari neo zelandesi pronti per essere usati

3.5.2 XVia

XVia è sempre uno strumento per inviare pagamenti, ma in questo caso si tratta solo di un'interfaccia standardizzata in RippleNet progettata per aziende, fornitori, banche che non vogliono installare alcun sofware specifico. Di fatto è un'interfaccia standard basata su API che permette ai clienti di cui sopra di interagire all'interno di una singola struttura, di creare pagamenti attraverso atri partner creditizi connessi e in generale di accedere a diversi vantaggi della RippleNet.
I servizi che offre questa interfaccia sono:

- **Tracciamento dei pagamenti** e conferma di consegna. Questa soluzione facilita la risoluzione di controversie tra le parti perché è uno strumento trasparente che registra tutto su Ledger distribuito.

- **Capital efficency**: In Brasile è già possibile liberare del capitale e convertirlo in XRP per poter usufruire dei servizi di trasferimento transfrontalieri.

- **Trasferimento di rich data**: i rich data sono usati per predire i comportamenti degli utenti, come ad esempio predire quando una persona comprerà qualcosa. XVia migliora significativamente il processo di riconciliazione attraverso rich data, incluse le fatture allegate ai pagamenti.

3.5.3 XRapid

XRapid è una soluzione di liquidità on-demand a basso costo che utilizza XRP come valuta ponte tra diverse valute fiat. Si tratta di una tecnologia molto efficace per le banche che operano in mercati emergenti, dove i pagamenti richiedono conti nella valuta locale prefinanziati. in questi casi lo spread può essere molto alto perchè stanno lavorando con valute trattate raramente.
Ad esempio, per inviare 100 euro in Nuova Zelanda con questo sistema mi affido all'istituzione finanziaria FIN che utilizza di prassi la soluzione xRapid. Quest'ultima riceve i soldi, li converte in XRP, e li invia attraverso la RippleNet, infine vengono riconvertiti in dollari neozelandesi. Questo processo ha bassissimi costi di cambio valuta, di trasferimento ed è praticamente istantaneo, può avvenire in 4 secondi.

3.5.4 Chi usa questo sistema?

Tra i clienti più famosi di Ripple Inc. c'è il famoso istituto di credito Santander che fornisce il nuovo servizio **One Pay FX** attraverso un'applicazione dello smartphone, e che permette pagamenti tra zona euro e USA. Anche **American Express** sta lavorando per integrare questo sistema all'interno della sua infrastruttura.
Per quanto riguarda **l'Asia** la partecipazione è ancora più diffusa, diverse banche giapponesi e sud coreane si sono unite al gruppo di lavoro per adottare questo sistema di pagamento.

3.6 XRP Ledger e Ethereum Virtual Machine

Nel contesto dell'evoluzione e del potenziale del sistema, Ripple sta testando una soluzione in grado di permettere agli sviluppatori di implementare smart contracts realizzati per Ethereum direttamente nella blockchain XRPL. L'estensione ha l'obiettivo di consentire l'interoperabilità tra le reti Ripple e Ethereum, aprendo nuove possibilità di interazione con le applicazioni decentralizzate Ethereum-compatible (DApps) e Web3 wallets.
In generale una sidechain è un registro indipendente avente propri tipi di transazioni, algoritmo di consenso, regole e nodi (inclusi i validatori). Agisce come la blockchain associata, funzionando in parallelo alla mainchain e consentendo il trasferimento di valore tra le due senza compromettere la velocità, l'efficienza e il throughput della mainchain. Le sidechain possono personalizzare il protocollo XRP Ledger in base alle esigenze e farlo funzionare come la blockchain associata. Ad esempio è possibile:

- Creare uno strato di smart contracts, alimentato da un engine compatibile con Ethereum Virtual Machine (EVM).
- Creare una propria stablecoin con tipi di registro personalizzati e regole di transazione.

La nuova **EVM compatible XRP Ledger sidechain** si presenta quindi come una potente blockchain di ultima generazione con le seguenti caratteristiche:

- Supporta fino a 1000 transazioni al secondo, gestendo così carichi e throughput elevati.
- Ha un tempo di conferma delle transazioni ridotto, in media, poiché un blocco viene prodotto ogni 5 secondi.
- Una volta che un blocco viene aggiunto alla catena e confermato, viene considerato definitivo (tempo di finalizzazione di 1 blocco).
- Fornisce piena compatibilità con l'Ethereum Virtual Machine (EVM), consentendo di connettere il proprio portafoglio e interagire o pubblicare contratti intelligenti scritti in Solidity.

La Sidechain EVM utilizza un algoritmo di consenso proof-of-stake (PoS). Lo staking avviene quando si impegnano le proprie monete per la verifica delle transazioni. Il modello proof-of-stake consente di fare staking della criptovaluta e creare i propri nodi validatori. Le proprie monete sono bloccate durante lo staking, ma è possibile annullare lo staking se si desidera scambiarle. In una blockchain proof-of-stake, il potere di mining dipende dalla quantità di monete che un validatore sta mettendo in gioco. I partecipanti che mettono in staking più monete hanno maggiori probabilità di essere scelti per l'aggiunta di nuovi blocchi. La tecnologia che è alla base del consenso della sidechain è Tendermint [7], un engine per la creazione di blockchain tollerante ai guasti bizantini. La blockchain utilizza la libreria `cosmos-sdk` di Tendermint per creare e personalizzare la blockchain utilizzando i suoi moduli integrati, tra cui è presente il modulo Ethermint `cosmos-sdk` fornisce compatibilità con l'EVM.
Attualmente la sidechain EVM-compatible è disponibile solo per scopi di sviluppo e il bridge è connesso alla XRP Ledger Devnet. L'integrazione dovrebbe diventare definitiva entro la fine del 2023 ed è il frutto di un processo che prevede prima che la sidechain diventi permissionless, cioè che chiunque entrarne a far parte, e poi che Ripple sviluppi completamente la componente software.

Capitolo 4

Ripple vs altre tecnologie

4.1 Vantaggi e Svantaggi

Ricapitolando quanto detto fin'ora, possiamo elencare vantaggi e svantaggi di Ripple e della sua criptovaluta XRP.

4.1.1 Vantaggi

- **Rapidità delle transazioni**:Il processo di conferma delle transazioni è incredibilmente veloce: in genere richiede da quattro a cinque secondi, mentre le banche possono impiegare diversi giorni per effettuare un bonifico. Bitcoin, invece, verifica le transazioni in alcuni minuti o talvolta in qualche ora.

- **Commissioni molto basse**: Il costo per completare una transazione sulla rete Ripple è di soli 0,0001 XRP.

- **Versatilità come rete di scambio**: Il network Ripple non solo elabora transazioni in XRP, ma può essere utilizzato anche per altre valute fiat, criptovalute e materie prime.

- **Utilizzo da parte di grandi istituti finanziari**: Ripple è utilizzata come piattaforma per la gestione di transazioni anche dalle grandi imprese. Santander, Axis Bank e Yes Bank sono solo alcuni degli istituti che utilizzano il network, un dato che testimonia la più elevata diffusione di Ripple presso le grandi società del mercato rispetto alla maggior parte delle criptovalute.

4.1.2 Svantaggi

- **Fortemente centralizzato**: Una delle caratteristiche alla base del successo delle criptovalute è la loro decentralizzazione, che ha permesso di svincolarle dal controllo delle grandi banche e dei governi. Essendo un sistema centralizzato, Ripple si pone in contrasto con questa filosofia.

- **Ripple Labs è l'unica fonte in grado di generare XRP**: Ripple Labs decide quando emettere i token, esercitando un maggiore grado di controllo sul network rispetto ad altre criptovalute. Grazie all'attività di mining, infatti, nella quasi

totalità dei sistemi crypto i token vengono immessi sul mercato in maniera lenta e costante. Questa differenza consente a Ripple Labs di influire in modo diretto sul valore di XRP, decidendo in quali quantità e con quali tempistiche emettere i token.

- **Interventi normativi nei confronti di XRP**: L'anno scorso, negli Stati Uniti, la Securities and Exchange Commission (SEC) ha avviato un'azione legale contro Ripple, sostenendo che, dal momento che è la società a decidere quando emettere XRP, la criptovaluta dovrebbe essere registrata come titolo. Ulteriori dettagli rispetto a queste controversie sono descritti in dettaglio nei paragrafi successivi.

4.2 Ripple/XRP vs Bitcoin

La rete Ripple è stata costruita con principi simili a quella di Bitcoin. Tuttavia, a differenza di Bitcoin, le decisioni non sono prese dalla comunity Ripple, ma da un azienda privata (Ripple Inc.) e questo rende la criptovaluta centralizzata.

Bitcoin è basato sulla tecnologia blockchain che è una rete peer-to-peer decentralizzata. Il meccanismo di consenso usato da blockchain sfrutta la proof-of-work. I miners si occupano di validare le transazioni e rendere sicura la rete. Mentre Ripple utilizza il cosidetto Ripple Protocol Consensus Algorithm (RPCA). Tale algoritmo sfrutta dei validatori scelti dalla compagnia Ripple stessa che si occupano di validare le transazioni e rendere sicura la rete. Il meccanismo di consenso di Ripple è più semplice e quindi richiede molta meno energia rispetto alla Proof of Work di bit coin. Per questo Ripple può essere considerato più efficiente dal punto di vista energetico. L'efficienza energetica è un fattore cruciale per valutare complessivamente una criptovauta.

Anche per quanto riguarda la velocità delle transazioni le due tecnologie utilizzano diversi approcci. Una transazione bitcoin può richiedere da qualche minuto fino anche a qualche ora per essere portata a termine (il tempo medio richiesto è 10 minuti). La velocità di esecuzione dipende dal livello di congestione della rete, che è capace di processare un certo numero limitato di transazioni. Gli utenti possono aumentare la quota pagata ai miners per aumentare la probabilità che la propria transazione sia aggiunta nel prossimo blocco. Ripple svolge invece le sue transazioni in maniera più veloce rispetto a Bitcoin (3-5 secondi).
Per quanto riguarda la scalabilità, Ripple afferma che XRP Ledger è in grado di gestire 1500 transazioni al secondo, contro le 5 di bitcoin (in media). Ripple si avvicina quindi a processori di pagamenti standard come VISA, che gestiscono 1700 transazioni al secondo, il che rende questa tecnologia un a buona soluzione per le aziende finanziare che hanno bisogno di un'infrastruttura stabile per alti volumi di transazioni. Si può dunque affermare che la tecnologia Ripple è più scalabile di quella di Bitcoin.
Ripple e Bitcoin vengono utilizzati in diversi settori. Bitcoin è abitualmente utilizzato come riserva di valore asset di investimento e come mezzo di scambio in alcuni settori (per questo Bitconin viene spesso definito "oro digitale"). D'altra parte Ripple è anche spesso utilizzato da istituzioni finanziarie e banche. Di fatto, l'obiettivo dei fondatori di Ripple non è quello di smantellare il sistema bancario, ma di renderlo più efficiente. Ripple e la sua criptovaluta XRP propongono un sistema che ha come obbiettivo l'au-

mento della liquidità delle istituzioni finanziarie, mentre l'obiettivo principale di Bitcoin è quello di eliminare completamente il bisogno di banche e autorità centrali.

4.3 Ripple vs SWIFT

Ripple sfrutta la tecnologia blockchain e offre un nuovo approccio per pagamenti cross-border che potenzialmente potrebbe rivoluzionare i sistemi tradizionali. In questa sezione descriviamo quindi un analisi comparativa fra Ripple e SWIFT (Society of Worldwide Interbank Financial Telecommunication). SWIFT è un sistema di messaggistica esistente da 45 anni ed è tradizionalmente il sistema più utilizzato nella finanza globale per completare le transazioni. SWIFT dipende da vari intermediari bancari per permettere alle transazioni di essere svolte, per questo la liquidità e il credito sono sottoposti ad un rischio. Un centro di compensazione (clearing center) o un centro di regolamento (settlment center) sono sempre necessari presso il mittente e destinatario della transazione. Ciò rende il percorso di una transazione lungo. I dettagli di una transazione sono inseriti all'interno della rete SWIFT dove saranno processati da una serie di step. Ad ogni step il messaggio viene salvato e verificato. Il flusso dei messaggi viene mantenuto separato dal flusso di pagamento, il pagamento viene effettivamente portato a termine dopo che si è verificata la liquidità. Per questo SWIFT è considerata una tecnologia altamente sicura. Tuttavia SWIFT è soggetto ad alcune vulnerabilità di sicurezza tipiche dei sistemi centralizzati: single point of failure e attacchi informatici. Diversamente, Ripple evita di utilizzare i livelli di banche intermedi e sfrutta la tecnologia Blockchain per portare a termine il processo dei pagamenti cross-border. Il percorso per terminare le transazioni di Ripple è molto più semplice. RippleNet consente alle banche e ad altre istituzioni finanziarie di connettersi direttamente tra loro e di inviare pagamenti in tempo reale utilizzando XRP come mezzo di scambio. Questo approccio elimina la necessità di intermediari bancari e semplifica il processo dei pagamenti. Le transazioni attraverso Ripple sono notevolmente più veloci rispetto a quelle tradizionalmente effettuate tramite SWIFT. Le transazioni Ripple possono essere completate in pochi secondi, consentendo ai partecipanti di ricevere i fondi in modo quasi istantaneo.

Capitolo 5

Limiti, controversie e vulnerabilità

In questo capitolo riassumiamo tutti i problemi che sono stati evidenziati con maggiore enfasi della tecnologia Ripple e della sua criptomoneta. Come molte altre criptovalute, il prezzo di XRP può essere estremamente volatile. Le fluttuazioni dei prezzi possono essere influenzate da fattori come l'andamento generale del mercato delle criptovalute, gli annunci di partnership o adozione da parte di importanti attori del settore finanziario, le regolamentazioni governative e le notizie di carattere positivo o negativo riguardanti Ripple o XRP. Questa volatilità può portare a rapidi cambiamenti di valore, con possibili conseguenze finanziarie per gli investitori. Uno dei rischi specifici associati a XRP è la concentrazione di token in mano a Ripple Labs, (l'azienda che ha sviluppato Ripple). Essa detiene una quantità significativa di XRP (circa il 55% della massima disponibilità). Ciò significa che le decisioni e le azioni di Ripple Labs possono influire sull'andamento del mercato di XRP. Inoltre, l'esistenza di una grande quantità di token in mano a un'entità centrale può suscitare preoccupazioni riguardo alla decentralizzazione e alla governance della criptovaluta.

Al momento il costo di una transazione Ripple corrisponde allo 0.001% del valore originale di XRP. Secondo [8] un aumento della richiesta di transazioni Ripple provocherà un aumento del costo e porterà la compagnia a rilasciare una maggiore quantità di XRP nel mercato libero per supportare un più grande volume di transazioni.

Un'altra minaccia deriva dalla competizione con le altre criptovalute estremamente diffuse (Bitcoin ed Ethereum per esempio). Tale competizione è critica perchè l'adozione di Ripple e XRP da parte delle istituzioni finanziarie e degli attori del settore è fondamentale per il successo della piattaforma. Se Ripple non riesce ad ottenere un'ampia adozione da parte delle banche e delle istituzioni finanziarie tradizionali, potrebbe essere difficile per XRP realizzare il suo pieno potenziale come mezzo di scambio diffuso.

5.1 Contenziosi legali

Alcuni recenti sviluppi legali potrebbero rappresentare un pericolo esistenziale per Ripple. In questa sezione presentiamo brevemente le questioni che hanno portato al contenzioso e le possibili ritorsioni. Un acquirente di XRP di nome Ryan Coffe ha intentato

un'azione legale collettiva contro Ripple il 3 maggio 2018, per conto di tutti gli acquirenti di XRP. Coffey ha affermato che XRP presentava tutte le caratteristiche necessarie per essere considerato un titolo finanziario, ma che Ripple Labs non ha registrato XRP come titolo finanziario secondo le leggi federali sui titoli. Coffey ha affermato di aver perso dei soldi comprando e rivendendo XRP per via dei problemi legali della criptomoneta e ha quindi richiesto che lui e gli altri investitori venissero risarciti dei danni subiti e che il tribunale impedisse a Ripple Labs di continuare a violare le leggi sui titoli attraverso la vendita non registrata di XRP.

Sebbene abbia volontariamente ritirato la sua causa, la denuncia di Coffey ha fornito una solida base per future cause legali contro Ripple. Nei mesi successivi alla prima azione collettiva di Coffey, Vladi Zakinov, David Oconer e Avner Greenwald [9] hanno presentato azioni collettive contro Ripple in un tribunale statale della California, facendo accuse simili a quelle di Coffey.

Ripple ha di fatto respinto le accuse. Il 26 febbraio 2020, il giudice della Corte distrettuale degli Stati Uniti per il Distretto Settentrionale della California ha permesso che la causa continuasse, respingendo solo alcune delle accuse presentate in base alle leggi dello stato della California. Le cause in sospeso costituiscono una minaccia esistenziale per Ripple Labs. Anche se Ripple vincesse questa causa specifica, rimarrebbe un obiettivo costante per cause legali e azioni regolamentari a causa dello status di sicurezza legale ambiguo di XRP.

5.2 Manipolazione del mercato: Pump and Dump

XRP, così come molte altre criptovalute, ha una liquidità limitata, che le rende estremamente vulnerabili alla manipolazione del mercato. [10] conduce un'indagine approfondita su una delle principali manipolazioni del mercato effettuate dalle comunità online: il pump and dump. Pump and dump è un tipo di truffa di manipolazione del mercato che comporta l'aumento artificiale del prezzo di un titolo posseduto prima di venderlo ad altri investitori per un prezzo molto più alto. Questo imbroglio è antico quanto il mercato azionario. Pump and dumps sono diventati più importanti che mai con l'emergere dei mercati caotici e spesso non regolamentati per le criptovalute, i cui prezzi sono semplici da manipolare. Pump and dumps sono disposti da numerosi gruppi online auto-organizzati, e il fenomeno è diffuso ma ancora relativamente sconosciuto. I maggiori pump and dumps avvenuti hanno come target Dogecoin e XRP. Il pump and dump consiste in un acquisto massiccio. I truffatori di un gruppo si coordina e acquistano una grande quantità della criptovaluta scelta in modo da innescare un aumento del prezzo. Questo aumento artificiale del prezzo viene definito "pump" (pompa) e attira l'attenzione degli investitori che sperano di ottenere profitti rapidi. Durante la fase di pump i truffatori promuovono la criptovaluta attraverso vari canali di comunicazione, enfatizzando l'aumento di prezzo e spingendo gli altri a investire. Questo crea una domanda crescente per la criptovaluta. Quando il prezzo della criptovaluta ha raggiunto il picco desiderato, i truffatori vendono repentinamente le loro grandi quantità di criptovaluta sul mercato. Questa vendita massiccia fa diminuire il prezzo drasticamente, facendo perdere valore agli investitori che sono stati attirati dal "pump". Ad oggi si sono registrati vari casi di pump and dump che prendono di mira Ripple XRP. Fra i tanti citiamo

[11] in cui un gruppo di utenti si sono coordinati su un canale Telegram per comprare quantità ingenti di XRP in una precisa data e ora (13:30 del 1° febbrario 2021). Tale azione ha portato XRP ad un aumento di valore del 56% in un giorno, ottenendo il più alto guadagno in una singola giornata mai registrato dal dicembre 2017.
La prima conseguenza per una criptovaluta presa di mira da un pump and dump è la crescita di popolarità immediata. Questo potrebbe aiutare a rendere la criptovaluta più forte. Tuttavia, il prezzo torna rapidamente alla normalità. Di conseguenza, gli investitori potrebbero a dubitare sulla credibilità della criptomoneta. Potrebbe quindi essere estremamente difficile ricostruire la fiducia nella criptovaluta. XRP è stato più volte utilizzato come target di pump and dumps. Questo potrebbe essere un altro fattore che si contrappone alla crescita della moneta stessa. Tuttavia, per limitare questo problema, ad oggi esistono vari algoritmi per il rilevamento di pump and dumps in tempo reale. [10] propone un algoritmo che per la rilevazione di pump and dumps sfrutta l'insolita ondata di cosiddetti "market buy orders", che vengono utilizzati quando un investitore vuole acquistare qualcosa rapidamente e a qualsiasi prezzo. Tale modello supera di gran lunga gli altri modelli allo stato dell'arte sia per quanto riguarda il tempo necessario alla rilevazione, che in termini di accuratezza.

Capitolo 6

Conclusioni

In questo studio abbiamo esaminato il sistema Ripple e la criptovaluta XRP, mettendo in luce i loro potenziali punti di forza, nonché le criticità e le debolezze associate. Durante la nostra analisi, abbiamo compreso come funziona il protocollo di consenso Ripple che ha permesso la nascita dell'approccio innovativo per facilitare i pagamenti e i trasferimenti di denaro su scala globale, sfruttando la tecnologia della blockchain.
È stato messo in luce come la capacità di Ripple di offrire trasferimenti di denaro rapidi ed economici, eliminando i ritardi e le inefficienze dei metodi convenzionali di pagamento abbia attirato l'attenzione del settore finanziario, rendendo XRP popolare come mezzo di scambio immediato per i trasferimenti di valore tra valute. Nel confronto con le altre tecnologie (Bitcoin e SWIFT) è stato visto come Ripple possegga il potenziale di avere un impatto nel settore dei pagamenti e dei trasferimenti di denaro, data la sua alta scalabilità, versatilità ed eco-sostenibilità.
Abbiamo esaminato anche le attuali applicazioni offerte da Ripple, tra cui XCurrent, XVia e XRapid, insieme all'innovativa implementazione che dovrebbe arrivare a fine 2023 degli smart contract per Ethereum sulla blockchain XRPL.
Tuttavia, queste tecnologie non sono esenti da controversie che hanno alimentato dibattiti e sollevato preoccupazioni, potenzialmente influenzando il tasso di adozione e limitando l'incremento del valore di XRP.
In conclusione, Ripple rappresenta un'innovazione nel settore dei pagamenti e dei trasferimenti di denaro, offrendo un'alternativa interessante ai modelli tradizionali. Tuttavia, affinché Ripple possa raggiungere pienamente il suo potenziale e garantire il suo successo a lungo termine, sarà fondamentale affrontare le questioni sollevate e lavorare verso una maggiore trasparenza, decentralizzazione e aderenza alle normative vigenti.

Bibliografia

[1] David Schwartz, Noah Youngs, and Arthur Britto. The ripple protocol consensus algorithm. *Ripple Labs Inc. Whitepaper*, 2014.

[2] Brad Chase and Ethan MacBrough. Analysis of the xrp ledger consensus protocol, 2018.

[3] Frederik Armknecht, Ghassan O. Karame, Avikarsha Mandal, Franck Youssef, and Erik Zenner. Ripple: Overview and outlook. In Mauro Conti, Matthias Schunter, and Ioannis Askoxylakis, editors, *Trust and Trustworthy Computing*, pages 163–180, Cham, 2015. Springer International Publishing.

[4] Michael J Fischer, Nancy A Lynch, and Michael S Paterson. Impossibility of distributed consensus with one faulty process. *Journal of the ACM (JACM)*, 32(2):374–382, 1985.

[5] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. Cryptology ePrint Archive, Paper 2011/368, 2011. https://eprint.iacr.org/2011/368.

[6] Sufian Hameed and Sameet Farooq. The art of crypto currencies. *International Journal of Advanced Computer Science and Applications*, 7(12), 2016.

[7] Jae Kwon. Tendermint : Consensus without mining. 2014.

[8] Yuan Gao Ruidong Zhang, Tianyi Qiu. Ripple vs. swift: Transforming cross border remittance using blockchain technology, 2018.

[9] Avner Greenwald. Greenwald v. ripple labs, inc, 2018.

[10] Massimo La Morgia, Alessandro Mei, Francesco Sassi, and Julinda Stefa. The doge of wall street: Analysis and detection of pump and dump cryptocurrency manipulations, 2021.

[11] Omkar Godbole. Xrp posted biggest single-day gain in 3 years in a coordinated buying attack, 2021.

Appendice A

Algoritmi

Algorithm 1 Validazione dalla prospettiva di P_i

```
vals = {}        ▷ vals è una mappa che associa il blocco L un insieme di nodi che ha validato L
ricezione V_{L,j} do
    if P_j ∈ UNL_i then
        vals[L] ← vals[L] ∪ j
        if |vals[L]| ≥ q_i and seq(L) > seq(L̂) then
            L̂ ← L
        end if
    end if
end ricezione
```

Algorithm 2 Preferred branch dalla prospettiva di P_i

```
lastVals = {} ▷ lastVals è una mappa che associa nodo fidato al blocco validato più recentemente
ricezione V_{L,j} do
    if P_j ∈ UNL_i then
        lastVals[j] ← L
    end if
end ricezione

function PreferredLedger()
    L ← antenato comune più remoto in lastVals
    done ← False
    while |children(L)| > 0 and not done do
        C ← lista dei children(L) in ordine decrescente di supp_branch, φ è usata per rompere i pareggi
        Δ ← supp_branch(C[0])
        if |children(L)| > 1 then
            Δ ← Δ − supp_branch(C[1]) + φ(C[0], C[1])
        end if
        if Δ > uncommitted(seq(L) + 1) then
            L ← C[0]
        else
            done ← True
        end if
    end while
    if L ∈ ancestors(L̃) then
        return L̃
    else
        return L
    end if
end function
```

Algorithm 3 Deliberazione dalla prospettiva di P_i

```
s_max ← 0        ▷ Tiene traccia del più grande numero di sequenza dei blocchi validati
function START(L)
    L̃ ← L, r ← 0
    T ← transazioni in attesa di essere messe in un blocco
    props ←                                   ▷ Mappa nodo - proposte di blocco
    Inizializza props con le proposte ricevute per L̃
    broadcast P_{T,r,L̃,i}    ▷ r-esima proposta di deliberazione per la transazione T da
applicare ad L del nodo P_i
end function

ricezione P_{T',r',L,j} do
    if P_j ∈ UNL_i and L̃ = L and r' > props[j].r then
        props[j] ← P_{T',r',L,j}
    end if
end ricezione

function UPDATE()    ▷ Chiamata ad un intervallo di tempo definito dal protocollo
    if L̃ ≠ PREFERREDLEDGER() then
        START(PREFERREDLEDGER())
    else
        UPDATEPOSITION()
        if CHECKCONSENSUS() then
            L̃ ← APPLY(T, L̃)
            if seq(L̃) > s_max then
                broadcast V_{L̃,i}
                s_max ← seq(L̃)
            end if
            START(L̃)
        end if
    end if
end function

function UPDATEPOSITION()
    T_all ← ⋃_{P∈props} P.T                ▷ Insieme di tutte le transazioni proposte
    τ ← threshold(r)n_i
    T ← {x ∈ T_all : SUPPORT(x) > τ}        ▷ SUPPORT è il numero di nodi che
propongono x
    r ← r + 1
    broadcastP_{T,r,L̃,i}
end function

function CHECKCONSENSUS()
    n_a ← |{P ∈ props : P.T = T}|    ▷ Numero di nodi che concordano con la nostra
proposta
    return n_a ≥ q_i
end function
```

I SERVIZI DELLA BLOCKCHAIN TON

Cristian Brunetto, Melissa Cannas, Stefano Leto, Sonia Vittonero

POLITECNICO DI TORINO

Tesina di Blockchain e Criptoeconomia

I servizi della Blockchain TON

Responsabili del corso

prof. Bazzanella Danilo
prof. Gangemi Andrea

Partecipanti

Cristian Brunetto
Melissa Cannas
Stefano Leto
Sonia Vittone

Anno Accademico 2022-2023

Indice

1 Introduzione **4**
1.1 La nascita della blockchain TON 4

2 Struttura della blockchain TON **6**
2.1 Tipi di blockchain 6
2.2 Creazione e regole di convalida dei blocchi 8
2.2.1 I validatori 8
2.2.2 Convalida dei blocchi 9
2.2.3 Elezione del successivo blocco candidato 9
2.2.4 Validatori per le masterchains 9

3 I servizi e le applicazioni TON **10**
3.1 TON come progetto multi-blockchain 10
3.2 Strategie d'implementazione del servizio TON 10
3.2.1 Applicazioni on-chain pure 11
3.2.2 Servizi di rete puri 12
3.2.3 Servizi misti 12
3.2.4 Servizi misti decentralizzati o fog services 12
3.3 Connettere utenti e fornitori di servizi 13
3.3.1 Registri on-chain, misti e off-chain 13
3.3.2 Registro in una side-chain 13
3.3.3 Registro in una workchain 13

4 TON DNS **14**
4.1 DNS sicuro, privato e decentralizzato 14
4.2 Un protocollo per il networking anonimo 15
4.3 TON DNS smart contracts 15
4.3.1 Registrazione di nuovi sottodomini 15
4.3.2 Recupero dati da uno smart contract DNS 15
4.3.3 Traduzione di un dominio TON DNS 16
4.3.4 Accesso ai dati contenuti negli smart contract 16
4.3.5 User interface di uno smart contract 17

5 TON Payments **18**
5.1 Payment Channels 18
5.1.1 Trustless Payment Channels 19
5.1.2 Bidiretional synchronous trustless Payment Channels . . . 19
5.1.3 Asynchronous payment channel: una blockchain semplice con due validatori 20
5.1.4 Promises 20
5.1.5 TON VM: supporto per "smart" payment channels 21
5.2 Lightning Network 21
5.2.1 Limitazione dei Payment Channels 21
5.2.2 Payment channel networks, or lightning networks" 21
5.2.3 Chain money transfer 22
5.2.4 Paths nella lightning network 22
5.2.5 Considerazioni Finali 22

6 Conclusioni **23**

Capitolo 1

Introduzione

1.1 La nascita della blockchain TON

The Open Network (TON) è una blockchain veloce, sicura e scalabile, in grado di gestire milioni di transazioni al secondo. Nel 2019 il team di Telegram capitanato dai fratelli Pavel e Nikolai Durov ha cominciato a esplorare soluzioni blockchain per l'app di messaggistica. Viene così lanciata la prima testnet di The Open Network con un'ICO (Initial coin offering) della crypto del network, che allora si chiamava Gram.

In quest'occasione la SEC (US Securities and Exchange Commission) ha aperto un'indagine per verificare che Telegram non avesse venduto senza autorizzazione la crypto Gram come se fosse una security, ovvero un titolo, e dopo varie battaglie legali, la SEC ha stabilito che gli acquirenti di Gram si aspettavano ragionevolmente dei profitti che sarebbero derivati dagli sforzi imprenditoriali della società. Quella di Gram viene quindi vista come una vendita non autorizzata di titoli. Telegram prova a difendersi, sostenendo che le affermazioni della SEC siano infondate, ma accetta di rinviare il lancio della TON fino a quando le questioni legali non saranno risolte. Dopo mesi di "battaglie legali" con gli Stati

Uniti, Telegram decide di rinunciare, consapevole di non poter raggiungere un accordo totalmente a proprio favore. Il team di Telegram cessa lo sviluppo di TON , paga una multa da 18,5 milioni di dollari e accetta di restituire i fondi agli investitori.
A questo punto, tra il 2020 e il 2021, un piccolo team di sviluppatori open-source - NewTON - studia il codice, l'architettura e la documentazione di TON. Riprende così lo sviluppo attivo di TON in linea con il progetto dettagliato nella documentazione originale. Il ripristino della blockchain The Open Network è iniziato a Gennaio 2021 e dopo dieci mesi la blockchain è stata riportata in vita con l'infrastruttura e gli strumenti di base. Il team di NewTON viene così rinominato TON Foundation - una comunità no-profit focalizzata su un ulteriore supporto e sviluppo della rete. A Novembre 2021 The Open Network è stata inaugurata e nel corso del 2022 si sono concentrati gli sforzi degli sviluppatori per fornire The Open Network della tecnologia e della sicurezza adeguata.

Capitolo 2

Struttura della blockchain TON

TON è in più precisamente una raccolta di blockchains o una *"blockchain di blockchains"*, e questo gli permette di raggiungere l'obiettivo di elaborare milioni di transazioni al secondo, al contrario dei singoli progetti blockchain, il cui standard attuale è di decine di transazioni al secondo.

2.1 Tipi di blockchain

TON è costituita da tre diversi tipi di blockchain:

- Una master blockchain, o *masterchain* in breve, contenente informazioni generali sul protocollo e i valori correnti dei suoi parametri, l'insieme dei validatori e la loro "posta in gioco", l'insieme delle workchains attualmente attive e i loro "shards" (ogni shard è un frammento della workchain ed è responsabile dell'elaborazione di una sola parte dei dati archiviati nella rete). Infine, la Masterchain contiene l'insieme delle hash dei blocchi più recenti di tutte le workchains e shardchains.

- Vi sono diverse (fino a 2^{32}) working blockchains, *workchains* in breve, che contengono le transazioni di trasferimento di valore e smartcontract. Differenti workchains possono avere regole diverse, cioè diversi formati per gli indirizzi degli account e per le transazioni, diverse macchine virtuali (VM) per gli smartcontract, diverse criptovalute e così via. Tuttavia, tutte le workchains devono soddisfare determinati criteri di interoperabilità di base per rendere possibile e relativamente semplice l'interazione tra loro. A questo proposito, si può affermare che la TON Blockchain è **eterogenea**.

- Ogni workchains può essere suddivisa fino in 2^{60} shard blockchains, o *shardchains*, aventi le stesse regole e lo stesso formato di blocco della workchain stessa, ma responsabile solo di un sottoinsieme di account, a seconda di

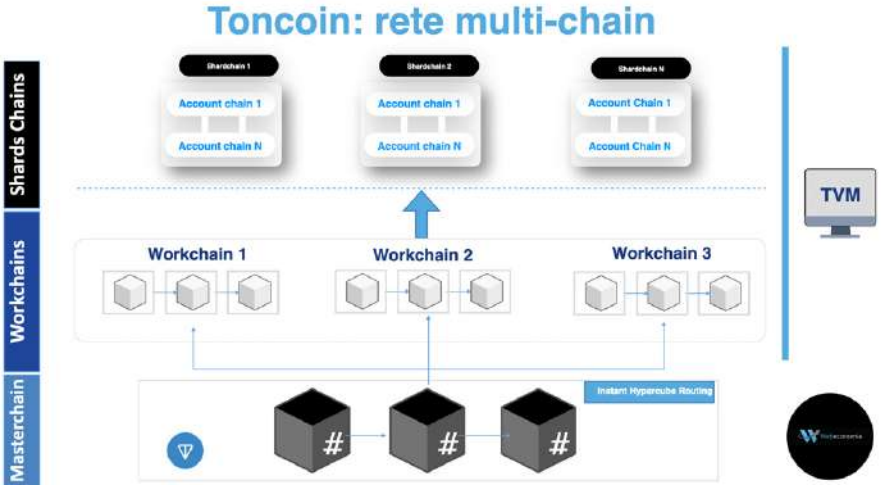


Figura 2.1: Struttura gerarchica della blockchain TON, dal basso verso l'alto: una masterchain, le workchains ed infine le shardchains.

diversi primi bit (i più significativi) dell'indirizzo dell'account stesso. In altre parole, vi è una forma di condivisione ("sharding") incorporata nel sistema. Dal momento che tutte queste shardchains condividono un formato e regole di blocco comuni, la TON Blockchain si può considerare **omogenea** in questo senso.

- Ogni blocco in una shardchain (e nella masterchain) non è in realtà solo un blocco, ma una piccola blockchain. Normalmente, questo "blocco di blockchain" o "blockchain verticale" consiste esattamente di un blocco, quindi potremmo pensare che questo sia solo il corrispondente blocco della shardchain (chiamato anche "blockchain orizzontale" in questa situazione). Tuttavia, se diventa necessario correggere i blocchi shardchain che presentano errori, un nuovo blocco viene commesso nella blockchain verticale. Quest'ultimo può contenere o la sostituzione per il blocco non valido, o un "blocco di differenza", contenente solo una descrizione delle parti della versione precedente che devono essere modificate. Questo è un meccanismo specifico di TON per sostituire i blocchi non validi rilevati, senza arrivare ad avere una vera e propria fork di tutte le shardchains coinvolte. Si osserva quindi che ogni shardchain (e masterchain) non è una blockchain convenzionale, ma una blockchain di blockchains, o 2D-blockchain, o più semplicemente 2-blockchain.

2.2 Creazione e regole di convalida dei blocchi

I diversi blocchi shardchains e le masterchains presentate precedentemente devono essere creati, convalidati e propagati attraverso la rete a tutte le parti interessate, affinché il sistema funzioni senza intoppi e correttamente.

2.2.1 I validatori

TON utilizza un approccio Proof-of-Stake (PoS) per generare nuovi blocchi nelle shardchains e nella masterchain. Questo significa che c'è un insieme di nodi designati, i *validatori*, nodi speciali che hanno depositato *stakes* (grandi quantità di monete TON) da una speciale operazione Masterchain, per essere eleggibili per la nuova generazione e la convalida di blocchi. Essenzialmente, qualsiasi nodo che desideri diventare un validatore può farlo, a condizione che abbia a disposizione una quota sufficientemente grande da fornire come deposito(in monete TON) nella masterchain. I validatori vengono premiati per mantenere la TON Blockchain funzionante. I vari "rewards" possono essere "gas fees" derivanti dalle transazioni nel blocco, nuove monete recentemente coniate, transazioni. Questo reddito è distribuito tra tutti i validatori partecipanti, proporzionalmente alla loro posta in gioco. D'altra parte, essere un validatore porta ad avere un'alta responsabilità. Se si firma un blocco non valido, si può essere puniti perdendo parte o tutta la ricompensa, e si può essere temporaneamente o permanentemente esclusi dall'insieme dei validatori. Inoltre, se un validatore si astiene alla creazione di nuovi blocchi per un lungo periodo di tempo, può perdere parte del suo premio e anche in questo caso può essere sospeso o permanentemente escluso dal gruppo di validatori. Tutto questo sottolinea come il validatore non ottenga i suoi soldi per niente; infatti deve tenere traccia degli stati di tutte o di alcune shardchains (ogni validatore è responsabile per la convalida e la creazione di nuovi blocchi in un certo sottoinsieme di shardchains), eseguire tutti i calcoli richiesti da smartcontracts trattati in queste shardchains, ricevere aggiornamenti su altre shardchains e così via. Questa attività richiede notevole spazio su disco, potenza di calcolo e larghezza di banda della rete.

Validatori per le shardchains

L'insieme globale di validatori (dove ogni validatore è considerato presente con molteplicità uguale alla sua quota, altrimenti potrebbe essere tentato di assumere diverse identità e dividere la sua quota con gli altri) viene utilizzato solo per convalidare il nuovo blocco masterchain. Una precisazione necessaria è che i blocchi shardchain sono convalidati solo da sottoinsiemi di validatori appositamente selezionati, presi dal set globale di validatori. Questi sottoinsiemi di validatori sono definiti per ogni shard, sono ruotati ogni ora (in realtà, ogni 2^10 blocchi masterchain), e sono conosciuti un'ora di anticipo, in modo che ogni validatore sappia quali shards esso avrà bisogno di convalidare, e potrà prepararsi per questo (ad esempio, scaricando dati mancanti di shardchain). L'algoritmo utilizzato per selezionare i gruppi di attività del validatore per ogni shard è de-

terministico pseudocasuale. Usa numeri pseudocasuali incorporati da validatori in ogni blocco masterchain per creare un seme casuale, e quindi calcola l'hash per ogni validatore. Questi ultimi sono ordinati per il valore di questo hash, e i primi sono selezionati in modo da avere almeno 5 validatori per ogni gruppo.

2.2.2 Convalida dei blocchi

Una volta che un blocco candidato è ricevuto da un validatore e la firma del validatore originario è verificata, il ricevente verifica la validità, eseguendo tutte le transazioni in esso e controllando che il loro risultato coincida con quello sostenuto. Tutti i messaggi importati da altri blockchains devono essere supportati da adeguate prove Merkle nei dati raccolti, altrimenti il blocco il candidato è considerato non valido. D'altra parte, se il blocco candidato è ritenuto valido, il ricevente validatore firma e propaga la sua firma ad altri validatori nel gruppo. È importante sottolineare come un validatore non ha bisogno di accedere allo stato della sua shardchain o di quelle vicine al fine di verificare la validità di un blocco. Questo permette alla validazione di procedere molto rapidamente (senza accessi al disco), e alleggerisce il calcolo e la memorizzazione, onerosa per i validatori.

2.2.3 Elezione del successivo blocco candidato

Una volta che un blocco candidato raccoglie almeno due terzi delle firme di validità da parte dei validatori nel gruppo di lavoro, può essere impegnato come prossimo blocco shardchain. Un protocollo BFT (Bizantyne Fault Tolerance) viene eseguito per raggiungere il consenso sul candidato blocco (ci può essere più di una proposta), preferendo il blocco con la massima priorità per il turno. Come risultato dell'esecuzione di questo protocollo, le firme sul blocco arrivano ad essere circa due terzi delle totali. Queste firme testimoniano non solo la validità del blocco in questione, ma anche la sua elezione da parte del protocollo BFT. Infine, il blocco (senza dati raccolti) è combinato con tutte queste firme, serializzato in modo deterministico, e propagato attraverso la rete a tutte le parti interessate.

2.2.4 Validatori per le masterchains

Dopo la generazione di nuovi blocchi shardchain, un nuovo blocco masterchain può essere generato. La procedura è essenzialmente la stessa appena presentata per i blocchi shardchain, con la differenza che tutti i validatori (o almeno due terzi dei loro) devono partecipare al processo. Poiché gli headers e le firme dei nuovi blocchi shardchain vengono propagati a tutti i validatori, le hash dei più recenti blocchi in ogni shardchain possono e devono essere inclusi nella nuova masterchain. Una volta che queste hash sono tutte impegnate nel blocco masterchain, gli osservatori esterni e le altre shardchains possono considerare i nuovi blocchi shardchain impegnati e immutabili.

Capitolo 3

I servizi e le applicazioni TON

Qualsiasi progetto di blockchain richiede non solo una specifica del formato dei blocchi e delle regole di convalida della blockchain, come presentate nel capitolo precedente, ma anche di un protocollo di rete utilizzato per propagare nuovi blocchi, inviare e raccogliere i candidati alle transazioni e così via. In altre parole, ogni progetto blockchain deve creare una rete peer-to-peer specializzata.

3.1 TON come progetto multi-blockchain

Mentre le esigenze di rete dei progetti single-blockchain, come Bitcoin o Ethereum, possono essere soddisfatte abbastanza facilmente (bisogna essenzialmente costruire una rete peer-to-peer casuale e propagare tutti i nuovi blocchi e le transazioni candidate tramite un protocollo di gossip), i progetti *multi-blockchain*, come la TON Blockchain, sono molto più esigenti (ad esempio, bisogna essere in grado di sottoscrivere gli aggiornamenti solo di alcune shardchain, non necessariamente di tutte). D'altra parte, una volta che i protocolli di rete più sofisticati necessari per supportare la TON Blockchain sono stati realizzati, si scopre che possono essere facilmente utilizzati per scopi non necessariamente legati alle esigenze immediate della TON Blockchain, fornendo così maggiori possibilità e flessibilità per la creazione di nuovi servizi nell'ecosistema TON, come verrà presentato in seguito.

3.2 Strategie d'implementazione del servizio TON

Si inizia con una discussione su come diverse applicazioni e servizi legati alla blockchain e alla rete possono essere implementati all'interno dell'ecosistema TON. Prima di tutto, è necessario fare delle precisazioni.

Applicazioni e servizi

I termini *applicazione* e *servizio* vengono utilizzati in modo intercambiabile. Tuttavia, esiste una distinzione sottile e un po' vaga: un'applicazione di solito fornisce alcuni servizi direttamente agli utenti umani, mentre un servizio è solitamente sfruttato da altre applicazioni e servizi.

Posizione dell'applicazione: on-chain, off-chain o mista

Un servizio o un'applicazione progettati per l'ecosistema TON devono conservare i propri dati ed elaborarli da qualche parte. Questo porta alla seguente classificazione delle applicazioni (e dei servizi):

- Applicazioni *on-chain*: tutti i dati e l'elaborazione si trovano nella TON Blockchain.
- Applicazioni *off-chain*: tutti i dati e l'elaborazione si trovano al di fuori della TON Blockchain, su server disponibili attraverso la rete di TON.
- Applicazioni *miste*: alcuni dati ed elaborazioni, ma non tutti, si trovano nella TON Blockchain; il resto è su server off-chain che è disponibile attraverso la rete di TON.

Applicazioni centralizzate e decentralizzate

Vi è inoltre l'esigenza di capire se l'applicazione (o il servizio) si basa su un cluster di server centralizzato oppure è realmente distribuito. Tutte le applicazioni on-chain sono automaticamente *decentralizzate* e distribuite. Le applicazioni off-chain e quelle miste possono presentare gradi diversi di *centralizzazione*.

3.2.1 Applicazioni on-chain pure

Uno dei possibili approcci è quello di distribuire un'applicazione (comunemente abbreviata in *dapp*) completamente nella blockchain TON, come uno smart contract o un insieme di smart contracts. Tutti i dati saranno conservati come parte dello stato permanente di questi smart contracts e tutte le interazioni con il progetto avverranno tramite messaggi inviati o ricevuti da questi smart contracts. Questo approccio ha i suoi svantaggi e limiti, ma ha anche dei vantaggi: un'applicazione distribuita di questo tipo non ha bisogno di server su cui girare o di memorizzare i suoi dati (gira nella blockchain, cioè sull'hardware dei validatori) e gode dell'altissima affidabilità e accessibilità della blockchain. Lo sviluppatore di un'applicazione distribuita di questo tipo non ha bisogno di acquistare o noleggiare alcun hardware; tutto ciò che deve fare è sviluppare del software (cioè il codice per gli smart contracts). Dopodiché, affitterà effettivamente la potenza di calcolo dai validatori e la pagherà in monete TON, sia da solo sia facendo ricadere questo onere sulle spalle dei suoi utenti.

3.2.2 Servizi di rete puri

Un'altra opzione estrema è quella di distribuire il servizio su alcuni server e renderlo disponibile agli utenti attraverso il protocollo di rete. In questo modo, il servizio sarà *totalmente off-chain* e risiederà nella rete TON, quasi senza utilizzare la blockchain. La TON Blockchain potrebbe essere utilizzata solo per individuare l'indirizzo del servizio, magari con l'ausilio di un servizio come il TON DNS che verrà trattato nel capitolo successivo.

3.2.3 Servizi misti

Alcuni servizi potrebbero utilizzare un *approccio misto*: fare la maggior parte dell'elaborazione off-chain, ma avere anche una parte on-chain (ad esempio, per registrare i propri obblighi nei confronti degli utenti e viceversa). In questo modo, una parte dello stato verrebbe comunque conservata nella TON Blockchain (cioè un libro mastro pubblico e immutabile) e qualsiasi comportamento scorretto del servizio o dei suoi utenti potrebbe essere punito dagli smart contracts. Un esempio di tale servizio è dato da *TON Storage*. Nella sua forma più semplice, consente agli utenti di conservare i file off-chain, mantenendo sulla catena solo un hash del file da conservare ed eventualmente uno smart contract in cui altre parti accettano di conservare il file in questione per un determinato periodo di tempo a fronte di un compenso prenegoziato.

3.2.4 Servizi misti decentralizzati o fog services

Abbiamo parlato di servizi e applicazioni miste centralizzate. Mentre la loro componente on-chain viene elaborata in modo decentralizzato e distribuito, essendo situata nella blockchain, la loro componente off-chain si affida ad alcuni server controllati dal fornitore del servizio nel solito modo centralizzato. Un approccio decentralizzato all'implementazione della componente off-chain di un servizio consiste nel creare un mercato, in cui chiunque possieda l'hardware necessario e sia disposto ad affittare la propria potenza di calcolo o lo spazio su disco, offra i propri servizi a chi ne ha bisogno. Ad esempio, potrebbe esistere un *registro* (che potrebbe anche essere chiamato *mercato* o *exchange*) in cui tutti i nodi interessati a mantenere i files di altri utenti pubblicano le loro informazioni di contatto, insieme alla capacità di memoria disponibile, alla politica di disponibilità e ai prezzi. Chi ha bisogno di questi servizi può cercarli lì e, se la controparte è d'accordo, creare smart contract nella blockchain e caricare files tramite l'archiviazione off-chain. In questo modo un servizio come TON Storage diventa veramente decentralizzato, perché non ha bisogno di affidarsi a un cluster centralizzato di server per l'archiviazione dei files. Anche la piattaforma *TON Payments* è un esempio di applicazione mista decentralizzata, di cui parleremo nel capitolo 5.

3.3 Connettere utenti e fornitori di servizi

I *fog services* (cioè i *servizi misti decentralizzati*) avranno bisogno quindi di mercati, dove coloro che hanno bisogno di servizi specifici possano incontrare coloro che li forniscono. Tali mercati saranno implementati come servizi on-chain, off-chain o misti, centralizzati o distribuiti.

3.3.1 Registri on-chain, misti e off-chain

Un tale registro di fornitori di servizi potrebbe essere implementato *completamente on-chain*, con l'aiuto di uno smart contract che manterrebbe il registro nella sua memoria permanente. Tuttavia, questo sarebbe piuttosto *lento* e *costoso*. È più efficiente un *approccio misto*, in cui il registro on-chain, relativamente piccolo e raramente modificato, viene utilizzato solo per indicare alcuni nodi, che forniscono servizi di registro off-chain (*centralizzati*). Infine, un *approccio decentralizzato*, puramente off-chain, potrebbe consistere in una rete pubblica, in cui coloro che sono disposti a offrire i propri servizi, o coloro che cercano di acquistare i servizi di qualcuno, semplicemente trasmettono le loro offerte, firmate dalle loro chiavi private.

3.3.2 Registro in una side-chain

Un altro approccio all'implementazione di *registri misti decentralizzati* consiste nella creazione di una blockchain specializzata indipendente (*side-chain*), gestita da un proprio insieme di validatori autoproclamati, che pubblicano le proprie identità in uno smart contract on-chain e forniscono l'accesso in rete a tutte le parti interessate a questa blockchain specializzata, raccogliendo i candidati alle transazioni e trasmettendo gli aggiornamenti dei blocchi attraverso reti dedicate. Quindi ogni nodo completo di questa catena secondaria può mantenere la propria copia del registro condiviso (essenzialmente uguale allo stato globale di questa catena secondaria) ed elaborare interrogazioni arbitrarie relative a questo registro.

3.3.3 Registro in una workchain

Un'ulteriore opzione è quella di creare una *workchain dedicata* all'interno della TON Blockchain, specializzata nella creazione di registri. Questo potrebbe essere più efficiente e meno costoso rispetto all'utilizzo di smart contracts residenti nella workchain di base. Tuttavia, sarebbe comunque più costoso rispetto al mantenimento dei registri nelle side chain.

Capitolo 4

TON DNS

TON DNS è un servizio che permette di tradurre in modo leggibile dall'uomo i nomi dei domini (ad esempio marketplace.ton o candyzoo.gaming.ton) in *TON Network Addresses* per account, smart contract, servizi e nodi network. Proprio come Internet si basa internamente su indirizzi numerici (indirizzi IP) per identificare i diversi computer connessi, varie entità nella rete TON, come ad esempio il portafoglio TON, hanno degli indirizzi grezzi che non sono proprio facili da leggere e ricordare.

4.1 DNS sicuro, privato e decentralizzato

Il servizio tradizionale DNS svolge un ruolo importante nella rete perché le persone si affidano a nomi di dominio leggibili dall'uomo come amazon.com per navigare e trovare ciò di cui hanno bisogno. TON DNS è simile in principio, ma è più *sicuro*, *privato* e completamente *decentralizzato*. Attualmente, i nomi di dominio Internet sono venduti da società a scopo di lucro come GoDaddy che devono detenere il dominio per conto loro. Ciò presenta problemi di privacy poiché anche i domini rappresentati come privati non lo sono rispetto al registrar. Di conseguenza vi sono anche problemi di sicurezza poiché chiunque possa convincere il registrar di essere il proprietario del dominio, può di fatto prenderne il controllo. TON DNS risolve questi problemi eliminando intermediari come GoDaddy. Nella blockchain TON, i domini sono gestiti da *smart contract* invece che da società a scopo di lucro infatti essi vengono acquistati pagando direttamente Toncoin a questi contratti. Nessuno guadagna dalla vendita dei nomi (che sono asset della comunità), poiché tutti i proventi TON vengono distrutti e rimossi dalla circolazione. Le regole della vendita sono trasparenti e immutabili, garantendo un accesso equo ed uguale per tutti. Il sistema è completamente privato, poiché non sono archiviati fattori di identificazione o identità reali in nessun luogo, inoltre è anche completamente sicuro, poiché la proprietà del dominio è rappresentata da un *NFT* che gli utenti detengono personalmente.

4.2 Un protocollo per il networking anonimo

TON DNS porta la visione di una rete privata un passo avanti. Il protocollo di rete sottostante alla rete TON è chiamato *ADNL* e una delle sue caratteristiche è quella di permettere alle entità di rete di rimanere anonime. TON DNS può assegnare nomi leggibili dall'uomo a questi indirizzi ADNL anonimi, rendendoli facili da trovare. Si consideri un sito web come WikiLeaks, che vuole rimanere anonimo per resistere alla censura, ma richiede un nome ben noto per permettere ai suoi lettori di trovarlo. Ogni entità sulla rete TON può essere identificata da TON DNS; da un indirizzo del wallet a un nodo validatore, smart contract o qualsiasi servizio come TON Sites. Per utilizzare TON DNS oggi, gli utenti finali possono installare un'estensione sui principali browser come Chrome o navigare utilizzando server proxy di supporto che traducono automaticamente le richieste. In futuro, ci si aspetta anche di vedere TON DNS incorporato direttamente nei browser web. Si consideri Telegram Messenger, che potrebbe eventualmente supportare direttamente TON DNS e sfruttare la sicurezza, la privacy e la decentralizzazione che offre per facilitare l'adozione di massa.

4.3 TON DNS smart contracts

TON DNS è implementato mediante un albero di smart contract speciali (DNS). Ogni smart contract DNS è responsabile della registrazione di sottodomini di alcuni domini fissi. Lo smart contract *DNS root*, in cui vengono salvati i domini di livello uno del sistema TON DNS, si trova nella masterchain. Il suo identificatore di account deve essere codificato in ogni software che desidera accedere direttamente al database TON DNS. Qualsiasi smart contract DNS contiene una *hashmap*, mappando stringhe UTF-8 di lunghezza variabile terminate da un carattere nullo nei loro "valori". Questa hashmap è implementata come un *albero di Patricia* binario, una struttura dati usata per implementare una tabella hash con chiavi a lunghezza variabile, in cui ogni nodo interno rappresenta un prefisso comune a più chiavi e ogni foglia rappresenta una chiave.

4.3.1 Registrazione di nuovi sottodomini

Per registrare un nuovo sottodominio di un dominio esistente, si invia semplicemente un messaggio allo smart contract, che è il registrar di quel dominio, contenente il sottodominio (cioè la chiave) da registrare, il valore in uno dei vari formati predefiniti, l'identità del proprietario, una data di scadenza e una certa quantità di criptovaluta scelta dal proprietario del dominio. I sottodomini sono registrati sulla base del principio *first-come, first-served*.

4.3.2 Recupero dati da uno smart contract DNS

In principio, qualsiasi full node per la masterchain o la shardchain contenente uno smart contract DNS potrebbe essere in grado di cercare qualsiasi sottodominio nel database di quello smart contract, se la struttura e la posizione

dell'hashmap all'interno dello storage persistente dello smart contract sono note. Tuttavia, questo approccio funzionerebbe solo per alcuni smart contract DNS. Fallirebbe miseramente se venisse utilizzato uno smart contract DNS non standard. Invece, si utilizza un approccio basato su interfacce di smart contract generali e metodi di recupero. Qualsiasi smart contract DNS deve definire un *metodo di recupero* con una "firma nota", che viene invocato per cercare una chiave. Questo approccio ha senso anche per altri smart contract, soprattutto quelli che forniscono servizi on-chain e misti.

4.3.3 Traduzione di un dominio TON DNS

Una volta che ogni full node, agendo da solo o per conto di qualche light client, può cercare voci nel database di qualsiasi smart contract DNS, è possibile tradurre in modo ricorsivo nomi di dominio TON DNS, a partire dall'identificatore dello smart contract DNS root. Ad esempio, se si desidera tradurre A.B.C, si cercano le chiavi .C, .B.C e A.B.C nel database del dominio root. Se la prima di esse non viene trovata, ma la seconda sì e il suo valore è un riferimento a un altro smart contract DNS, allora si cerca A nel database di quello smart contract e si recupera il valore finale.

4.3.4 Accesso ai dati contenuti negli smart contract

Abbiamo già visto che a volte è necessario accedere ai dati memorizzati in uno smart contract senza modificarne lo stato. Se si conoscono i dettagli dell'implementazione dello smart contract, è possibile estrarre tutte le informazioni necessarie dalla memoria persistente di quest'ultimo, accessibile a tutti i full node della shardchain in cui risiede lo smart contract. Tuttavia, questo è un modo non proprio corretto di procedere, dipendente molto dall'implementazione dello smart contract. Un modo migliore sarebbe definire alcuni metodi GET nello smart contract, cioè alcuni tipi di messaggi in ingresso che non influenzano lo stato al momento della consegna, ma generano uno o più messaggi di output contenenti il "risultato" del metodo di recupero. In questo modo, è possibile ottenere dati da uno smart contract, sapendo solo che implementa un metodo di recupero con una firma nota (cioè un formato noto del messaggio in ingresso da inviare e dei messaggi in uscita da ricevere come risultato). Questo modo è molto più elegante e in linea con la programmazione orientata agli oggetti (OOP). Tuttavia, finora presenta un evidente difetto: è necessario effettuare una transazione nella blockchain (inviando il messaggio di recupero allo smart contract), attendere che venga confermata e processata dai validatori, estrarre la risposta da un nuovo blocco e pagare per il gas (cioè per l'esecuzione del metodo di recupero sull'hardware dei validatori). Questo è uno spreco di risorse: i metodi di recupero non modificano comunque lo stato dello smart contract, quindi non è necessario eseguirli nella blockchain.

4.3.5 User interface di uno smart contract

L'esistenza di un'interfaccia pubblica per uno smart contract offre vari vantaggi. Ad esempio, un'applicazione client di un wallet potrebbe scaricare tale interfaccia mentre esamina uno smart contract su richiesta di un utente e visualizzare un elenco di metodi pubblici (ovvero, azioni disponibili) supportati dallo smart contract, forse con alcuni commenti leggibili dall'utente se presenti nell'interfaccia formale. Dopo che l'utente seleziona uno di questi metodi, potrebbe essere generato automaticamente un modulo secondo lo schema TL, in cui all'utente verranno richiesti tutti i campi necessari dal metodo scelto e l'importo desiderato di criptovaluta (ad esempio, monete TON) da allegare a questa richiesta. L'invio di questo modulo creerà una nuova transazione blockchain contenente il messaggio appena composto, inviato dall'account blockchain dell'utente.

In questo modo, sarà in grado di interagire con smart contracts arbitrari dall'applicazione client del wallet in modo user-friendly, compilando e inviando determinati moduli, a condizione che questi smart contracts abbiano pubblicato le loro interfacce. Per quanto riguarda i TON Services, l'unica differenza è che il messaggio serializzato in TL risultante non viene inviato come transazione nella blockchain; al contrario, viene inviato come una query RPC all'indirizzo astratto del "ton-service" in questione e la risposta a questa query viene analizzata e visualizzata secondo l'interfaccia formale (ovvero, uno schema TL).

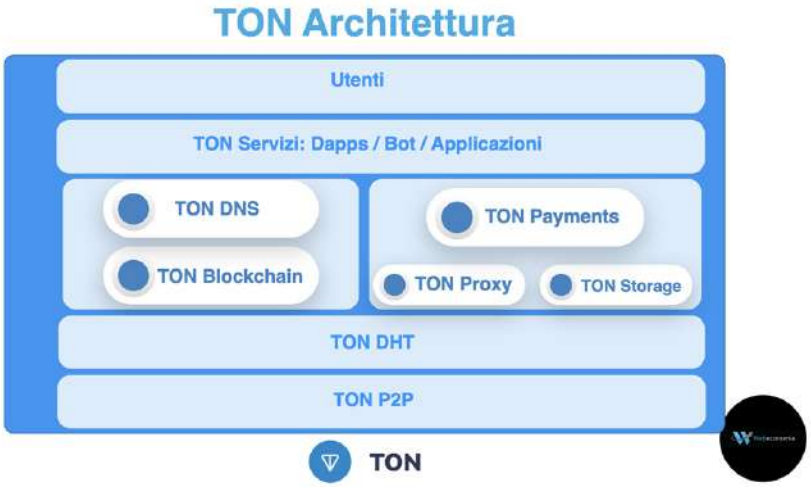


Figura 4.1: Architettura di TON.

Capitolo 5

TON Payments

Ton Payments è una piattaforma che permette di creare canali di micropagamenti, i quali garantiscono pagamenti "istantanei" senza la necessità di pubblicarli tutti sulla blockchain evitando così le fees e di aspettare 5 secondi finché venga inserito il blocco contenente le transazioni

5.1 Payment Channels

Un canale di pagamento è una connessione punto-punto tra due parti, A e B, che sanno di dover effettuare molti pagamenti l'un l'altro nel futuro. Invece di registrare sulla blockchain ogni pagamento come transazione, gli interessati creano una "money pool" condivisa versandoci ognuno del denaro. La money pool è assimilabile a una piccola banca con soli due conti, e tutto ciò si può ottenere con uno smart contract dedicato a cui versare i soldi.

Per iniziare i due interessati si accordano sul protocollo da usare. Loro vogliono tenere traccia dello stato (a,b) della pool, lo stato rappresenta il saldo di ognuno, A inizialmente ha versato a monete mentre B ne ha versate b. Se per esempio A volesse versare d a B il nuovo stato sarebbe (a',b') = (a-d, b+d). Tutti questi trasfermenti sono effettuati off-chain e per nessuno di essi si dovranno pagare fee o attendere i tempi di inserimento del blocco. Nel momento in cui A e B decidessero ritirare il loro saldo dovranno mandare un messaggio con la stato finale su cui sono d'accordo firmandolo entrambi allo smart contract che procederà a versare i saldi corrispondenti allo stato finale. In particolare è da notare la natura di un payment channel che è un mixed service perché risiede in parte sulla blockchain e in parte fuori da essa. Lo smart contract vive sulla blockchain mentre gli scambi di valore sono offchain; in questo modo le due parti potranno effettuare quanti pagamenti vorranno dovendo pubblicare sulla blockchain solo due transazioni, l'apertura e la chiusura dello smart contract.

5.1.1 Trustless Payment Channels

L'esempio precedente benché funzionante prevede che i partecipanti siano collaborativi e non vogliano imbrogliare ma non si possono dare per scontate queste condizioni, bisogna perciò introdurre una modifica al protocollo in maniera da essere usato anche tra chi non ha fiducia reciproca

Per prima cosa il protocollo necessita che gli stati intermedi vengano firmati e inviati all'altro da entrambe le parti. Lo smart contract funziona come un arbitro che gestendo i problemi e confiscando tutti i soldi alla parte colpevole e dandoli alla parte lesa.

5.1.2 Bidiretional synchronous trustless Payment Channels

Un esempio realistico è quello del canale sincrono bidirezionale, questo canale può essere descritto dalla terna: (δ_i, i, o_i) dove i è il sequence number dello stato e parte da zero; δ_i è la "differenza" del canale nel senso che A e B possiedono rispettivamente a+δ_i e b-δ_i e infine o_i è il partecipante autorizzato a generare il prossimo stato. Indipendentemente da chi genera il prossimo ogni stato deve essere firmato da entrambi i partecipanti. In questo tipo di canale di pagamenti sono possibili principalmente due situazioni: A ha vuole effettuare un trasferimento è ha il diritto di generare il prossimo stato, oppure A vuole effettuare un trasferimento è *non* ha il diritto di generare il prossimo stato.

Nel primo caso A semplicemente genera lo stato $S_{i+1} = (\delta_{i+1} - d, i+1, o_{i+1})$ lo firma e lo invia a B che lo firma a sua volta inviandolo di nuovo ad A adesso entrambi hanno uno stato firmato dalle due parti e si può eventualmente effettuare un nuovo trasferimento.

Se invece A non ha il diritto per effettuare il trasferimento perché $o_i = B$, deve prima chiedere a B di firmare uno stato con $\delta_{i+1} = \delta_i$ quindi senza nessun trasferimento se non con il cambiamento $o_i = A$ per dare l'autorità ad A di effettuare il prossimo trasferimento.

Quando si decide di chiudere il canale entrambi firmano l'ultimo stato e lo mandano firmato allo smart contract che effettua i trasferimenti verso i partecipanti, questa procedura è detta *two-sided finalization method*. Ma se uno dei due non firma o non risponde? In questo caso si può ricorrere alla *unilateral finalization* in questo caso si manda allo smart contract la propria versione finale dello stato e la propria firma finale insieme all'ultimo stato firmato da entrambi. A questo punto lo smart contract aspetta un certo tempo di grazia durante il quale l'altra parte può fornire la propria versione finale se questo stato è compatibile con quello dell'altra parte allora si finalizza il contratto, se invece la seconda parte fallisce nel presentare lo stato finale (non è compatibile o non lo manda proprio) il contratto allo scadere del tempo finalizza lo stato finale presentato inizialmente.

Questo protocollo è equo, nel senso che ogni parte può sempre ottenere ciò che le è dovuto, con o senza la cooperazione dell'altra parte, e rischia di perdere tutti i fondi impegnati nel canale di pagamento se tenta di imbrogliare.

5.1.3 Asynchronous payment channel: una blockchain semplice con due validatori

Il canale sincrono discusso presenta un'evidente svantaggio: non si può iniziare la transazione successiva prima che la precedente sia stata confermata dalla controparte. Questo inconveniente può essere risolto sostituendo la singola blockchain generata dagli stati successivi del canale precedentemente descritto con un sistema di due workchain virtuali che interagiscono tra loro.

La prima di queste workchain contiene solo transazioni di A e i suoi blocchi possono essere generati solo da A e lo stato è definito come: $S_i = (i, \phi_i, j, \psi_i)$ dove i è il numero del blocco, ϕ_i è il totale trasferito da A verso B, j è il numero del blocco valido più recente inserito da B di cui A è a conoscenza e infine ψ_i è la quantità totale di soldi trasferiti da B verso A nelle j transazioni. Deve anche far parte dello stato l'hash del blocco precedente della catena di A, l'hash del blocco j della catena di B e la firma con cui B valida il j-esimo blocco. Ogni blocco ha delle condizioni di validità sugli importi:

$\phi_i \geq 0, \quad \phi_i \geq \phi_{i-1} \quad if \quad i = 0, \quad \psi_j \geq 0, \quad -a \leq \psi_j - \phi_i \leq b$

Ora, se A vuole trasferire del denaro a B, crea semplicemente un nuovo blocco nella sua workchain, lo firma e lo invia a B, senza attendere conferme.

Il canale di pagamento viene chiuso quando A firma lo stato finale della sua blockchain (con la sua speciale firma finale), B firma lo stato finale della propria blockchain e vengono presentati questi due stati finali allo smart contract che provvederà alla chiusura del canale.

È possibile anche una finalizzazione unilaterale, ma in questo caso lo smart contract dovrà attendere che l'altra parte presenti la sua versione dello stato finale, almeno per un certo periodo.

Un caso particolare si ha quando l'interazione è tra un service provider e un cliente, in questo caso basa una sola workchain in cui l'user effettua i pagamenti, senza la necessità della seconda catena che permetterebbe anche al provider di inviare soldi all'utente.

5.1.4 Promises

I canali di pagamento per come sono stati definiti offrono la flessibilità, la rapidità e la scalabilità per la maggior parte delle applicazioni ma c'è ancora una necessità, i pagamenti condizionali, ovvero dei pagamenti che si effettuino solo al verificarsi di certe condizioni, nella blockchain ton questi condizioni sono chiamate Promesse. Le promesse possono essere facilmente implementate on-chain da uno smart contract e le si desidera anche per i pagamenti off-chain. I canali di pagamento definiti come workchains sono da intendersi come lo stato che contiene le promesse non ancora soddisfatte e i fondi dovuti a queste promesse in questo caso è necessario che un nuovo blocco sia collegato al precedente tramite l'hash di quest'ultimo, mentre il resto rimane uguale.

5.1.5 TON VM: supporto per "smart" payment channels

Vista l'introduzione degli hash per legare gli stati dei canali di pagamento è necessario che la TON Blockchain e in particolare la TON VM li supporti nativamente. La Merkle Proof è verificata automaticamente dalla workchain e quando lo smart contract accede alla Merkle Proof presentata, che corrisponde a un blocco del canale di pagamento esso la valuterà con la funzione *ev_block* confrontando l'hash fornito con quello calcolato "al momento" del blocco precedente, stabilendone la validità.

Si potrebbe dire quindi che la TON VM è dotata di un supporto integrato per la verifica della validità di altre semplici blockchain.

5.2 Lightning Network

Avendo definito gli smart payment channel possiamo ora discuter il Lightning Netowrk di TON Payments che permette trasferimenti istantanei di valuta tra qualsiasi coppia di nodi partecipanti alla rete.

5.2.1 Limitazione dei Payment Channels

Un canale di pagamento è utile quando le parti si aspettano molti trasferimenti di denaro tra di loro, ma se invece c'è bisogno di trasferire soldi solo una o due volte creare un canale di pagamento non sarebbe pratico e tra le altre cose significherebbe impegnare una importante quantità di soldi nel canale che richiederebbe in ogni caso almeno due transazioni sulla Blockchain TON. Inoltre i canali di pagamento sono stati definiti come connessioni punto-punto tra gli utenti della Blockchain TON ma questo porterebbe ad avere $n \cdot (n-1)$ connessioni.

5.2.2 Payment channel networks, or lightning networks"

Le reti di canali di pagamento superano le limitazioni dei canali di pagamento consentendo trasferimenti di denaro lungo catene di essi. Se A vuole trasferire denaro a E, non ha bisogno di stabilire un canale di pagamento con E. É sufficiente avere una catena di canali di pagamento che collegano A con E attraverso diversi nodi intermedi - ad esempio, quattro canali di pagamento: da A a B, da B a C, da C a D e da D a E.

Una rete di canali di pagamento, viene detta lightning network, consiste in un insieme di nodi partecipanti, alcuni dei quali hanno stabilito tra loro canali di pagamento di lunga durata. Il nodo A che vuole effettuare un pagamento a E deve trovare un percorso che collega A ed E nel lightning network e poi effettua un "chain money transfer".

5.2.3 Chain money transfer

Nei trasferimenti di denaro tramite la rete A non li invia direttamente ad E ma a degli intermediari, come può tutelarsi A ed essere sicuro che quando invierà dei soldi a B, B li invierà a C e così via fino ad arrivare ad E? Per farlo A deve utilizzare le Promesse: ovvero A manda a B la promessa v di inviargli un certo importo quando B gli presenterà il numero u tale che $v = Hash(u)$. B quindi farà la stessa cosa C fino a generare una catena fino ad E. La catena di promesse è tutta vincolata allo stesso $v = Hash(u)$, dopo un certo tempo A invierà a E il numero u per risolvere la promessa che poi risalendo la catena sbloccherà tutte le promesse fino ad A. Le promesse devono avere differenti tempi di scadenza per garantire che se A non dovesse rendere pubblico il risultato nessuno perda i soldi impegnati nella promessa o li incassi senza poi darli al successivo.

5.2.4 Paths nella lightning network

L'ultima cosa che ci resta da discutere è come A ed E possano trovare un percorso che li connetta dentro al lightning netowrk.

Per fare ciò si può usare un protocollo della famiglia OSPF. Tutti i nodi della rete creano una rete sovrapposta e poi tutti i nodi propagano tutte le loro connessioni ai loro vicini. A questo punto tutti i nodi hanno una lista completa di tutti i canali di pagamento nella rete e sono così in grado di calcolare il percorso più breve verso la destinazione desiderata utilizzando l'algoritmo di Dijstra opportunamente adattato tenendo conto ad esempio della massima cifra che può essere trasportata tra due link.

5.2.5 Considerazioni Finali

È stato illustrato come le tecnologie blockchain e di rete del progetto TON sono utilizzate per creare TON Payments, una piattaforma per trasferimenti istantanei di denaro e micropagamenti off-chain. Questa piattaforma può essere estremamente utile per i servizi che risiedono nell'ecosistema TON, consentendo loro di raccogliere facilmente micropagamenti quando e dove necessario.

Capitolo 6

Conclusioni

TON si rivela quindi come una blockchain davvero pensata per ogni tipo di utente: gamers, creators, startup, etc.
Si presenta come un internet decentralizzato e aperto, creato dalla comunità utilizzando una tecnologia progettata da Telegram.
Riferendosi alla trattazione presentata, si vede come Ton sia un'architettura multi-blockchain scalabile in grado di supportare una criptovaluta ampiamente popolare e applicazioni decentralizzate con interfacce user-friendly. Per ottenere la scalabilità necessaria, la TON Blockchain è anche un sistema multi-blockchain strettamente accoppiato con approccio bottom-up allo sharding e inoltre per aumentare ulteriormente le prestazioni potenziali, vi è il meccanismo 2-blockchain per la sostituzione di blocchi.
Infine, Ton propone e rende disponibili ben 537 tra servizi e applicazioni. In particolare la nostra trattazione ha riguardato i TON DNS, un servizio per la traduzione di identificatori di oggetti leggibili dall'uomo nei loro indirizzi, e i TON Payments, una piattaforma per trasferimenti di denaro a catena o istantanei che le applicazioni possono utilizzare per micropagamenti. Questi due servizi sono largamente utilizzati e accessibili in primis all'utente di massa, sottolineando come ancora una volta Ton sia pensata per essere pratica, completa e per ogni tipo di pubblico.

Bibliografia

[1] Durov Nikolai (2019), *Telegram Open Network*.

[2] https://www.fxempire.it/news/article/la-blockchain-ton-di-telegram-in-fase-test-152767

[3] https://www.webeconomia.it/toncoin/

[4] https://ton.org/en/roadmap

[5] https://ton.org/en/apps

SPATIAL

Giorgia delle Grazie, Jacopo Taramasso, Daniele Miola, Gabriele Canova

POLITECNICO DI TORINO
DIPARTIMENTO DI SCIENZE MATEMATICHE
CORSO DI LAUREA IN MATEMATICA PER L'INGEGNERIA

BLOCKCHAIN E CRIPTOECONOMIA

SPATIAL

Giorgia delle Grazie
Jacopo Taramasso
Daniele Miola
Gabriele Canova

ANNO ACCADEMICO 2022/2023

Indice

1 Introduzione 3

2 Virtual Reality e Metaverso 5
- 2.1 Realtà Virtuale . . . 5
  - 2.1.1 Storia . . . 5
- 2.2 Metaverso . . . 7
  - 2.2.1 Origini del metaverso . . . 7
  - 2.2.2 Il metaverso di Facebook . . . 7
- 2.3 Metaverso come strumento educativo . . . 10

3 Spatial e NFT 12
- 3.1 Crypto art . . . 12
  - 3.1.1 Approfondimento sugli NFT . . . 12
  - 3.1.2 Come creare un NFT . . . 14
- 3.2 Wallet in Spatial . . . 15
  - 3.2.1 MetaMask . . . 15
  - 3.2.2 Solana wallet . . . 16
  - 3.2.3 Come caricare un wallet su Spatial . . . 17
- 3.3 3D NFT . . . 18
  - 3.3.1 Introduzione agli NFT 3D . . . 18
  - 3.3.2 NFT Envirometns . . . 19
- 3.4 Creator toolkit e modelli predefiniti . . . 20

4 NFT e ambiente 21
- 4.1 "Climate-positive" NFT . . . 21
- 4.2 Progetti "climate-positive" su Spatial . . . 23

5 Spatial environment 25
- 5.1 Come interagire su spatial . . . 25
- 5.2 Eventi ospitati su spatial . . . 25
- 5.3 Piani a pagamento . . . 26
- 5.4 Confronto con altri metaversi . . . 27

6 Conclusioni 29

Bibliografia 30

Capitolo 1

Introduzione

Il metaverso è una visione di ciò che molti nell'industria informatica credono sia la prossima frontiera dell'internet che conosciamo: uno spazio virtuale condiviso, immersivo, persistente e tridimensionale in cui gli esseri umani vivono vere e proprie esperienze. Per alcuni aspetti possiamo considerare il metaverso una trasposizione del mondo reale pur essendo però un agglomerato di elementi reali e digitali, virtualizzazioni tridimensionali di oggetti fisici. L'accesso a questa nuova realtà è possibile per mezzo di internet e dispositivi hardware capaci di interagire con le piattaforme esistenti.
La recente pandemia Covid-19 ha evidenziato come, malgrado la socialità possa venire limitata, le tecnologie digitali offrono alternative valide mettendo a disposizione ambienti virtuali su cui socializzare, esperienze condivise e accessibilità a livello geografico. Tra i vari metaversi, Spatial si distingue in modo particolare per la semplicità con cui gli utenti possono creare, condividere e quindi interagire con altri utenti senza necessariamente essere esperti del settore.

Figura 1.1. Creative Owls: International Women's Day Artist Spotlight [17]

Spatial è stata fondata nel 2016 da Anand Agarawala e Jinha Lee, ed i loro investitori iNovia Capital, White Star Capital, Expa, Kakao Ventures, Lerer Hippeau, Leaders Fund, Samsung NEXT, oltre a privati tra cui Mark Pincus (fondatore di Zynga), Andy Hertzfeld (co-inventore di Macintosh) e Mike Krieger (co-fondatore di Instagram).
Spatial viene gestito da un team di esperti di MetaVerse e designer 3D distribuito su tutto il territorio degli Stati Uniti, con sede a New York.
Nasce con l'intenzione di dare l'opportunità agli utenti di creare ambienti virtuali in cui incontrarsi, socializzare, imparare e godere di esperienze culturali di gruppo. Alle aziende è offerta la possibilità ad aziende di sfruttare questi spazi virtuali per condividere progetti, il tutto utilizzando la tecnologia blockchain per monetizzare i propri prodotti.
Per partecipare al metaverso spatial è necessario utilizzare un browser web, un dispositivo mobile (iOS/Android) o un visore VR grazie al supporto cross-platform offerto.
A rendere più semplice ancora la condivisione delle proprie realtà all'interno di Spatial, si possono invitare partecipanti da ogni parte del mondo, permettendo loro l'accesso tramite link privati e personalizzati.[13].

Figura 1.2. iTeacher: Education Metaverse by Andrew Wright [17]

Capitolo 2

Virtual Reality e Metaverso

2.1 Realtà Virtuale

Con il termine realtà virtuale (a volte abbreviato in VR dall'inglese virtual reality) si identificano vari modi di simulazione di situazioni reali mediante l'utilizzo di computer e l'ausilio di interfacce appositamente sviluppate [1].
L'avanzamento delle tecnologie informatiche ha permesso di navigare in ambientazioni fotorealistiche in tempo reale, interagendo con gli oggetti presenti in esse.
Anche se, a livello teorico, la realtà virtuale potrebbe essere costituita attraverso un sistema totalmente immersivo in cui tutti i sensi umani possono essere utilizzati (più specificamente realtà virtuale immersiva o RVI), attualmente il termine viene applicato a qualsiasi tipo di simulazione virtuale creata attraverso l'uso del computer, dai videogiochi che vengono visualizzati su un normale schermo, alle applicazioni che richiedono l'uso degli appositi guanti muniti di sensori (wired gloves), l'utilizzo di visori o della semplice connessione ad internet.

2.1.1 Storia

Morton Heilig, già dalla metà del XX secolo, parlò del cosiddetto "cinema esperienza" (Experience Theater, come lo definì lui) che poteva coinvolgere tutti i sensi in maniera realistica, immergendo lo spettatore nell'azione che si svolgeva sullo schermo. Costruì un prototipo della sua visione, chiamato Sensorama, nel 1962, insieme a cinque film che questo apparecchio proiettava e che coinvolgevano molti sensi (vista, udito, olfatto, tatto). Costruito prima dei computer digitali, il Sensorama era un dispositivo meccanico che funziona ancora oggi.

Figura 2.1. The Sensorama VR machine [20]

Nel 1968 Ivan Sutherland, con l'aiuto del suo studente Bob Sproull, creò quello che è considerato il primo sistema di realtà virtuale con visore. Era primitivo sia in termini di interfaccia utente sia di realismo, il visore da indossare era così pesante da dover essere appeso al soffitto e la grafica era costituita da semplici stanze in wireframe. L'aspetto di quel dispositivo ne ispirò il nome, La Spada di Damocle.

Figura 2.2. La Spada di Damocle [20]

Il primo passo decisivo verso l'ipermedia, e il primo dispositivo che possa essere considerato di realtà virtuale è stato l'Aspen Movie Map realizzato sotto forma di software dal MIT nel 1977. Il principale scopo di questo simulatore era ricreare virtualmente Aspen, cittadina del Colorado; agli utenti era concesso di camminare per le vie in modalità estate, inverno e in modalità poligonale. Mentre le prime due modalità erano indirizzate alla replica di filmati delle strade della cittadina, la terza si basava su una poligonazione tridimensionale, con una grafica scarsa visti i limiti tecnologici di allora.

La nascita del termine VR, Virtual Reality, risale al 1989, anno in cui Jaron Lanier, uno dei pionieri in questo campo, fondò la VPL Research (Virtual Programming Languages, "linguaggi di programmazione virtuale"). Il concetto di cyberspazio, ad esso collegato strettamente, si era originato nel 1982 grazie allo scrittore statunitense William Gibson.

Con le tecnologie attuali, la percezione di un mondo virtuale è ancora distinguibile da quella del mondo reale: il fotorealismo delle immagini rende completa o quasi l'esperienza visiva, tuttavia gli altri sensi sono parzialmente trascurati (olfatto e tatto, ad esempio, sono poco stimolati). È chiaro che tra le varie tipologie di ambiente che possono essere proposte attraverso la realtà virtuale, sono quelli 3D a ricevere e a veicolare oggi un maggior interesse. Questo sembra derivare prevalentemente dal fatto che nell'uomo è la vista il senso dominante, motivo per cui gli ambienti virtuali devono essere caratterizzati innanzitutto da qualità visive eccelse, capaci quindi di presentarsi anche come sostituti della realtà, mentre invece gli altri sensi sembrano avere, almeno agli esordi della realtà virtuale, un peso meno influente.

Molto usato in ambito culturale negli anni novanta del XX secolo, il termine realtà virtuale è stato poi eccessivamente utilizzato fino a produrre l'effetto opposto e a cadere in disuso.

Assume particolare importanza e rilevanza la realtà aumentata (augmented reality) che si basa sull'ampliamento o sull'integrazione della realtà circostante con immagini generate al computer, che modificano l'ambiente originario senza influire sulle possibilità di interazione.

Il mercato di AR / VR è già diventato un mercato da un miliardo di dollari e si prevede che continuerà a crescere ben oltre i $120 miliardi entro pochi anni.

2.2 Metaverso

Il metaverso comprende qualsiasi esperienza digitale su Internet che sia persistente, immersiva, tridimensionale (3D) e virtuale, che non accade nel mondo fisico. Con il termine persistente si intende la costante presenza del fruitore dell'esperienza all'interno del mondo virtuale. Per immersiva si fa riferimento al totale coinvolgimento di tutti e cinque i sensi durante "l'immersione". Infine, la tridimensionalità e la virtualità sono caratteristiche intrinseche e proprie del Metaverso. Le esperienze che "viviamo" nel Metaverso ci offrono l'opportunità di giocare, lavorare, connetterci o acquistare e solo per rendere le cose ancora più coinvolgenti, le cose che acquistiamo possono essere reali o virtuali. [2]
Forse è anche improprio dire "il Metaverso" come se fosse un universo unico, connesso o addirittura interoperabile, perché non lo è. Ogni entità che crea un mondo virtuale lo fa con il proprio accesso, appartenenza, diritti di monetizzazione e formati di espressione creativa; quindi, le specifiche tecniche e aziendali variano notevolmente. Perciò, il Metaverso non è un luogo specifico, è il nome che si dà a tutti quei "mondi" virtuali nei quali si accede tramite computer, joystick o sensori.
Il numero di questi mondi è in costante aumento. Cominciando dai primi che sono nati, TheSandbox e Decentraland, e attualmente i più noti e di più facile accesso, si può notare quanto questi metaversi abbiano già sconvolto, o perlomeno cambiato, le abitudini di numerose persone.

2.2.1 Origini del metaverso

Le origini teoriche del metaverso si collocano nella letteratura fantascientifica e quindi nella fantasia umana più che in un progetto concreto. In particolare, la teorizzazione del metaverso viene ricondotta al celebre romanzo cyberpunk Snow Crash di Neal Stephenson, pubblicato nel 1992.
La storia raccontata nel libro parla di un hacker di nome Hiro, che per vivere lavora come fattorino delle pizze per l'azienda che domina il mercato delle consegne a domicilio in una Los Angeles futuristica, dove le istituzioni sono state sostituite dalle grandi corporazioni internazionali che governano le porzioni di territorio che hanno conquistato. In questo contesto si colloca il Metaverso, uno spazio libero con strade, locali, negozi, creato da alcuni programmatori indipendenti, e al cui interno le persone interagiscono e si spostano tramite i loro avatar.
Questo mondo digitale assorbe le vite delle persone, costringendole a vivere un'esistenza alternativa per sfuggire ad una realtà difficile in minuscoli appartamenti. Il metaverso diventa quindi uno spazio aperto e libero che si contrappone ad una vita reale claustrofobica. In questo spazio, la differenza tra le classi sociali è rappresentata dalla risoluzione del proprio avatar e dalla possibilità di accesso a luoghi esclusivi.
Nel tempo, molti hanno provato a riprodurre quanto immaginato da Stephenson, soprattutto nel mendo videoludico. Si pensi, ad esempio, al videogioco Second Life lanciato nel 2003, dove gli utenti accedono al mondo virtuale attraverso il loro avatar, potendo esplorare, telatrasportarsi da un punto all'altro di una mappa, comunicare con gli altri utenti, e partecipare a mostre, raduni o concerti. [3]

2.2.2 Il metaverso di Facebook

Facebook è una delle più grandi piattaforme sociali al mondo ed è stata fondamentale nel rendere mainstream il concetto di metaverso. Facebook ha investito in modo significativo nello sviluppo del metaverso e ha adottato una serie di iniziative per entrare in questo spazio emergente.

Una delle prime mosse di Facebook nel metaverso è stata l'acquisizione di Oculus VR nel 2014. Oculus è un'azienda specializzata nella realtà virtuale, conosciuta per i suoi dispositivi come l'Oculus Rift e l'Oculus Quest. Questa acquisizione ha permesso a Facebook di entrare nel settore

della realtà virtuale e di sfruttare la tecnologia per creare esperienze immersive all'interno del metaverso.

Successivamente, Facebook ha introdotto Horizon, una piattaforma di social VR progettata per consentire agli utenti di creare e condividere esperienze virtuali interattive. Horizon permette agli utenti di creare avatar personalizzati e di esplorare mondi virtuali con altri utenti. È possibile partecipare a giochi, eventi, esplorare ambienti virtuali e socializzare con persone provenienti da tutto il mondo. Facebook ha aperto un programma di accesso anticipato a Horizon per consentire agli utenti di sperimentare la piattaforma e fornire feedback per migliorarla.

Nel 2021, Mark Zuckerberg, CEO di Facebook, ha annunciato l'obiettivo a lungo termine dell'azienda di trasformarsi in un'azienda "metaversale" cambiando anche il nome dell'impresa in Meta. Ha affermato inoltre che il metaverso rappresenta la prossima grande piattaforma di condivisione dopo i telefoni cellulari e le reti sociali. Zuckerberg ha anche evidenziato il ruolo che il metaverso potrebbe giocare nell'offrire nuove opportunità economiche, sociali e creative.

Facebook ha iniziato a implementare elementi del metaverso sulla sua piattaforma principale. Ad esempio, gli utenti possono già partecipare a esperienze virtuali come eventi in live streaming, tour virtuali, giochi sociali e altro ancora. La piattaforma di realtà aumentata di Facebook, Spark AR, consente agli sviluppatori di creare filtri e effetti interattivi che possono essere utilizzati durante le chiamate video o condivisi nelle storie.

Problemi e preoccupazioni

Mentre Facebook si impegna a entrare nel metaverso e sviluppare esperienze innovative, ci sono diversi problemi e preoccupazioni che possono sorgere lungo il percorso. Di seguito sono elencati alcuni dei principali problemi del metaverso di Facebook ma che possono essere estesi anche ad altri metaversi:

- **Controllo centralizzato**: Uno dei principali problemi del metaverso di Facebook è il controllo centralizzato dell'azienda sulla piattaforma. Facebook detiene un'enorme quantità di dati personali degli utenti e questa concentrazione di potere solleva preoccupazioni sulla privacy e sulla sicurezza. Gli utenti potrebbero temere che Facebook utilizzi i dati personali raccolti nel metaverso per scopi pubblicitari o per influenzare le decisioni degli utenti, come già accusati in precedenza.
- **Monopolio e concorrenza**: Facebook è già una delle piattaforme sociali più dominanti al mondo, e la sua entrata nel metaverso potrebbe portare a un ulteriore consolidamento del suo potere. Ciò potrebbe limitare la concorrenza e ostacolare lo sviluppo di alternative più aperte e decentralizzate nel metaverso. Questo potrebbe avere conseguenze negative sulla diversità delle esperienze e sull'innovazione nel settore.
- **Esclusione digitale**: L'accesso al metaverso richiede l'utilizzo di dispositivi tecnologici come occhiali intelligenti o visori VR. Questi dispositivi possono essere costosi e non accessibili a tutti. Ciò potrebbe creare una disparità digitale, con alcune persone che hanno accesso privilegiato al metaverso, mentre altre rimangono escluse. Inoltre, ci potrebbero essere sfide per le persone con disabilità nel godere pienamente delle esperienze del metaverso, a meno che non siano state prese in considerazione soluzioni di accessibilità.
- **Dipendenza e impatto sulla salute mentale**: Facebook e altri social media sono già stati oggetto di critica per il loro impatto sulla salute mentale degli utenti. L'immersione nel

metaverso potrebbe portare a una maggiore dipendenza e isolamento sociale. È importante considerare le implicazioni per la salute mentale degli utenti e adottare misure per mitigare gli effetti negativi.

- **Controllo delle informazioni e disinformazione**: Con l'ingresso di Facebook nel metaverso, sorge la preoccupazione riguardo al controllo delle informazioni e alla diffusione della disinformazione. Con un'enorme base di utenti e la capacità di influenzare l'accesso alle informazioni, Facebook potrebbe avere un impatto significativo sulla verità e sulla manipolazione delle notizie nel metaverso. È essenziale affrontare questi problemi per garantire un ambiente informativo e affidabile.

- **Sicurezza e cybercrime**: Il metaverso potrebbe presentare nuove sfide per la sicurezza digitale. La presenza di una vasta comunità di utenti interagente nel metaverso potrebbe essere sfruttata da malintenzionati per attività come frodi, hacking o abusi. È fondamentale che Facebook implementi robuste misure di sicurezza per proteggere gli utenti e prevenire l'abuso nel metaverso.

- **Interoperabilità e standard aperti**: Con l'espansione del metaverso, è importante garantire l'interoperabilità tra diverse piattaforme e promuovere standard aperti. Ciò consentirebbe agli utenti di muoversi liberamente tra i diversi mondi virtuali e favorirebbe la concorrenza e l'innovazione nel settore. Facebook deve evitare di creare un metaverso chiuso e lavorare per promuovere l'interoperabilità e la collaborazione con altre aziende e progetti nel settore.

2.3 Metaverso come strumento educativo

Durante la pandemia, il settore dell'istruzione ha affrontato gravi difficoltà a livello globale. Circa il 91% degli studenti di 192 paesi, pari a circa 1,6 miliardi di persone, ha subito interruzioni nel proprio percorso educativo. Per affrontare questa situazione critica, il mondo dell'istruzione ha cercato soluzioni, come ad esempio l'implementazione diffusa di piattaforme educative. Tuttavia, tali soluzioni non hanno raggiunto tutti gli studenti, dato che il 29% dei giovani nel mondo, corrispondente a circa 364 milioni di individui, non ha ancora accesso a Internet. Questa disparità digitale ha causato una perdita di migliaia di ore di lezioni per questi studenti, amplificando ulteriormente il divario digitale. L'attuale sfida dell'istruzione consiste nel rendere l'apprendimento online una componente integrale dell'educazione. Ciò dovrebbe portare a soluzioni pedagogiche più inclusive e creative, come la creazione di un ecosistema virtuale di centri di ricerca: è qui che nasce l'Eduverso.

Il problem solving e le abilità di comunicazione possono essere sviluppate in diversi contesti educativi. Ad esempio, un ambiente virtuale può offrire un'opportunità di apprendimento coinvolgente.
La Figura 2.3 offre una rappresentazione visiva di un check-in con informazioni sui voli.

Figura 2.3. The Airport Departure "experience" (Image Credit: IMMERSE)

A seconda dello scenario gli studenti hanno modo di apprendere attraverso l'esperienza diretta, aumentando quello che è il valore educativo:

- **Apprendimento esperienziale**: gli studenti possono sperimentare un ambiente simulato che richiede loro di affrontare scenari e problemi realistici incrementando l'apprendimento pratico e l'acquisizione di competenze attraverso esperienza diretta.

- **Collaborazione**: in contesti diversi gli studenti possono interagire assumendo ruoli diversi, viene incoraggiata la creatività e la collaborazione. Inoltre, assume valore aggiunto la comunicazione efficace e il relativo sviluppo di abilità sociali, necessarie alla vita reale.

- **Flessibilità e adattabilità**: potendo cambiare ruolo all'interno della simulazione didattica viene necessario l'adattamento e la comprensione delle diverse prospettive e responsabilità dei vari attori coinvolti.

- **Pensiero critico e problem solving**: in ultimo lo studente è coinvolto in prima persona in una 'sfida', vi è necessità di analisi critica, valutazione e risoluzione dei problemi attraverso soluzioni efficaci.

Risulta chiaro che vi sia la possibilità di affiancare il tradizionale approccio alla conoscenza "learning by book" ad un modo nuovo, in cui l'interazione diretta con i contenuti offre un approccio "learning by doing", coinvolgente ed efficace. Il metaverso costituisce pertanto una grandissima opportunità per l'educazione e la divulgazione scientifica, un'opportunità ancora da esplorare che ha potenzialità ancora tutte da scoprire. I vantaggi e le opportunità dell'educazione scientifica nel metaverso vanno oltre gli aspetti tecnologici ed esperienziali, contribuendo anche al progresso socio-economico e aprendo nuove strade per la sostenibilità e l'inclusione.

Secondo un articolo di Forbes intitolato "How The Metaverse Can Make Science Learning More Accessible", il metaverso offre almeno tre grandi opportunità per l'educazione tecnico-scientifica.

- **Accessibilità**: I tradizionali sistemi di insegnamento hanno dimostrato limiti nell'offrire un'adeguata educazione scientifica a categorie specifiche, come coloro che soffrono di disturbi cognitivi. Nel metaverso, è possibile costruire mondi virtuali ad hoc, consentendo a ogni individuo di godere di un'esperienza di formazione personalizzata in un ambiente sicuro e controllato. Questi vantaggi si applicano anche alla produzione di esperienze virtuali personalizzate per diversi tipi di pubblico, inclusi i ricercatori, che possono utilizzare strumenti per simulare rapidamente gli effetti di esperimenti scientifici e valutare molteplici alternative.

- **Diversità**: Il metaverso può contribuire a superare i tradizionali stereotipi di genere nel campo delle discipline STEM, incoraggiando un maggior coinvolgimento delle donne nella formazione scientifica. Inoltre, il metaverso può favorire l'inclusione di individui che vivono in aree svantaggiate o in paesi in via di sviluppo, offrendo loro risorse educative che altrimenti sarebbero difficili da ottenere. La formazione di una comunità globale in grado di sostenere lo studio di determinati argomenti attraverso l'uso di applicazioni digitali avanzate è fondamentale per superare le barriere culturali e valorizzare la diversità nel campo delle discipline STEM.

- **Opportunità economiche**: L'educazione scientifica nel metaverso consente di raggiungere un vasto pubblico grazie alla riduzione dei costi garantita dalle applicazioni digitali. Molte università di prestigio offrono piattaforme che consentono agli studenti di accedere a risorse e esperienze interattive senza dover frequentare fisicamente i corsi. Questa modalità di apprendimento a distanza, resa ancora più evidente durante la pandemia di COVID-19, riduce i costi rispetto alla frequenza tradizionale in sede.

Capitolo 3

Spatial e NFT

3.1 Crypto art

Spatial sta vivendo una crescente popolarità soprattutto grazie agli NFT e le crypto art. Con il termine **crypto art** ci si riferisce a tutte quelle forme artistiche che prevedono la digitalizzazione di un'opera fisica oppure una creazione di un'opera digitale. Ad ogni opera d'arte viene associato un NFT, ovvero codici crittografici che ne certificano la provenienza e le proprietà. Trasferire un token equivale a cedere il certificato di proprietà di un bene, questo però non significa aver acquistato il diritto di rivendicare il copyright o di utilizzare l'opera per scopi commerciali senza il permesso dell'artista. Il funzionamento della crypto art in relazione alla blockchain segue i seguenti step [11]:

- un artista crea un'opera e la carica e viene caricata all'interno di una galleria virtuale;
- lo smart contract della galleria blockchain scelta (Ethereum, Binance Smart Chain) crea un NFT associata all'opera e trasferisce questo token nel portafoglio digitale dell'artista;
- la galleria memorizza il file dell'opera sulla rete peer-to-peer, in modo tale che né il token nè l'opera sono su alcun server;
- i collezionisti possono fare delle offerte per l'acquisto dell'opera trasferendo l'importo nello smart contract della galleria;
- infine l'artista accetta una delle offerte ricevute: il token viene trasferito dallo smart contract della galleria nel portafoglio dell'offerente e la criptovaluta concordata nel portafoglio dell'artista.

3.1.1 Approfondimento sugli NFT

L'utilizzo degli NFT non solo fornisce un modo per autenticare il lavoro di un'artista ma consente di vedere e scambiare le proprie creazioni in un nuovo e entusiasmante mercato. Inoltre, l'artista dell'opera riceve il 100% dei proventi della vendita.
A differenza dell'arte fisica la quale viene riconosciuta attraverso una firma o numerandola, l'arte digitale può essere replicata all'infinito.
Questo ha portato ad una svalutazione dell'arte digitale e la creazione degli NFT, attraverso il cosiddetto 'minting' (processo di creazione di un NFT) e l'attribuzione di un identificatore unico al file digitale il quale viene memorizzato sulla blockchain, rendono la duplicazione o contraffazione impossibile. Per questo motivo diversi enti stanno iniziando a creare NFT per iscrizioni, pass per eventi e altro ancora. Questo dimostra l'autenticità di un oggetto, traccia una proprietà e

permette di trasferire informazioni più facilmente.
Un NFT può avere un solo proprietario alla volta e sapere come crearne uno fornisce agli artisti uno strumento per proteggere e monetizzare il proprio lavoro in modo più efficace. Ma anche i compratori traggono vantaggio dall'utilizzo di tali token perché diventano proprietari di un oggetto originale creato da un artista.

Figura 3.1. 1111 Gallery [15]

Fino a settembre 2022, le cinque vendite di NFT più note sono [12]:

- "The Merge" di Pak, venduto il 2 dicembre 2021 su Nifty Gateway per l'equivalente di 91,8 milioni di dollari a quasi 29.000 collezionisti. L'NFT è diventato contemporaneamente il NFT più costoso mai venduto e uno dei metodi di vendita e creazione di valore più innovativi.

- "Everydays: The First 5000 Days" è una collezione di opere d'arte iniziata nel 2007 dal rinomato artista digitale Beeple. Nel 2021, ha coniato tutta la sua opera fino a quel punto, creando un NFT che è stato venduto da Christie's per 69 milioni di dollari, diventando il NFT più costoso venduto a un singolo proprietario e il secondo più costoso in assoluto.

- "Human One" è un'altra opera d'arte digitale di Beeple. Descritto come una scultura video 3D custodita in una scatola alta 7 piedi, l'artista lo ha definito il "primo ritratto di un umano nato nel metaverso". L'NFT corrispondente è stato venduto a Christie's nel novembre 2021 per l'equivalente di 25 milioni di dollari.

- "CryptoPunk" #7523 (popolarmente conosciuto come "Masked Alien" o "Covid Alien") è il terzo NFT singolo più raro nella collezione CryptoPunks. È solo 1 su 9 nella collezione Alien Punks ed è stato venduto da Sotheby's nel giugno 2021 per 11,8 milioni di dollari.

- "Doge" è un popolare meme di Internet che esiste da oltre un decennio. L'anno scorso, il servizio fotografico originale con il popolare e amato Shiba Inu è stato venduto all'asta per 4 milioni di dollari. Dopo la vendita, l'NFT è stato suddiviso in 17 miliardi di pezzi e ha raggiunto una valutazione di oltre 300 milioni di dollari.

3.1.2 Come creare un NFT

Prima di creare un NFT bisogna prima decidere cosa rappresenta, l'operazione di conversione prende il nome di tokenizzazione. Tra le opere convertibili è possibile trovare [12]:

- Arte digitale
- Musica
- Video
- Meme
- Testo
- Abbigliamento
- Biglietti
- Altro

Lo step successivo è trovare dove vendere gli NFT.
Sapere invece dove venderli dipende in gran parte dalla piattaforma utilizzata. Esistono diverse piattaforme per la conversione degli NFT, ma per selezionarne una è necessario capire quale criptovaluta si vuole usare, a quanto corrisponde il costo per la creazione di un NFT su tale piattaforma, se è presente una tariffa aggiuntiva per tale operazione e infine se ci sono delle restrizioni dovute ai tipi di contenuti.
Solitamente il prezzo medio per la creazione di un NFT parte da 0.05 $ arrivando anche a 150 $, ciò dipende dalla blockchain selezionata.
Generalmente Ethereum è la blockchain con il prezzo maggiore per la creazione di un NFT, raggiumgendo i 70$, mentre se si sceglie di utilizzare Solana si arriva a spendere 0.01$. Polygon permette la creazione di un NFT senza costi aggiuntivi così come per certi tipi di asset che vengon convertiti in OpenSea. Questi prezzi dipendono principalmente dalle fees necessarie all'utilizzo della rete stessa.
Quando si decide che tipo di blockchain usare è importante considerare quali di queste possiedono i potenziali acquirenti, perchè se ad esempio questi ultimi effettuano transazioni tramite Ethereum mentre venditori hanno convertito i propri asset sulla rete Polygon, questo comporterebbe alla riduzione delle vendite.
È possibile creare il proprio smart contract e vendere i propri NFT gratuitamente, ma ciò è raccomandato solo per sviluppatori esperti.
Una volta selezionata la piattaforma che rispecchie le esigenze del cliente è possibile in seguito collegare i propri portafogli crittografici come: MetaMask, Formatic e Coinbase Wallet.
A questo punto è possibile caricare i propri file digitali e creare i propri NFT seguendo le istruzioni della piattaforma selezionata. Per la maggior parte delle piattaforme è possibile aggiungere più NFT in un set, gruppo o collezione.
Altre richiedono agli artisti di creare gli NFT e pagare una tassa per tale operazione, una volta ricevuto il pagamento la piattaforma converte l'opera in NFT e lo inserisce nell'elenco sul mercato. Questo modello può essere adottato da alcune piattaforme per coprire i costi di creazione e di gestione della piattaforma stessa.
Altre piattaforme invece pubblicano l'elenco senza pagare tasse ma addebitano una commissione sulle transazioni di vendita.
Un possibile modo utilizzato per vendere gli NFT è quello di considerare un **prezzo fisso** ovvero si imposta un costo prefissato associato ad un singolo o ad un gruppo di NFT tramite il metodo FIFO *first in first out* . Dopo aver effettuato l'acquisto il token viene eliminato dalla lista e

consegnato al suo nuovo propreitario.
Le **aste** sono un altro metodo con cui è possibile diventare proprietari di un'opera d'arte digitale. Si associa un valore iniziale al bene e si decide la durata tale evento, al termine del quale si consegna il token al miglior offerente.
A differenza di un'asta normale il prezzo di partenza non è necessariamente il valore minimo che si può offrire. Acquirente e venditore possono concordare il prezzo di vendita [12].

Le varie piattaforme possono avere politiche diverse su come creare gli NFT e venderli ma l'idea generale è sempre la stessa.

- Si carica un file
- si associa un NFT ad esso
- lo si inserisce in un elenco di mercato online

Da questo momento in poi gli acquirenti possono acquistare il proprio NFT utilizzando la criptovaluta preferita. Una volta creati gli NFT questi sono pronti per essere visualizzati ed esposti.
Una possibile opportunità è quella di creare la propria galleria d'arte virtuale su Spatial in cui è possibile costruire una comunità intorno al lavoro di un'artista o collezionista.
In Spatial è sufficiente selezionare il modello della propria galleria e scegliere le opere d'arte che si vogliono mostrare.
Un'altra alternativa può essere quella di collegare il proprio portafoglio MetaMask e posizionare le immagini ovunque in una stanza prescelta.

3.2 Wallet in Spatial

All'interno di Spatial è possibile collegare il proprio portafoglio digitale, consentendo agli utenti di accede e gestire in modo efficiente i propi asset digitali all'interno dell'ambiente virtuale. Grazie a questa funzionalità, gli utenti possono effettuare operazioni di acquisto, vendita o scambio di NFT e token in modo continuo e senza interruzioni. Tale funzionalità rappresenza una soluzione efficiente per la gestione degli asset digitali.

3.2.1 MetaMask

MetaMask è un'applicazione di portafoglio che funzione come un'estensione del browser, consentendo agli utenti di conservare in modo sicuro le proprie chiavi private di Ethereum.
Grazie alla sua funzionalità di portafoglio per Ether e altri token, MetaMask consente agli utenti di interagire con numerose applicazioni decentralizzate e con gli smart contract.
Ciò che distingue MetaMask da altri portafogli digitali è la sua caratteristica di non richiedere alcuna informazione personale, come password o indirizzo email. Questa caratteristica rende MetaMask un'opzione conveniente e sicura per gli utenti che desiderano gestire i propri asset digitali.
Le principali caratteristiche di questo portafoglio possono essere riassunte nei seguenti punti:

- compatibilità con le blockchain che usano Ethereum Virtual Machine, cioè gli utenti possono accedere a una vasta gamma di applicazioni decentralizzate e interagire con gli smart contract
- la possibilità di creare vari account per gestire crypto in diversi account garantendo una certa flessibilità per le gestione degli asset digitali
- funzionalità per lo scambio dei token, garantendo agli utenti una gestione sicura delle proprie transazioni

- funzionalità di staking (ovvero un metodo di guadagno passivo), consentendo agli utenti di guadagnare interesse sui prorpi asset digitali

3.2.2 Solana wallet

La blockchain Solana rappresenta una rinomata rete utilizzata per le transazioni nell'ambito degli NFT.
Essendo stata progettata per essere efficiente dal punto di vista energetico, il consumo di energia di Solana risulta essere inferiore rispetto ad altre blockchain, rendendola ideale per l'acquisto o la vendita di asset digitali.
All'interno di Spatial. gli utenti possono facilmente collegare il proprio Solata wallet e caricare i propri NFT.
Nella scelta di un wallet per conservare i propri NFT Solana, è necessario considerare diversi aspetti tra cui il costo, l'interfaccia, la cinvenienza, la complessità dell'apprendimento e altri fattori.
Spatial consente di caricare un Solana wallet, offrendo agli utenti una selezione di wallet tra cui scegliere [14]:

Ledger

Questo wallet è considerato il più sicuro e versatile in quanto consente di acquistare, vendere o caricare un NFT senza il rischio di perdere i propri asset a causa di eventuali attacchi informatici. Grazie alla sua funzionalità di inserimento offline delle informazioni private, il Ledger wallet rappresenta la soluzione ideale per garantire la massima sicurezza nella gestione degli asset digitali. Infatti, tutti gli hardware di questo wallet sono costituiti da dispositivi fisici che utilizzano un chip sicuro per caricare in modo sicuro le proprie chiavi e i propri NFT. Anche in caso di attacchi informatici o infezioni da malware del computer, i propri asset digitali sono tenuti al sicuro dal Ledger wallet.

Phantom

La soluzione più diffusa per la gestione degli asset digitali all'interno della rete Solana è l'utilizzo del portafoglio hardware Phantom, il quale risulta particolarmente adatto per il caricamento e l'accumulo di NFT. Inoltre, questo portafoglio è compatibile con MetaMask, offrendo una maggiore flessibilità nella gestione degli asset digitali.
A differenza del Ledger, il Phantom wallet è un portafoglio software, il che significa che non offre lo stesso livello di sicurezza del portafoglio hardware. Nonostante ciò, Solana è noto per la sua facilità d'uso e la sua ampia adozione, e il Phantom wallet rappresenta una soluzione conveniente e accessibile per la gestione degli asset digitali all'interno dell'ecosistema Solana.

Solflare

Rappresenta una soluzione sicura e affidabile per la gestione degli asset digitali nella rete Solana, grazie all'utilizzo di avanzate tecnologie di crittografia e all'implementazione di un sistema di autenticazione a due fattori e di un supporto multi-firma.
Solfare è stato appositamente progettato per consentire agli utenti di caricare SOL, SPL e NFT in modo facile e intuitivo, offrendo inoltre l'accesso alle applicazioni decentralizzate di Solana.
Per garantire un'elevata sicurezza degli asset digitali, un team di esperti monitora costantemente la blockchain di Solana, intervenendo tempestivamente per prevenire qualsiasi attività sospetta.

3.2.3 Come caricare un wallet su Spatial

Dopo aver selezionato il portafoglio digitale desiderato tra quelli elencati in precedenza, per poterlo utilizzare all'interno di Spatial è necessario eseguire i seguenti passaggi [9]:

- Accedere su Spatial tramite il browser Google Chrome;
- Selezionare il proprio profilo dal menu principale;
- Selezionare la sezione "Integrations";
- Premere il pulsante "Connect";
- Selezionare il tipo di portafoglio digitale che si desidera connettere;
- Inserire le proprie credenziali per effettuare l'accesso al portafoglio digitale selezionato.

Una volta completati questi passaggi, il portafoglio digitale selezionato sarà connesso a Spatial e pronto per essere utilizzato per la gestione degli asset digitali.

3.3 3D NFT

3.3.1 Introduzione agli NFT 3D

Gli NFT 3D rappresentano token digitali che offrono gli stessi vantaggi, funzionalità e utilità dei beni digitali bidimensionali descritti in precedenza, ma con caratteristiche distintive che li differenziano dai loro predecessori.
L'aggiunta di una terza dimensione conferisce un valore artistico aggiuntivo e offre ai designer un nuovo mezzo creativo per esprimersi. Inoltre, gli oggetti 3D come NFT offrono un'ulteriore utilità reale, poiché possono essere immersivi e flessibili dal punto di vista concettuale, rendendo le serie NFT 3D coinvolgenti ed estremamente attrattive.
Gli NFT rappresentano un modo ideale per dimostrare la proprietà di un oggetto digitale, con i metadati associati in grado di garantire che tutte le transazioni siano tracciate e che sia specificato l'attuale proprietario di un asset digitale. In sintesi, gli NFT 3D rappresentano una soluzione altamente innovativa e coinvolgente per la gestione degli asset digitali, in grado di offrire un'ampia gamma di vantaggi e utilità per artisti, designer e appassionati di tecnologia. Rappresentano una vera e propria rivoluzione nel concetto di proprietà, in quanto contengono una serie di file associati all'NFT stesso. Questo significa che il proprietario di un NFT 3D non solo ha la prova di proprietà dell'asset digitale, ma ha anche accesso ai file 3D associati, che possono essere utilizzati in diversi metaversi.
Alcuni progetti di NFT 3D consentono ai titolari di utilizzare questi file per migliorare l'esperienza digitale degli utenti, migliorando sensibilmente l'interazione del proprietario con l'asset digitale.
Inoltre, sono ampiamente utilizzati per migliorare il mondo dei giochi digitali, creando oggetti di scena come persone ed edifici, che migliorano l'esperienza di gioco all'interno del metaverso.
Si prevede che entro il 2030, il 25% della popolazione mondiale passerà almeno un'ora al giorno all'interno del metaverso, rendendo gli NFT 3D un'opzione molto interessante per gli investitori e gli appassionati di tecnologia che desiderano sperimentare il mondo digitale in modo nuovo e coinvolgente [6].

Figura 3.2. Sound of Mystery Forest Space by Indie Game Hustle [6]

3.3.2 NFT Envirometns

Gli NFT Environments rappresentano un'importante caratteristica di Spatial, la quale offre agli utenti una vasta gamma di ambienti predefiniti, tra cui gallerie e spazi all'aperto, ma consente anche di caricare qualsiasi modello 3D e di impostarlo come proprio ambiente personale. Inoltre, gli utenti possono godere degli ambienti creati da alcuni dei migliori e più talentuosi designer 3D del mondo.
A partire da dicembre 2021, Spatial ha avviato una collaborazione con alcuni artisti per creare ambienti in edizione limitata che possono essere utilizzati esclusivamente all'interno del metaverso, ma che possono essere utilizzati anche in altre piattaforme.
Per poter acquistare un elemento della collezione è necessario possedere un account/wallet MetaMask e delle criptovalute di Ethereum o Polygon.
Gli NFT Environments rappresentano una soluzione altamente innovativa e coinvolgente per gli appassionati di tecnologia e di arte digitale, offrendo un'esperienza immersiva e coinvolgente all'interno del metaverso. Grazie alla collaborazione con alcuni dei migliori designer 3D del mondo, Spatial è in grado di offrire una vasta gamma di ambienti unici e originali, che rappresentanouna grande attrazione per gli utenti che desiderano sperimentare il mondo digitale in modo nuovo e coinvolgente [6]. Per poter collezionare ambienti NFT all'interno del metaverso di Spatial, è necessario seguire i seguenti passaggi [7]:

- Dalla schermata principale di Spatial, creare un nuovo spazio con '+Nuovo'
- Ogni ambiente con l'icona da collezionare è un ambiente da acquistare
- Se non si è già in posseso di un ambiente bisognerà visualizzare l'elenco su OpenSea in cui poter acquistare tramite fondi sul wallet MetaMask
- Terminato l'acquisto si ritorna in Spatial e poter utilizzare il proprio ambiente come si preferisce.

Figura 3.3. Bubble Park by Daewha Kang Design [6]

3.4 Creator toolkit e modelli predefiniti

Spatial.io è una piattaforma che si vanta non solo di fornire esperienze interattive agli utenti ma ha come punto forte anche la possibilità di dare libertà creativa a chiunque voglia cimentarsi e ne abbia il bisogno. È stato infatti implementato il creator Toolkit, potente strumento di creazione ambienti ed esperienze che si appoggia sul sofware Unity. Molte funzioni sono completamente gratuite mentre altre più specifiche sono a pagamento. Vediamo alcune di queste funzioni:

- Spatial.io offre uno strumento chiamato "Spatial Studio" che consente agli utenti di creare ambienti virtuali interattivi utilizzando una serie di elementi predefiniti. Puoi trascinare e rilasciare oggetti, configurare ambienti e personalizzare l'aspetto e il comportamento degli oggetti nell' ambiente virtuale.
- 3D Modeling Tools: Se si desidera creare oggetti personalizzati da utilizzare in Spatial.io, si può utilizzare un qualsiasi software di modellazione 3D come Blender, Autodesk Maya o 3ds Max. Questi strumenti ti consentono di creare modelli 3D dettagliati che possono essere importati in Spatial.io per arricchire l'esperienza virtuale.
- E' possibile utilizzare software come Unity per ricreare le ambientazioni da importare. Unity è un motore di sviluppo di giochi popolare e potente che può essere utilizzato per creare contenuti per Spatial.io. Supporta la creazione di ambienti 3D interattivi, personaggi animati e molto altro. Puoi utilizzare il toolkit Unity per sviluppare contenuti personalizzati e quindi esportarli per l'uso in Spatial.io.
- 360° Photo/Video Tools: Se desideri creare contenuti immersivi basati su foto o video a 360 gradi, puoi utilizzare strumenti come Adobe Photoshop o Adobe Premiere Pro per creare foto o video panoramici. Questi contenuti possono essere quindi caricati e condivisi su Spatial.io per offrire esperienze virtuali coinvolgenti.

Quindi è possibile importare spazi virtuali, singoli oggetti, contenuti multimediali e NFT per ricreare lo spazio utile a soddisfare le proprie esigenze. Spatial, inoltre, mette a disposizione degli ambienti già pronti e personalizzabili, nei quali è possibile caricare i propri contenuti senza dover per forza essere in grado di gestire la creazione e texturizzazione di mesh.

Capitolo 4

NFT e ambiente

4.1 "Climate-positive" NFT

Nonostante gli artisti e i collezionisti traggano diversi benefici dall'utilizzo degli NFT, si sta sviluppando una crescente preoccupazione in merito all'impatto ambientale che tali token possono avere sul pianeta. Tale preoccupazione è dovuta al fatto che molte delle transazioni avvengono su blockchain ad alta intensità energetica, il che potrebbe contribuire ai problemi relativi al cambiamento climatico.
La maggior parte delle transazioni NFT vengono effettuate sulla blockchain di Ethereum, che, sebbene non consumi tanta energia quanto la blockchain Bitcoin, presenta comunque un consumo di energia e emissioni di carbonio non trascurabili. Tuttavia, negli ultimi anni, gli NFT si stanno evolvendo per diventare "climate-positive".
È importante sottolineare che non tutte le emissioni di carbonio di Ethereum possono essere attribuite agli NFT, poiché questi rappresentano solo una piccola frazione delle transazioni sulla blockchain. Inoltre, si sta lavorando per sviluppare soluzioni volte a rendere gli NFT migliori per l'ambiente.
Di seguito verranno riportate alcune soluzioni NFT per il cambiamento climatico che potrebbe contribuire a ridurre l'impatto ambientale degli NFT e della tecnologia blockchain in generale e renderli "climate-positive" [8].

Figura 4.1. Earth day on spatial [8]

Compensazioni di carbonio

Le compensazioni di carbonio sono un metodo per compensare le emissioni di gas serra, come l'anidride carbonica, impegnandosi a ridurre o rimuovere tali gas come ad esempio investire in energia verde o tecnologie di cattura del carbonio sono esempi di attività che possono generare compensazioni di carbonio.
Nel contesto NFT, alcuni progetti hanno sperimentato l'associazione delle transazioni con le compensazioni di carbonio piantando alberi, per compensare alle emissioni prodotte dalla blockchain.

Green Crypto Networks

Il problema ambientale causato dagli NFT è derivato dall'energia consumata dalle blockchain che verificano le transazioni. In alcune reti, addirittura una singola transazione può richiedere una quantità considerevole di elettricità. Per mitigare il consumo di energia e migliorare l'impatto ambientale, una possibile soluzione potrebbe essere quella di passare all'utilizzo di fonti di energia rinnovabile.
La comunità crittografica può incentivare i miners a creare strutture in luoghi in cui si utilizza energia rinnovabile. In alternativa, i miners possono contribuire alla sostenibilità e risparmiare denaro installando pannelli solari per alimentare le loro strutture. In questo modo, è possibile promuovere l'utilizzo di "green crypto networks", ovvero reti crittografiche verdi, in grado di ridurre l'impatto ambientale dei processi di verifica delle transazioni e di promuovere un uso più sostenibile dell'energia.

Lazy Minting and Batch Minting

Un'altra possibile soluzione per gestire l'impatto ambientale degli NFT consiste nell'indirizzare gli artisti e i collezionisti verso tecniche di creazione di NFT più sostenibili. Ad esempio, ci sono opzioni come il batch minting e il lazy minting.
Con il batch minting , è possibile creare NFT in grandi quantità, in modo che diventino tutti parte della stessa transazione. Con il lazy minting, si crea l'NFT e lo si mette in vendita, ma la creazione non avviene fino alla vendita. Questo permette di consolidare tutte le transazioni che si verificano durante la creazione e la vendita di un NFT in una sola transazione, anche le più piccole.
Sebbene queste tecniche siano generalmente conosciute per limitare i costi delle commissioni, potrebbero anche essere utilizzate come metodi per ridurre il consumo di energia sulla blockchain.

Proof of Stake Mining

A causa del mining basato sulla Proof of Work (PoW), i miners necessitano di una quantità considerevole di energia per validare i blocchi. Come alternativa, alcune blockchain utilizzano la Proof of Stake (PoS) mining, dove i miners devono impegnare monete crypto invece di potenza di elaborazione, e una quantità maggiore di monete impegnate corrisponde a una maggiore potenza di mining.
Già adesso, alcuni mercati NFT utilizzano blockchain PoS come metodo per garantire una maggiore accessibilità e sostenibilità. Inoltre, sono stati pianificati degli aggiornamenti PoS per Ethereum.

Per ridurre l'impatto ambientale degli NFT, è necessario adottare diverse soluzioni.
Tuttavia, se gli artisti e i collezionisti faranno sentire la loro voce e se saranno implementate le soluzioni giuste, gli NFT potrebbero diventare carbon neutral. Inoltre, potrebbero diventare uno strumento per combattere il cambiamento climatico.

4.2 Progetti "climate-positive" su Spatial

Spatial si preoccupa dell'impatto delle criptovalute sul mondo e cerca di comprendere in che modo il trading di criptovalute può influenzare l'ambiente. Inoltre, si impegna a garantire un uso sostenibile della sua piattaforma, cercando di minimizzare l'impatto ambientale che può essere causato dalla creazione e dal trading di NFT sulla piattaforma [8].

ZooLife rappresenta il primo zoo virtuale al mondo che trasmette in diretta gli animali su Spatial. In tale contesto, vengono offerte diverse esperienze immersive con gli animali, accompagnate da esperti del settore, e gli utenti possono osservare e camminare intorno a loro, come se si trovassero in un vero e proprio zoo.
Ogni esperienza è stata appositamente progettata con l'obiettivo di avvicinare l'utente agli animali e ai problemi relativi alla natura, offrendo metodi innovativi per apprendere, proteggere e interagire con il mondo naturale. In Spatial, questa mostra si svolge all'interno della "Galleria Safari" del fotografo naturalista Steve Cannon.

La **National park week** rappresenta un'opportunità per la comunità di National Parks NFT, la quale conta più di 1800 utenti, di incontrarsi e condividere la propria passione per la natura. In questa settimana vengono svolti incontri che consistono in attività di vario genere tra cui quiz che consentono di accumulare punti utilizzabili per l'acquisto di veri pass per i parchi nazionali. Sostenere i nostri parchi nazionali aiuta a conservare la fauna selvatica e la biodiversità, dimostrando l'impegno per la protezione dell'ambiente e del patrimonio naturale del nostro paese.

Figura 4.2. National parks NFT [16]

Sunken Blimp è una piattaforma progettata per essere un ambiente in cui nascono progetti basati sulla comunità che fornisce all'utente strumenti e conoscenze per creare innovazioni utili per il futuro. In tale piattaforma gli utenti possono collaborare e condividere le proprie idee per lo sviluppo di soluzioni che portano al miglioramento della vita. Ha un approccio phygital ovvero combina elementi fisici e digitali come la stampa 3D, il mapping di proiezione, la realtà virtuale e aumentata.

Terrafor-Meta è un ambiente che offre la possibilità di visualizzare la Terra da una stazione spaziale e di apprezzare la bellezza del pianeta da una prospettiva totalmente diversa.

Capitolo 5

Spatial environment

5.1 Come interagire su spatial

E' possibile accedere su Spatial.io tramite diverse piattaforme: web, mobile (Android e IOS) e tramite VR. Ognuna di queste piattaforme è differente e in base all'utilizzo di ciascun utente è consigliata una diversa piattaforma.
Per ulteriori informazioni è possibile consultare: [18].
L'interazione su spatial ricorda molto i giochi 3D contemporanei. Per muovere l'avatar si usano i classici tasti WASD mentre per ruotare la visuale si possono usare tre diversi metodi: le frecce direzionali, il mouse oppure una modalità automatica. E' possibile inoltre far correre il proprio avatar tramite il tasto SHIFT, farlo saltare tramite la barra spaziatrice ed è anche presente il doppio salto. Tutti questi comandi sono molto comodi per le stanze in cui ci sono dei giochi. E' anche possibile usare emoji o fare balletti ed anche utilizzare il microfono per interagire con gli altri utenti presenti nella stanza.

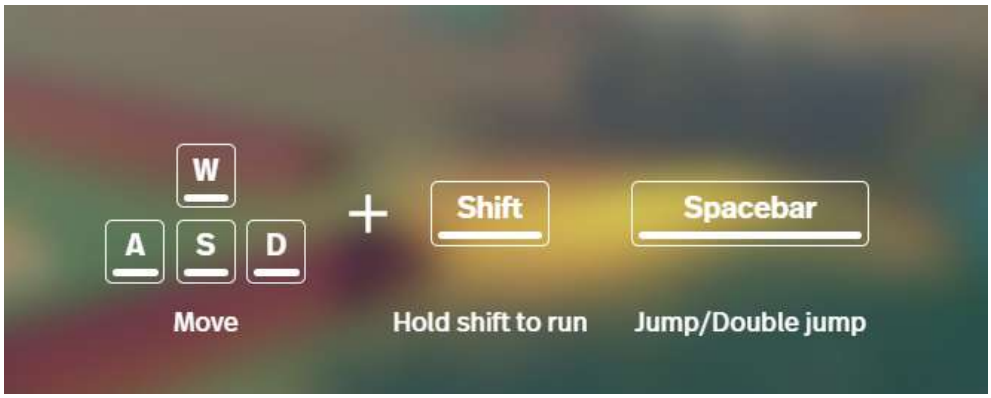


Figura 5.1. Come muoversi in Spatial

5.2 Eventi ospitati su spatial

Spatial è stato utilizzato anche per organizzare una varietà di eventi virtual, conferenze da remoto, team building online e feste a distanza. La piattaforma consente infatti agli utenti di creare i propri avatar e spazi virtuali per organizzare eventi dal vivo e interagire con altre persone in un ambiente virtuale.

- Uno degli eventi più importanti e degni di nota si è tenuto durante la *Metaverse Fashion Week 2023* ed è stata la mostra **Luis Fern x MetaMundo # *MVFW23*** , che presentava straordinarie opere d'arte che celebravano la cultura e il futuro della moda di famosi artisti iinternazionali. Durante la settimana dell'evento alcune piattaforme tra cui Spatial sono state teatro d'incontro tra digitalizzazione e moda, aprendo nuove possibilità di incontro tra domanda e offerta. Si poteva infatti comodamente da casa visitare delle gallerie piene di NFT inerenti al mondo della moda e partecipare ad escosivi party a tema nel metaverso insieme a molti nomi noti del settore. L'evento presentava alcuni dei nomi più rinomati del design digitale, tra cui agenzie 3D, case di moda digitali e designer digitali. I partecipanti potevano aspettarsi di ammirare sculture 3D, costumi digitali 3D, opere d'arte e NFT.

- Di grande rilevanza anche l'evento che ha come ideatore ibis Styles. Questa compagnia è infatti sbarcata nel Metaverso aprendo la possibilità a diversi artisti e architetti di poter mettere in mostra le loro opere digitali e NFT. Un esempio Made in Italy è quello della mostra NFType. NFType, mostra di Lorenzo Marini dedicata alla 'Nft Art', esposta all'interno di una galleria virtuale. Il percorso espositivo presenta 12 opere di arte dinamica, tra cui opere native digitali e digitalizzazioni di opere fisiche che proiettano il visitatore in un'esperienza immersiva ed ipnotica che mette in risalto l'arte dell'architetto Marini.

- Un altro esempio da riportare è quello del Brend A-More. E' infatti possibile accedere tramite visore o desktop ad un vero e proprio negozio digitale (sempre di proprietà italiana, di una giovane imprenditrice di nome Camilla Clemente). In questo negozio presente sulla piattaforma di Spatial è possibile vedere manichini che indossano abiti del brand e altri oggetti in vendita. Si può decidere se pagare tramite Wallet (MetaMask) o collegarsi con link direttamente al sito e pagare da lì.

5.3 Piani a pagamento

Spatial al contrario di tutti gli altri metaverso fornisce la possibilità di creare luoghi gratuitamente, inoltre è possibile:

- Ospitare fino a 50 persone in una stanza.
- Crea un avatar 3D realistico da un selfie.
- Upload di file da Metamask/Google Drive/OneDrive.
- Condivisione dello schermo.
- Creazione di Sticky Notes per lasciare messaggi nel tuo spazio.
- Strumenti di moderazione per bannare, mutare o espellere visitatori molesti.

Esiste anche un piano a pagamento che per 25$ al mese consente di:

- Permettere l'accesso al tuo spazio basandosi sul possesso di token NFT.
- Accesso fino a 500 persone (10 diverse istanze dello stesso spazio).
- Host tools.
- Maggiore controllo di cosa gli ospiti possono dare nel tuo spazio.
- Traduzione live.

Figura 5.2. [19]

E' necessario sottolineare il fatto che la fatturazione avviene tramite carta di credito senza nessuna possibilità di effettuare pagamenti tramite cryptovalute.
Un controsenso.

5.4 Confronto con altri metaversi

Spatial.io è un metaverso giovane, viene progettato per essere semplice da utilizzare sia per i creator che per i visitatori ed è utilizzata in diversi settori come marketing, istruzione, divertimento e lavoro.
L'obiettivo dichiarato è quello di progettare spazi 3D di alta qualità per la collaborazione e le comunità, con un occhio di riguardo all'arte digitale e al mondo della moda.
La piattaforma ha creato la possibilità per gli artisti di tutto il mondo di mostrare i propri progetti tramite mostre e sfilate, ma ben presto il suo utilizzo si è esteso anche alla socialità, al gioco e alla musica.
Spatial.io si è posizionata come una realtà libera e inclusiva, in grado di permettere a chiunque di iscriversi, crearsi un avatar e modellare il proprio spazio, rendendolo accessibile a tutti.
Nel corso dell'ultimo anno, la piattaforma ha raggiunto una grandissima porzione di pubblico diventando una delle piattaforme più utilizzate in ambito metaverso.
ReadyPlayerMe ha supportato la creazione degli avatar degli utenti, che possono modellare il proprio spazio e renderlo accessibile a tutti.
Spatial ha di recente annunciato l'introduzione del proprio Creator Toolkit basato su Unity consentendo ai propri sviluppatori la creazione di esperienze ancora più immersive grazie al migliore motore di rendering. Unity non solo supporta il rendering in real-time ma permetterà una migliore resa fotografica, più realistica e più veloce, il tutto andando a pesare meno sul lavoro degli sviluppatori e dei dispositivi host.
Con l'integrazione di Spatial, gli utenti possono finalmente superare il limite dello spazio statico in cui erano solo visitatori passivi, diventando parte integrante dell'esperienza metaverse, animando il proprio avatar, scrivendo o disegnando, interagendo con altri utenti e creando stanze virtuali in cui incontrarsi e collaborare con colleghi in un ambiente completamente virtuale.
Spatial.io si è dunque impostata nel giro di poco tempo come una delle principali piattaforme

social basate sulla navigazione 3D tramite avatar, con oltre 500.000 creatori registrati, 2 milioni di utenti unici e 127 milioni di ore trascorse sulla piattaforma negli ultimi 12 mesi. Spatial rappresenta così un'alternativa libera e gratuita alla creazione di ambienti metaverse, che ha l'obiettivo di rendere le piattaforme immersive facili e accessibili per chiunque entri e inizi a costruire, senza necessità di conoscenze pregresse in digital design, rendendola una piattaforma metaverse inclusiva e aperta.
Confrontando Spatial.io con alcuni dei metaversi più conosciuti come SandBox e Decentraland è evidente ci siano molte differenze, pur essendo tutti basati su tecnologie blockchain ed incentrati sull'attività partecipativa di più persone. Differentemente da The Sandbox e Decentraland, Spatial.io non ha una propria moneta nativa e non esiste perciò un ecosistema relativo all'uso della criptovaluta, rimane così una piattaforma di collaborazione virtuale che consente agli utenti di interagire e lavorare insieme in un ambiente 3D condiviso. Non essendovi moneta nativa ed economia interna all'ambiente spatial.io, non può esserci piena proprietà e controllo su alcun terreno o contenuto creato su di esso, non esiste la proprietà virtuale.
Mentre molti metaversi vogliono spostare o comunque formare una seconda vita al di fuori del mondo reale, Spatial.io vuole essere una chiamata Zoom più articolata, più interattiva. In sintesi, mentre Spatial è incentrata sulla creazione di ambienti metaverse accessibili e inclusivi, Decentraland e Sandbox si concentrano sulla creazione di un metaverso decentralizzato governato dalla comunità, governati da un'economia virtuale interna.

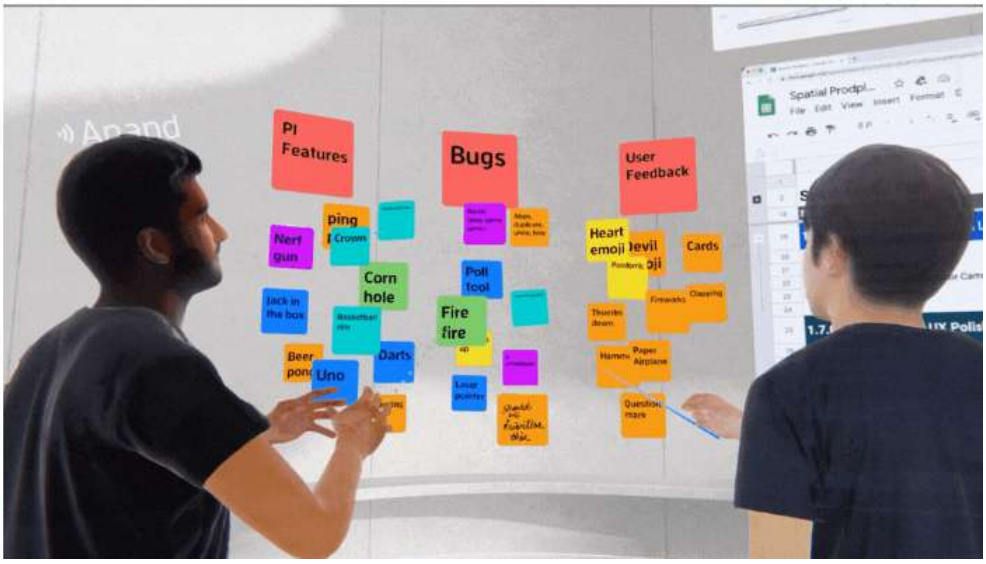


Figura 5.3. Brainstorming session in Spatial [17]

Capitolo 6

Conclusioni

Il Metaverso rappresenta un'opportunità unica per la socializzazione e la connessione tra persone provenienti da tutto il mondo. Inoltre, attraverso l'utilizzo di ambienti virtuali immersivi e interattivi, offre anche numerose opportunità per l'istruzione e la formazione, creando un'esperienza di apprendimento coinvolgente e innovativa.

In questo contesto, la piattaforma Spatial si distingue per la sua capacità di fornire ambienti stimolanti e personalizzabili, grazie ai quali gli utenti possono creare ambienti virtuali originali o godere di spazi creati da artisti affermati o emergenti. Attraverso la sua semplicità di utilizzo, gli utenti possono partecipare a esperienze uniche, come la Metaverse Fashion Week 2023 o l'Earth Day.
Diversamente da altri metaversi, Spatial non dispone di una propria moneta, il che significa che non consente pagamenti tramite criptovalute sulla piattaforma. Tuttavia, ciò non limita la sua capacità di fornire un'esperienza coinvolgente e creativa agli utenti.
D'altra parte Spatial è un metaverso completamente centralizzato, che sfrutta alcune funzioni della blockchain come gli NFT o l'accesso al profilo tramite wallet, strizzando l'occhio agli appassionati ma senza mai implementare politiche decentralizzate, non vi sono nemmeno modalità con cui suggerire o influire sulla crescita ed evoluzione della piattaforma.

Nella scelta dell'utilizzo della piattaforma è importante valutare attentamente le esigenze e gli obiettivi specifici dei singoli utenti. I pregi di questo sito sono molteplici ma non sono da sottovalutare i numerosi difetti.

Bibliografia

[1] https://it.wikipedia.org/wiki/Realt%C3%A0_virtuale
[2] http://tesi.luiss.it/35556/1/242831_LOPIZZO_FEDERICO.pdf
[3] https://www.agendadigitale.eu/cultura-digitale/metaverso-cose-come-si-entra-e-cosa-significa/
[4] https://www.agendadigitale.eu/cultura-digitale/metaverso-e-questo-il-futuro-che-ci-aspetta-tutti-gli-interrogativi-a-cui-dare-risposta/
[5] https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026
[6] https://www.spatial.io/blog/what-are-3d-nfts-and-4-things-you-can-do-with-them
[7] https://support.spatial.io/hc/en-us/articles/4412584089364-Collectible-NFT-Environments https://support.spatial.io/hc/en-us/articles/4412584089364-
[8] https://www.spatial.io/blog/4-nft-projects-with-a-positive-environmental-impact
[9] https://support.spatial.io/hc/en-us/articles/8236709274900-How-to-connect-your-Solana-NFT-wallet-
[10] https://support.metamask.io/hc/en-us/articles/360015489531-
[11] Getting-started-with-MetaMask https://www.singola.net/arti/blockchain-art-le-nuove-frontiere-dell-arte
[12] https://www.spatial.io/blog/how-to-make-an-nft-a-guide-for-artists-collectors-beginners
[13] https://www.spatial.io/about
[14] https://cyberscrilla.com/best-solana-nft-wallets/
[15] https://www.spatial.io/blog/what-is-an-nft-gallery-and-5-galleries-to-visit-in-spatial
[16] https://nationalparksnft.io/
[17] https://support.spatial.io/hc/en-us/articles/4419855279892-Host-Your-Next-Event-In-Spatial
[18] https://support.spatial.io/hc/en-us/articles/4417403884820-Web-Mobile-or-VR-Which-platform-is-right-for-me-
[19] https://www.spatial.io/create-an-avatar
[20] https://virtualspeech.com/blog/history-of-vr
[21] http://www.studioargento.com/immersiva/foto-immersiva6.html

HYPERLDEGER

Francesco Pio Barletta, Valerio Donnini, Alessandro Zamponi

Politecnico di Torino

Laurea Magistrale in Ingegneria Matematica

Blockchain e Criptoeconomia

Hyperldeger: cosa è e quali sono le sue principali caratteristiche

Studenti
Barletta Francesco Pio - s296114
Donnini Valerio - s296200
Zamponi Alessandro - s304833

Docente
Prof. Danilo Bazzanella

Anno Accademico 2022/2023

Indice

1 Introduzione **3**
1.1 Permissioned Blockchain . . . 3
1.2 Hyperledger . . . 4
1.3 Hyperledger Frameworks . . . 4
1.3.1 Hyperledger Fabric . . . 5
1.3.2 Hyperledger Indy . . . 5
1.3.3 Hyperledger Iroha . . . 5
1.3.4 Hyperledger Sawtooth . . . 6
1.3.5 Hyperledger Burrow . . . 6
1.4 Use cases . . . 6
1.4.1 Servizi Bancari . . . 6
1.4.2 Servizi Finanziari . . . 7
1.4.3 Assistenza Sanitaria . . . 8
1.4.4 IT: Gestione delle identità portabili . . . 9
1.5 Hyperledger Tools . . . 9

2 Le tecniche di consenso utilizzate e la Design Philosophy **11**
2.1 Algoritmi di consenso . . . 12
2.1.1 Consenso in Hyperledger Fabric . . . 15
2.1.2 Consenso in Hyperledger Indy . . . 16
2.1.3 Consenso in Hyperledger Iroha . . . 17
2.1.4 Consenso in Hyperledger Sawtooth . . . 19

3 Smart Contracts in Hyperledger **20**
3.1 Introduzione agli Smart Contracts . . . 20
3.1.1 Smart Contracts nei framework di Hyperledger . . . 20
3.2 Smart Contracts in Hyperledger Burrow . . . 21
3.2.1 Funzioni Native Sicure e livello di Permesso . . . 21
3.2.2 EVM permessionato . . . 22
3.2.3 Gateway, Firma e Interfacce . . . 22
3.3 Smart Contracts in Hyperledger Fabric . . . 23
3.3.1 Chaincode di Applicazione . . . 23
3.4 Smart Contracts in Hyperledger Indy . . . 24
3.5 Smart Contracts in Hyperledger Iroha . . . 24
3.6 Smart Contracts in Hyperledger Sawtooth . . . 24
3.6.1 Contratti Installati con Famiglie di Transazioni . . . 25
3.6.2 Contratti On-Chain con la Famiglia di Transazioni Seth . . . 25

4 Conclusioni **26**

Riferimenti bibliografici **27**

1 Introduzione

Partendo da un'analisi generale, la realizzazione della maggioranza dei servizi usati quotidianamente necessita dell'utilizzo di un database. Un esempio fra tanti potrebbe essere la gestione degli ordini in un'attività commerciale, dove si deve poter conoscere le rimanenze in magazzino di un determinato prodotto, così da contattare o meno i rifornitori. Inoltre, la crescente necessità di accedere agli stessi dati da parte di persone differenti, separate anche fisicamente, ha fatto si che si sviluppassero dei database, chiamati, *database distribuiti*, come alternativa ai classici database relazionali. Ovviamente si sono dovute risolvere alcune questioni come:

- Come si può avere la certezza dell'identità di chi accede al database?
- Che tipo di azioni possono essere effettuate?
- Come devono essere gestiti conflitti o incongruenze?
- Chi deve/può risolvere tali conflitti o incongruenze?
- Di chi ci si deve fidare per condividere i dati?

Avendo così chiarito qual è l'obiettivo e i relativi problemi, si è cercato poi di ideare una soluzione che risolvesse i punti sopracitati: *la tecnlogia blockchain*. Una blockchain infatti può essere considerata a tutti gli effetti un database distribuito senza un'autorità centrale che gestisce le autorizzazioni o l'attendibilità dei dati, basato sulla crittografia per codificare le informazioni contenute all'interno di essa. Esistono due principali tipi di blockchain:

- *Permissionless*: in questo caso qualsiasi utente può accedere alla blockchain ed utilizzarla.
- *Permissioned*: l'utente deve soddisfare dei requisiti specifici per accedere ed utilizzare la blockchain.

Ovviamenete questi 2 tipi di blockchain hanno dei casi d'uso diversi tra loro, poichè in alcune circostanze si necessita di un tipo di sicurezza differente da altri.

1.1 Permissioned Blockchain

In un contesto aziendale è sempre preferibile utilizzare delle *permissioned blockchain* : così facendo si ottiene la garanzia che solo gli impiegati autorizzati possano accedere ai dati salvati nella blockchain ed eventualmente apportare modifiche ad essi. Inoltre, questa nuova tecnologia sfrutta dei *sistemi di consenso* con lo scopo di mantenere corrette e coerenti le informazioni all'interno del database, così da risolvere possibili situazioni di concorrenza, dove due utenti diversi cercano di accedere e/o modificare lo stesso dato.

Un altro dettaglio non trascurabile è il guadagno che si potrebbe ottenere, in termini di tempo e denaro, attraverso l'uso delle blockchain, permettendo anche di snellire in maniera considerevole numerosi processi aziendali ma mantendendo un livello di sicurezza piuttosto alto. Il punto chiave è che l'utente non deve più fidarsi della persona con cui sta interagendo, ma bensì della tecnologia stessa, da cui si tenta di eliminare ogni tipo di intermediario e progettata per essere a prova di manomissione.

1.2 Hyperledger

Hyperledger nasce nel 2015 ed è un progetto open-source, ideato da diverse compagnie come Blockchain, ConsenSys, Digital Asset, R3, Onchain, che capirono come cooperare li avrebbe portati a raggiungere risultati migliori, rispetto a dei lavori individuali. Successivamente questo progetto venne messo sotto la tutela della Fondazione Linux. [3]

Figura 1: Logo di Hyperledger

Il principale obiettivo del progetto Hyperledger è quello di creare piattaforme modulari, open-source e facili da utilizzare. Una prima precisazione riguarda i diversi motivi per cui l'open-source è la scelta migliore per le blockchain aziendali:

- **Affidabilità e Popolarità**: le soluzioni sono di notevole qualità e permettono anche la personalizzazione in base alle esigenze specifiche vista la possibilità di accedere al codice sorgente.
- **Open source builds trust**: considerare un approccio open-source permette alle parti interessate di partecipare allo sviluppo. Questo consente di avere fiducia sulla bontà del risultato finale.
- **Open Governance**: le decisioni su come, quando e quali modifiche apportare vengono prese da un gruppo di developers, scelti dalla comunità di sviluppatori attivi, così che chiunque possa partecipare al progetto.
- **Interoperabilità**: fin dall'inizio le tecnologie open-source Hyperledger sono state ideate per poter essere intregrate con altre blockchain.

Hyperledger può essere usato anche come *greenhouse*, per lo sviluppo di blockchain aziendali. Questo garantisce una struttura modulare per lo sviluppo di nuove idee, fornendo le risorse necessarie. Inoltre permette la specializzazione dei casi d'uso, che come diretta conseguenza ha l'aumento della produttività: i developer che lavorano nelle stesse aree vengono incoraggiati a cooperare, invece che competere. Quest'ultimo aspetto permette di evitare sprechi di tempo e denaro per raggiungere un obiettivo comune.

1.3 Hyperledger Frameworks

Hyperledger mette a disposizione diversi framework e tra i più imporanti si possono trovare: *Hyperledger Fabric, Hyperledger Indy, Hyperledger Iroha, Hyperledger Sawtooth, Hyperledger Burrow.*

1.3.1 Hyperledger Fabric

Hyperledger Fabric è una piattaforma per creare soluzioni che possono svariare in ogni settore, garantendo una qualità piuttosto alta del prodotto in termini di flessiblità, scalabilità, sicurezza e resilienza. Sfrutta la tecnologia dei container per realizzare smart contracts anche noti come *chaincode*: quest'ultimi possono essere scritti in diversi linguaggi di programmazione, come Go o JavaScript. Si possono poi aggiornare i chaincode senza scaturire alcuna interruzione alla rete, andando così a rappresentare un aspetto significativo per le applicazioni aziendali. La caratteristica principale di Hyperledger Frabic risiede nella sua architettura, modulare e permissioned, rendendola una soluzione ideale per i contesti dove la privacy e la gestione dei dati richiedono una particolare attenzione. Più nello specifico, gli accessi e le autorizzazioni all'interno della rete possono essere gestiti in maniera granulare, lasciando la possibilità alle organizzazioni di gestire in autonomia la parte di autenticazione e autorizzazione. Inoltre, il framework permette anche di creare dei canali per le sotto-reti di una blockchain, dove solo gli utenti autorizzati possono accedere ai dati e alle transazioni, mantenedo anche una porzione di rete in comune.

1.3.2 Hyperledger Indy

Hyperledger Indy rappresenta un altro framework progettato ad-hoc per sviluppare sistemi di identità digitale decentralizzati basati sulle blockchain. Vengono messi a disposizione librerie, tools e componenti riutilizzabili per lo sviluppo. La finalità di questo framework è quella di dare all'utente il completo controllo delle proprie identità digitali e lasciare a quest'ultimo la decisione su quali dati condividere, senza un intermediario centralizzato. Le caratteristiche di Hyperledger Indy sono:

- **Privacy**: Indy preserva la privacy dell'utente, lasciandolo operare senza creare correlazioni tra le varie operazioni effettuate.
- **Verifiable Claims**: è possibile selezionare quali informazioni condividere, sfruttando le *zero-knowledge proofs*.
- **Self-Sovereignity**: Le informazioni legate alle identità digitali dell'utente vengono salvate in un ledger, dove solo il proprietario dei dati può cancellarli o modificarli.

Combinando insieme queste caratteristische si riesce a diminuire la quantità di dati personali salvati dalle organizzazioni, riducendo l'interesse e il rischio di attacchi hacker, mantenendo però un alto livello di privacy per l'utente.

1.3.3 Hyperledger Iroha

Il progetto Iroha ha come obiettivo quello di semplificare lo sviluppo, il testing e la distribuzione di applicazioni blockchain aziendali. I punti di forza sono un'architettura semplice e modulare, che facilita l'integrazione con applicazioni già esistenti, apportando una diminuzione in termini di tempo e risorse necessarie. Inoltre Hyperledger Iroha, differentemente dai progetti Fabric e Sawtooth, mette a disposizione delle features utili ai fini di sviluppare delle applicazioni per gli end-users, fornendo un set API-REST, che facilitano l'interazione con la blockchain. Il modello di autorizzazione usato da questo progetto è basato sugli account: per operare sulla blockchain si devono rispettare dei requisiti specifici.

1.3.4 Hyperledger Sawtooth

Hyperledger Sawtooth è un'altra piattaforma modulare e nasce per la costruzione e lo sviluppo di sistemi distribuiti: all'interno dei ledgers sono presenti dei record dove possono essere salvate delle informazioni, come ad esempio la proprietà di un determinato asset, senza la necessità di un'autorità centrale. Un altro obiettivo di Sawtooth è quello di mantenere gli smart contracts sicuri per gli scopi aziendali e per raggiungere tale obiettivo, sfruttando ancora la modularità, le varie organizzazioni possono personalizzare a proprio piacimento le applicazioni della blockchain. Un'altra caratteristica di Sawtooth è rappresentata da un modello di consenso *"pluggable"*,grazie al quale è possibile dare agli utenti stessi la facoltà di scegliere il protocollo di consenso più adatto alle loro esigenze.

Sawtooth rende disponibile anche uno scheduler avanzato che permette di eseguire in parallelo l'inserimento dei blocchi, andando a migliorare quella che è una delle maggiori debolezze delle blockchain in termini di performance.

Questo framework mette a disposizione delle funzionalità per raggruppare i diversi nodi necessari per la creazione di una rete blockchain, in quelli che vengono chiamati cluster, architetture di rete usate per garantire flessibilità e scalabilità. L'accesso ad ogni cluster viene poi regolato tramite diversi sistemi di autorizzazione, garantendo la privacy tra gli utenti di reti differenti. In questo contesto, se si dovessero realizzare delle transazioni tra catene differenti, si dovrebbe introdurre anche **Hyperledger Quilt**, la cui funzione principale è quella di agire come intermediario tra le varie parti.

1.3.5 Hyperledger Burrow

Il framework Burrow è basato su blockchain modulari ma aggiunge un *Permissioned Smart Contract Interpreter (PSCI)*. Ciò che differenzia questo framework dagli altri è che in questo caso il focus è nell'utilizzo delle Ethereum Virtual Machine (EVM) e l'utilizzo di smart contracts nelle reti permissioned. Infatti Burrow fornisce anche un tool per l'implementazione vera e propria di smart contracts scritti nel linguaggio *Solidity*. In generale però questo framework rispetto agli altri, rappresenta la scelta più dispendiosa, considerando ad esempio il tempo di risposta media e risorse utilizzate. [6]

1.4 Use cases

Ci sono diversi ambiti dove la tecnologia blockchain, potrebbe risultare piuttosto efficace.

1.4.1 Servizi Bancari

Nell'ambito dei sistemi bancari, generalmente le banche tendono a concedere prestiti solo agli utenti che presentano un buon rischio. Il punto è che per comprendere quanto elevato sia il rischio, le banche necessitano di avere numerose informazioni dell'utente, chiamate *Personally Identifiable Information (PII)*. Di conseguenza, questo rende le banche molto appettibili come possibili vittime di un attacco hacker.

La soluzione migliore tra i vari framework offerti da Hyperledger in questo caso è *Hyperledger Indy* dove, grazie alle sue caratteristiche, l'utente può decidere nello specifico quali informazioni condividere con le banche. Questa soluzione permette quindi all'utente di poter fare richiesta per un prestito ad un numero considerevole di istituti: i richiedenti del prestito

possono generare quindi delle *zero-knwoledge proofs* dove invece di fornire la propria data di nascita, viene creata una *proof* per dimostrare di essere maggiorenne o che il suo redditto è maggiore o minore di una certa soglia. Hyperledger Indy, grazie alla sua infrastruttura, permette quindi all'utente di controllare in modo privato e sicuro le proprie identità digitali, attraverso l'utilizzo di *identità digitali decentralizzate (DID)*. Essendo la rete di Indy distribuita, i diversi nodi cooperano per mantenere autentiche e integre le identità digitali: ogni nodo mantiene una copia del registro condiviso, noto come *Indy Ledger*, che può poi essere consultato da chi deve verificare le informazioni fornite da un utente.

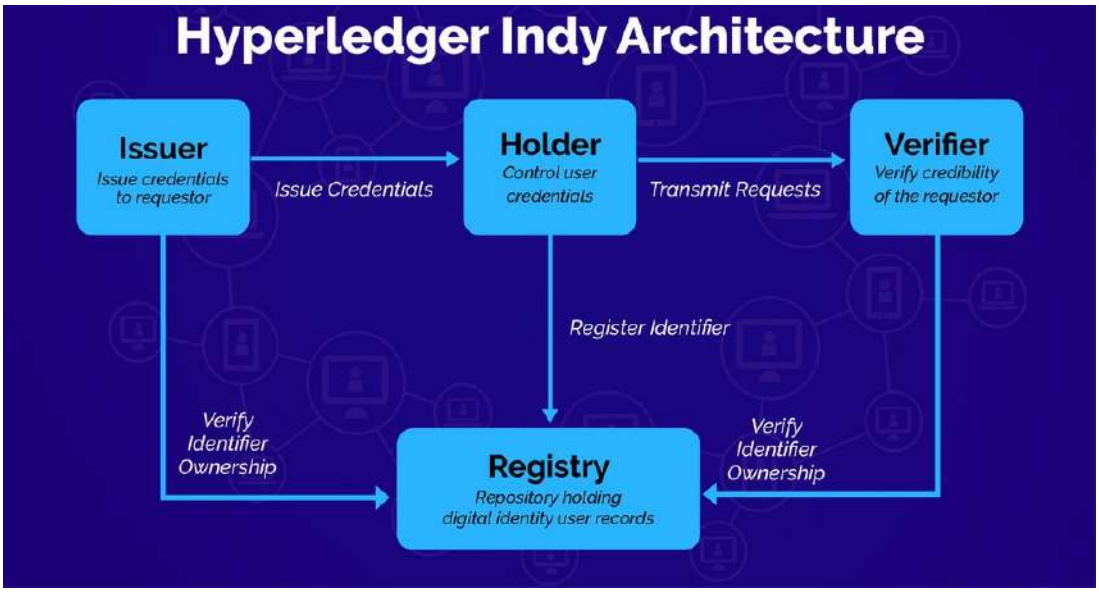


Figura 2: Hyperledger Indy Architecture

Come illsutrato in figura, il processo con cui un utente, che nella figura è rappresentato dall'holder, può fornire delle credenziali ad un specifico servizio, il verifier, si basa su un registry accessibile da tutte le figure coinvolte.

1.4.2 Servizi Finanziari

Ci sono alcune caratteristiche delle tecnologie blockchain che le rendono molto appetibili per essere integrate anche nei sistemi finanziari, come la privacy e la riservatezza. Più nel dettaglio, le blockchain che dovrebbero essere utilizzate sono quelle private o permissioned: considerando anche il grande volume di transazioni, le blockchain permettono anche di snellire l'elaborazine dei dati post-trade. Questa elaborazione è composta di diversi step, ognuno dei quali può essere affidato ad un dipartimento specifico, anche di differenti entità: il problema in questo contesto è che si necessitano di numerose interfacce tra i diversi attori, con sforzi considerevoli per mantenere coerenti le informazioni e una dilatazione, non trascurabile, delle tempistiche per concludere i processi. Sfruttando le comunicazioni peer-to-peer, dove l'utente può inserire le informazioni che possono poi essere verificate da altri, e la blockchain stessa, si possono inglobare tutti gli attori e i dati necessari su quest'ultima, alleggerendo così l'intero processo. Tuttavia, anche se è possibile assicurarsi

che le informazioni presenti nella blockchain non siano state modificate, si devono aggiungere altre features per migliorare il processo menzionato precedentemente:

- **Immediate finality**: L'inserimento delle transazioni nella blockchain deve essere veloce, così da essere fruibile per il destinatario di una transazione in tempi brevi. Questo implica che gli algoritmi di consenso come Proof-of-Work o Proof-of-Stake non sono adatti in questo contesto.
- **Future-Proof confidentiality**: le identità dei traders non devono essere rese pubbliche.
- **Streamlined performance**: le attività di post-trade dovrebbero avvenire quasi in tempo reale e non alla fine della giornata.

Ci quindi sono diversi framework di Hyperledger che potrebbero tornare utili:

- Hyperledger Fabric: la caratteristica di Fabric che potrebbe agevolare in questo contesto è la frammentazione della rete in sotto-reti completamente disgiunte. Questo permette di replicare i dati solo dove necessario.
- Hyperledger Sawtooth: rappresenta un modo efficace per supportare le attività di post-trade, vista la possibilità di eseguire le transazioni in parallelo.
- Hyperledger Indy: attraverso l'utilizzo dei *Verifiable Claims* si può semplificare il processo di valutazione dell'affidabilità degli attori coinvolti, senza compromettere la riservatezza dei dati personali.

1.4.3 Assistenza Sanitaria

Una delle pratiche più pesanti in ambito sanitario è quelle che coinvolge i medici stessi e prende il nome di *credentialing*: questa procedure è utilizzata dagli ospedali per avere la certezza che i medici abbiano le conoscenze richieste e il diritto di svolgere tale professione. Il problema risiede nella quantità di dati che il medico stesso deve raccogliere, come le valutazioni da parti di colleghi e le licenze mediche statali, che dovranno poi essere verificate dall'ospedale, dove si potrebbe perdere un quantitativo di tempo considerevole. Per introdurre una soluzione basata sulle blockchain si necessita però chiarire alcuni aspetti come:

- Quali informazioni salvare sulla blockchain?
- Qual è il modo migliore per gestire le identità delle parti coinvolte?
- Quali sono le richieste necessarie?

Ancora una volta Indy si offre come la soluzione migliore grazie ai *Verifiable Claims* che permettono al medico, ad esempio, di ottenere una prova della sua laurea, da condividere poi con i vari ospedali, rilasciata direttamente dall'università dove è stata conseguita. Successivamente l'ospedale sarà in grado di verificare, tramite le firme digitali, se l'informazione condivisa dal medico sia effettivamente valida.

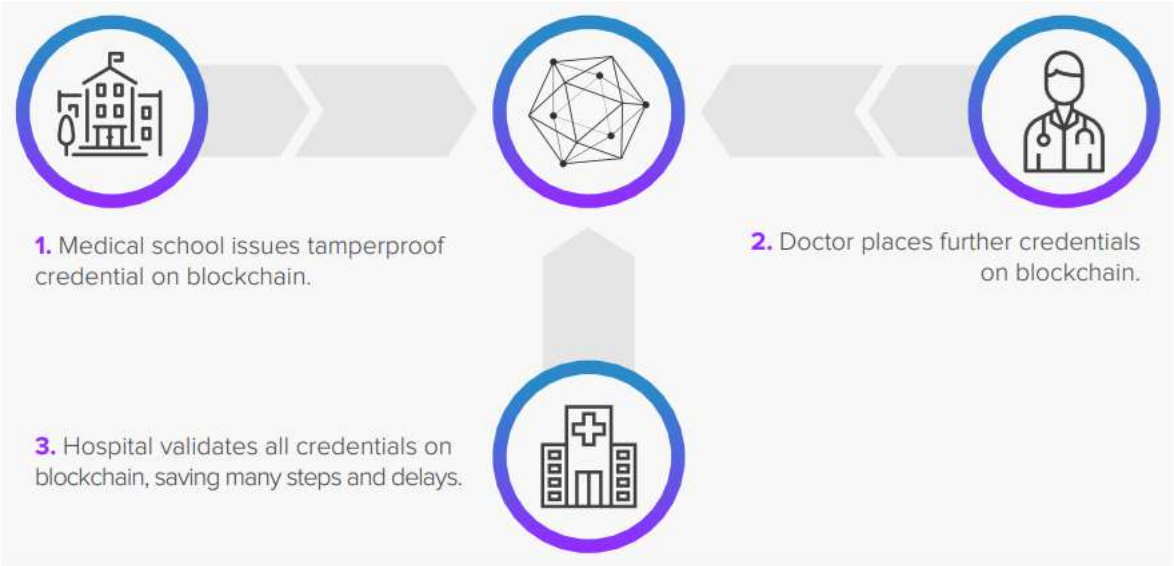


Figura 3: Possibile schema di una soluzione basata su blockchain

1.4.4 IT: Gestione delle identità portabili

Uno degli sviluppi più interessanti della tecnologia blockchain è legata sicuramente al concetto di **Self-Sovereign identity**, dove un individuo può controllare le proprie identità digitali, decidendo in maniera specifica quali dati condividere e con chi. Il principale focus di Hyperledger Indy, infatti, è appunto quello di permettere all'utente di creare delle identità che possano essere portabili e utilizzabili ovunque i ledger distribuiti siano accettati. Questo permettereebbe di utilizzare la stessa identità tra diversi sistemi, senza creare un nuovo profilo per ogni sistema.

1.5 Hyperledger Tools

Ci sono diversi tools messi a disposizone da Hyperledger, per lo sviluppo e la gestione di applicazioni basate sulla blockchain, come:

- **Caliper**: rappresenta un tool per monitorare le performance di ogni blockchain. Ogni report ha diversi indicatori come *Transaction Per Second (TPS)*, *Transaction latency e Resource utilization*, senza però rendere pubblica nessuna informazione
- **Cello**: è un toolkit per lo sviluppo on-demand all'interno dell'ecosistema blockchain:facilita l'uso di queste soluzioni da parte delle aziende, rendendo più efficente il *"Blockchain as a Service (BaaS)"*.
- **Composer**: questo tool permette di semplificare e velocizzare la creazione di smart contracts e applicazioni blockchain, agevolando l'integrazione con i sistemi già presenti all'interno di un'azienda.
- **Explorer**: fornisce una dashboard per consultare le informazioni relative ai blocchi, i log dei nodi, smart contracts, transazioni, statistiche e qualsiasi altra informazione

presente nella blockchain. Può essere integrato con ogni piattaforma di autenticazione o autorizzazione, dando le informazioni inerenti ai diversi privilegi degli utenti.

- **Hyperledger Quilt**: si occupa di rendere interoperabili i diversi ledger, grazie a *Interledger Protocol (ILP)*, creando un namespace globale e semplificando le transazioni tra ledger differenti.

.

2 Le tecniche di consenso utilizzate e la Design Philosophy

Le Business Blockchain possono avere requisiti differenti. Per esempio, si potrebbe avere:

- la necessità di sistemi di consenso e di conferma veloci che permettano l'inserimento di blocchi in poco tempo
- dei sistemi di consenso che possono "permettersi" di impiegare più tempo per la gestione dei blocchi

Si può considerare come la tecnologia si vada a basare su degli *optimization point* di cui i prinicipali risultano essere:

- scalabilità
- confidenza
- requisiti in termini di sicurezza

E' per questo motivo che ad Hyperledger non è associata un'unica tecnologia per Business Blockchain, bensì un insieme, che sono caratterizzate da *distributed ledgers*, *smart contracts* e via dicendo. La strategia che adotta, denominata $Hyperledger's\ umbrella\ strategy$, si basa sull'andare a riutilizzare gli stessi *building blocks* a partire da un framework architetturale che è modulabile.

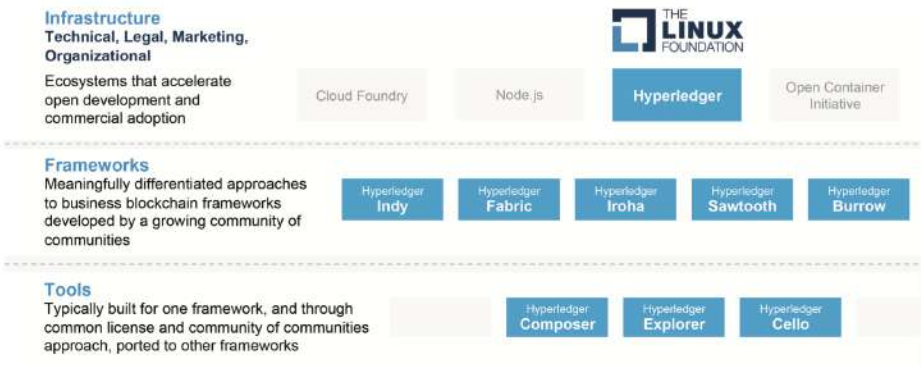


Figura 4: $Hyperledger's\ umbrella\ strategy$

Tutti i progetti che nascono a partire da Hyperledger presentano la stessa *Design Philosophy* che si basa sull'utilizzo di un approccio modulare ed estensibile, dove viene garantita l'interoperabilità e vengono rispettati dei principi di sicurezza, basandosi sull'assenza di una *cryptocurrency* nativa.
L' $Hyperledger\ Architecture\ Working\ Group$[1] ha definito i seguenti *building blocks* come componenti che devono essere associati ad una $Business\ Blockchain$:

[1] gruppo di lavoro che si occupa di definire un framework che può essere utilizzato come architettura modulare

- **Consensus Layer**: livello che nasce dalla necessità di riuscire a trovare un accordo sull'ordine e la conferma della correttezza di un'insieme di transazioni che costituisono un blocco
- **Smart Contract Layer**: livello utile per il *processing* delle richieste di transazione e per capire se le transazioni stesse siano valide o meno a partire da una logica di business
- **Communication Layer**: livello che permette la comunicazione *peer-to-peer* tra i vari nodi della stessa *ledger*
- **Data Store Abstraction**: componente che permette a dei database di essere utilizzati da molteplici moduli
- **Crypto Abstraction**: componente che dà la possibilità di cambiare i vari algoritmi criptografici che vengono utilizzati senza creare problemi ai vari moduli
- **Identity Services**: componente associato principalmente alla sicurezza: permette di avere autenticazione e autorizzazione ed inoltre stabilisce una *Root of Trust* nel momento in cui viene createa una nuova istanza di *Blockchain*. Durante le operazioni che vengono svolte in rete si preoccupa anche della registrazione delle diverse entità
- **Policy Services**: componente che si preoccupa della corretta gestione di tutte le tipologie di policy
- **APIs**: permettono ai *client* e alle applicazioni di potersi interfacciare con la blockchain
- **Interoperation**: consente la comunicazione tra differenti istanze di una blockchain.

2.1 Algoritmi di consenso

Nelle diverse applicazioni che una blockchain può avere, ci sono due problemi comuni che devono essere risolti: il *double spending problem*[7] e il *Byzantine Generals Problem*[8]. La prima tipologia di problema si traduce nella necessità di riuscire ad evitare che la stessa moneta venga utilizzata allo stesso tempo in due transazioni diverse. Nella blockchain questo problema viene risolto andando a utilizzare diversi nodi di rete che vanno a verificare le transazioni che vengono fatte, differentemente da quanto accade nella realtà, dove questa situazione di utilizzo multiplo della stessa moneta per diverse operazioni non può verificarsi, in quanto la moneta stessa è l'entità che permette lo scambio. Parlando invece di *Byzantine Generals Problem*, si va a trattare la situazione dove, data la natura distribuita del sistema, ci potrebbero essere degli utenti malevoli che dopo aver preso il controllo di alcuni dei nodi di rete, potrebbero andare a cambiare il contenuto della comunicazione. Quindi si deve andare ad integrare un algoritmo che consenta ai nodi "buoni" di riconoscere quando il contenuto di ciò che viene scambiato è stato alterato e ottenere allo stesso tempo dei risultati consistenti con gli altri nodi. Nel corso degli anni sono stati studiati e sviluppati differenti algoritmi di consenso che presentano ognuno delle caratteristiche proprie. A seconda di queste proprietà si vanno a rispettare dei modelli di *fault tolerance* differenti e soddisfare diversi requisiti di rete. Principali esempi di come il consenso viene implementato sono i seguenti:

- attraverso algoritmi basati sulla lotteria (come il *Proof of Elapsed Time*[9] (PoET) o il *Proof of Work*[10])
- attraverso metodi basati su delle votazioni (come *Redundant Byzantine Fault Tolerance*[11] (RBFT) e *Paxos*)

La principale caratteristica degli algoritmi basati su lotteria è che hanno una buona scalabilità, dato che il vincitore propone un blocco che viene poi inoltrato a tutti gli altri nodi che sono presenti sulla rete. D'altro canto hanno delle criticità quando ci sono due presunti vincitori che presentano un blocco, situazione nella quale ognuna delle due *fork* deve essere validata e ciò aumenta il tempo computazionale.
Analizzando invece gli algoritmi basati su delle votazioni, questi si basano sul principio di maggioranza rispetto la validazione di un blocco da parte dei vari nodi della rete. Quando ciò avviene si raggiunge il consenso e di conseguenza un accordo tra i vari nodi ed è per questo motivo che questa tipologia di algoritmi, a differenza di quanto accade con quelli basati su lotteria, garantiscono *low latency* per il raggiungimento dell'accordo. L'aspetto negativo che si presenta è associato al tipo di comunicazione, visto che in questi algoritmi solitamente ogni nodo deve comunicare con tutti gli altri: tanto più il numero dei nodi aumenta, tanto più tempo ci vorrà per la comunicazione e tanto più tempo di conseguenza ci vorrà per ottenere il consenso.
Quello che devono ricordarsi gli sviluppatori di Hyperledger, è che la rete delle *Business Blockchain* è considerata un ambiente di *partial trust*. Lo standard utilizzato dalla tecnologia Bitcoin per il consenso, la *Proof of Work*, non risulta essere stata inclusa tra gli algoritmi utilizzabili, in quanto dopo essere stata valutata, è risultata essere troppo dispendiosa in termini di risorse e tempo.

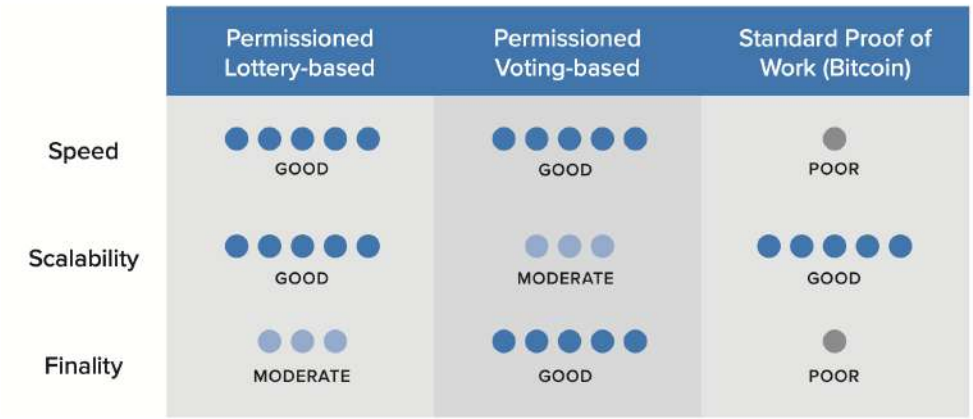


Figura 5: Confronto tra le varie tipologie di algoritmi di consenso

Per ottenere il consenso, i vari framework che implentano una *Hyperledger Business Blockchain* devono svolgere due attività che sono:

- Ordinamento delle transazioni
- Validazione delle transazioni

Se queste due operazioni vengono mantenute separate si ha la certezza che ogni framework di Hyperledger possa funzionare con qualunque modulo di Hyperledger che implementa il consenso. Il *consensus process flow* si può riassumere nei seguenti passi, sapendo che il livello di comunicazione è utilizzato dal livello di consenso per l'interfacciamento con il client e gli altri *peers* presenti sulla rete:

1. ricezioni delle transazioni dal client
2. inoltro delle transazioni an un *ordering service*[2]. Per proteggere le transazioni, queste solitamente vengono o cryptate o hashate prima di essere inviarte al servizio
3. ricezione delle transazioni da parte dell'*ordering service* a seconda dell'algoritmo di consenso e delle policy di configurazione.
4. raggruppamento delle transazioni in blocchi
5. validazione da parte dello *smart contract layer* di ogni transazione. Le transazioni che vengono respinte sono divisibili in due gruppi:
   - problemi di logica: transazione non conforme alle policy di configurazione
   - problemi di sintassi: problemi relati a input non validi, transazioni che si ripetono, ecc.

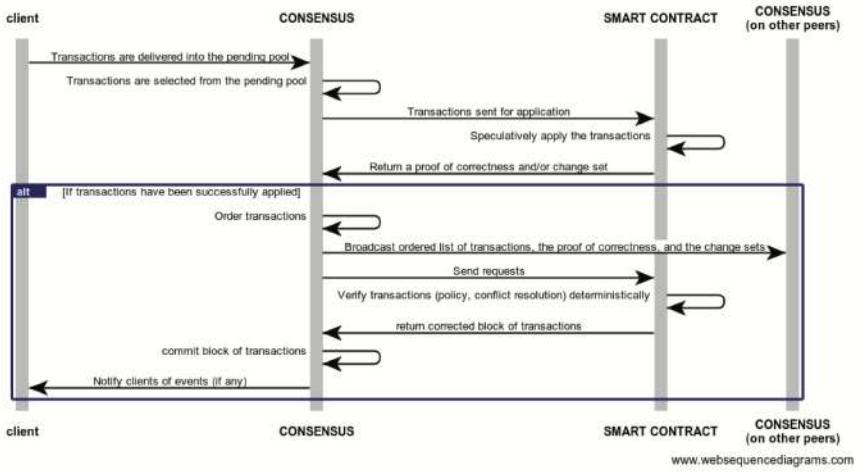


Figura 6: *Hyperldger Consensus Process Flow*

Gli algoritmi di consenso che vengono utilizzati nei vari framework di Hyperldger sono i seguenti:

- **Apache Kafka**[12] in Hyperledger Fabric
- **RBFT**[11] in Hyperledger Indy
- **Sumeragi**[12] in Hyperledger Iroha
- **PoET**[9] in Hyperledger Sawtooth

[2]Servizio che si preoccupa di ordinare le transazioni che può essere realizzato con un servizio centralizzato o con un protocollo distribuito

2.1.1 Consenso in Hyperledger Fabric

In Hyperledger Fabric[4] l'algoritmo di consenso usato si chiama Apache Kafka, appartenente alla categoria *permissioned voting based*, e si suddivide in tre fasi:

- $Endorsement$: fase che serve per andare a pubblicare una transazione da parte dei partecipanti che solitamente si basa su una policy
- $Ordering$: fase che permette di andare a decidere l'ordine con cui le transazioni valide verranno poi attaccate alla *ledger*
- $Validation$: fase che va a validare la correttezza del risultato delle transazioni ordinate, controllando anche se queste rispettino le *endorsement policies* e il $double - spending$

Fabric può essere integrato con servizi di consenso per ognuna delle tre fasi. Dipendentemente dal tipo delle applicazini e dai loro requisiti, ci possono essere modelli differenti associati alle varie fasi. Più nel dettaglio, parlando relativamente alle APIs che vengono utilizzate per interfacciarsi con l'*ordering service*, si può dire come queste debbano includere due operazioni:

- $broadcast(blob)$: operazione che permette la pubblicazione di un messaggio (blob) sul canale
- $deliver(seqno, prevhash, blob)$: operazione che permette all'*ordering service* di mandare un messaggio ad un client contenente il blob, la sequenza non negativa associata e l'hash del più recente blob ricevuto

I principali *ordering plugin* attualemente sviluppati sono i seguenti:

- BFT Smart[13]
- Simplified Byzantine Fault Tolerance (SBFT)
- Honey Badger of BFT[14]

Dipendentemente dagli use-cases dell'applicazione e dal modello di $fault - tolerance$, se ne sceglie uno piuttosto che un altro.

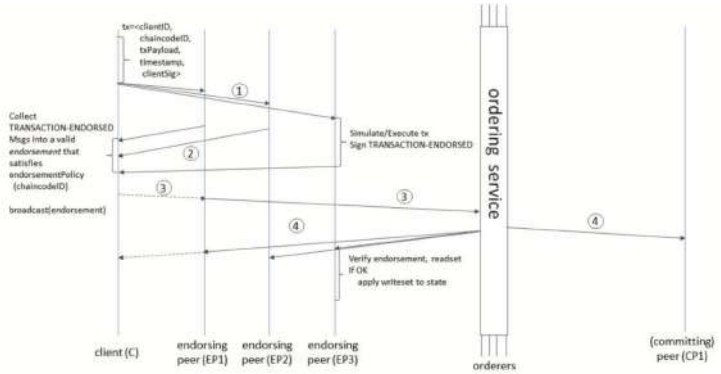


Figura 7: Un possibile $transaction\ flow$ in Hyperldger Fabric

2.1.2 Consenso in Hyperledger Indy

In Hyperledger Indy il consenso[4] si basa su *Redundant Byzantine Fault Tolerance* (RBFT), algoritmo di tipologia *permissioned voting based*, che può essere pensato come il far runnare molte istanze in parallelo di *Plenum Byzantine Fault Tolerance* (Plenum) (algoritmo da cui prende ispirazione). Il *ledger* viene aggiornato da un'istanza che prende il nome di *master* e che si preoccupa di ordinare le transazioni. Le prestazioni in termini di *throughput* e latenza di questa istanza vengono costantemente monitorate e confrontate con la media delle peformance delle altre istanze del nodo in esame, in modo tale che se le sue performance scendono troppo, si va a scegliere una nuova istanza come master. Per riuscire a garantire il fallimento di f nodi, si ha bisogno di avere nella rete almeno 3f +1 nodi funzionanti.
Il protocollo RBFT si basa sui seguenti passi:

1. il client invia la richiesta a f + 1 nodi
2. ogni nodo che riceve la richiesta, la inoltra a tutti gli altri nodi della rete (PROPAGATE)
3. in ogni nodo, ogni instanza leader (master) prepara una *proposal* chiamata PRE-PREPARE che invia agli altri nodi
4. i nodi che ricevono la PRE-PREPARE se la accettano, mandano una PREPARE come ack al nodo mittente
5. quando il nodo mettente ha ricevuto una *proposal* PRE-PREPARE e 2f messaggi di tipo PREPARE, accetta la *proposal* a manda un messaggio di COMMIT
6. quando un nodo riceve 2f + 1 messaggi di COMMIT, allora il batch delle richieste può essere ordinato e aggiunto al *ledger* visto che la maggioranza dei nodi hanno trovato l'*agreement* rispetto la *proposal* proposta

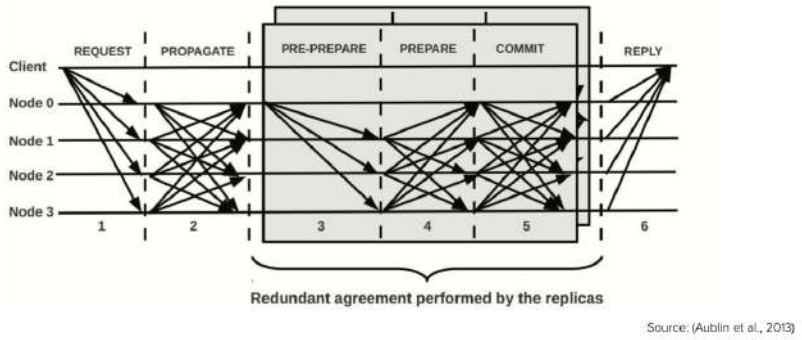


Figura 8: Flow di funzionamento di RBFT

Plenum e RBFT hanno anche associato il concetto di stato. Lo stato non è nient'altro che una proiezione della *ledger* contenente le sue variabili e i loro valori, che vengono cambiati ogni qualvolta un'operazione viene accettata. É salvato in una specifica struttura autenticata chiamata *Merkle Patricia tree*. RBFT utilizza un approccio ottimistico per l'update in

memoria delle transazioni della *ledger* e del loro risultante stato durante la *proposal phase*. Il leader viene aggiornato durante la fase di invio di una nuova *proposal*, mentre le repliche durante la fase di accettazione di una nuova *proposal*. Se per qualche ragione la *proposal* viene respinta, lo stato torna alla situazione precedente. Questo approccio è necessario per riuscire ad avere piu *proposal* che possono essere mandate, senza avere l'esigenza che la precedente sia stata completamente ordinata.
Hyperldger Indy utilizza RBFT sia per l'ordinamento che la validazione delle transazioni, ciò determina un unico *ledger* con ambo le transazioni.

2.1.3 Consenso in Hyperledger Iroha

Hyperledger Iroha utilizza Sumeragi[4] come algoritmo di consenso (di tipologia *Permissioned server reputation system*), che presenta le stesse peculiarità in termini di *fault tolerance* di tutti i sistemi BFT, ovvero riesce a gestire fino a un numero f di *Byzantine fault* nella rete. Si basa su due insiemi di peers, A e B, dove A è l'insieme di 2f + 1 peers, mentre B è il rimanenente numero dei peers presenti nel sistema; concetto cardine di questo algoritmo è l'avere un *ordine globale* di validazione che deve essere rispettato dai diversi peers. In una situazione standard dove non ci sono failure nei peers, dato che per validare una transazione sono necessarie 2f + 1 firme, rispetto alla totalità dei nodi di rete, solo 2f + 1 si preoccupano della validazione della transazione. Qualora ci fossero dei failure nei primi 2f +1 peers, allora verranno chiamati in causa dei nodi per validare la transazione, pescandolo nel set B. Il 2f + 1-esimo peer che effettua la *signature* viene chiamato $proxy - tail$.

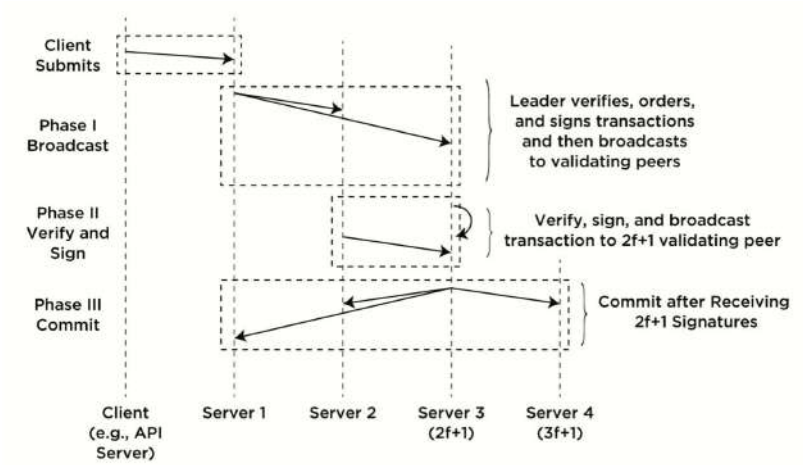


Figura 9: Flow di una transazione senza *failures*

I differenti passaggi necessari per la validazione di una transazione sono i seguenti:

1. il client manda una transazione da validare al *lead validating* peer
2. il peer che riceve la transazione, dopo averla verificata, la firma
3. il peer inoltra la transazione ai restati 2f + 1 peers

4. il processo si ripete fino ad arrivare al $proxy - tail$ che dopo aver ricevuto 2f +1 firme, inoltra il commit a tutti i server

L'ordine dei vari nodi di processamento viene scelto a partire da un indice chiamato *hijiri* che si basa su:

- da quanto tempo il server è online
- quante transazione sono state processate correttamente
- dal numero di failure che hanno avuto i vari server

Per riuscire ad identificare la presenza di un $failure$ in un server, ogni nodo nel momento in cui manda una transazione firmata in broadcast agli altri peer, setta un timer, entro il quale dovrebbe ricevere un reply dal $proxy - tail$ (il timer settato è una stima di quanto tempo impiegano gli altri nodi a firmare a mandare la loro *signauture* al *proxy tail* in modo tale da riuscire ad averne 2f +1 e poter fare il commit). Se non ci sono state risposte prima che il tempo termini, significa che c'è stato un guasto in un server intermedio, quindi i peer che hanno identificato questa situazione, mandano nuovamente la transazione con la loro firma al prossimo nodo nella coda dopo il $proxy - tail$.

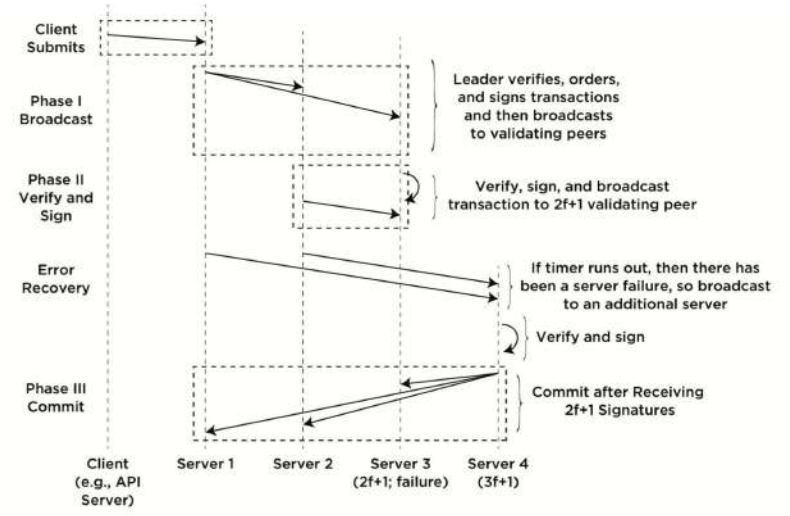


Figura 10: Flow di una transazione con $failure$ nel *proxy tail*

Il consenso in Sumeragi viene ottenuto sulle transazioni singole e su come cambia lo stato globale una volta che sono state applicate. I diversi step che svolge un *validating peer* sono i seguenti:

1. Verifica della firma
2. Verifica del contenuto della transazione
3. Applicazione temporanea della transazione alla *ledger* che si traduce anche nell'aggiornamento della $Merkle$ root dello stato globale

4. Firma del nuovo *Merkle* root e l'hash di ciò che è contenuto all'interno della transazione

5. Invio di un insieme finito ed ordinato di transazioni che prendono il nome di tupla

6. *Sharing* delle parti comuni del *Merkle tree* finchè non c'è match nel root, nel momento in cui deve avvenire la sincronizzazione con gli altri nodi

2.1.4 Consenso in Hyperledger Sawtooth

Hyperldger Sawtooth come algoritmo di consenso[4] utilizza *Proof of Elapsed Time* che un algoritmo di tipologia $lottery - based$ che si traduce in una "lotteria" per l'elezione di un leader. Questo viene scelto in base ad un tempo di attesa garantito che viene fornito da un *Trusted Execution Environment* (TEE). Le caratteristiche fondamentali di un algoritmo di consenso basato su lotteria sono:

- *Fairness*: l'elezione del leader dovrebbe essere distribuita su tutta la popolazione dei partecipanti

- *Investment*: quanto costa controllare l'elezione del leader dovrebbe essere proporzionale al guadagno atteso dalla stessa

- *Verification*: la verifica che il leader sia stato scelto in modo corretto, dovrebbe essere facile per tutti i partecipanti all'elezione

L'implementazione attuale di Hyperledger Sawtooth per l'elezione del leader si basa su *Software Guard Extensions*[15] (SGX), un TEE sviluppato da Intel che permette di avere la giusta randomicità senza ingenti costi in termini di potenza e senza aver bisogno di hardware specifico. Per poter diventare leader, un validator va a chiedere al TEE un tempo random di attesa. Il validator che ottiene il tempo di attesa più breve, ottiene la leadership per quello specifico *transaction block*. L'algoritmo *PoET* per andare ad eleggere un leader presenta delle ottime caratteristiche in termini di distribuzione della scelta rispetto l'intera popolazione di partecipanti andando a favorire in modo proporzionale chi contribuisce con più risorse, intese come processori con all'interno un TEE. Inoltre con questo algoritmo si ha la garanzia che il certificato venga creato all'interno del TEE e che il *validator* abbia effettivamente aspettato il suo *wait time* visto che tutto questo può essere verificato grazie a dalle informazioni che sono contenute in un'attestazione di esecuzione. Questo algoritmo può anche essere definito robusto perchè la popolazione dei *validator* è larga, dato che, il costo in termini di potenza per partecipare all'elezione, è basso.

3 Smart Contracts in Hyperledger

3.1 Introduzione agli Smart Contracts

Gli **Smart Contracts** sono protocolli digitali che definiscono e automatizzano l'esecuzione di accordi contrattuali tra le parti coinvolte. Essi sono basati su algoritmi e logica di programmazione che definiscono le condizioni e le azioni da intraprendere in risposta a determinati eventi o input. Esistono due tipi differenti di smart contracts[1]:

- ***Installed Smart Contracts*** installano la logica di business sui validatori della rete prima che la rete venga avviata.
- ***On-chain Smart Contracts*** distribuiscono la logica di business come una transazione registrata sulla blockchain e successivamente richiamata da transazioni successive. Con gli on-chain smart contracts, il codice che definisce la logica di business diventa parte del registro (ledger).

Gli Smart Contracts in Hyperledger sono implementati attraverso il concetto di *"chaincode"*. Questi chaincode vengono scritti in linguaggi di programmazione come Go, JavaScript o Java e vengono eseguiti all'interno dell'ambiente di esecuzione specifico del framework Hyperledger scelto.

Gli Smart Contracts offrono numerosi vantaggi, tra cui:

- ***Automazione***: automatizzano l'esecuzione di accordi contrattuali, eliminando la necessità di intermediari umani e riducendo il rischio di errori umani.
- ***Sicurezza***: sono immutabili e crittograficamente sicuri. Una volta eseguiti, non possono essere modificati e garantiscono l'integrità dei dati e delle transazioni.
- ***Efficienza***: consentono l'esecuzione automatica di transazioni, riducendo i tempi e i costi associati alle procedure manuali.

Gli Smart Contracts svolgono un ruolo fondamentale nella tecnologia blockchain di Hyperledger, fornendo la logica di business per l'esecuzione e la validazione delle transazioni sulla rete. Essi consentono la programmazione di regole e condizioni specifiche che vengono applicate in modo autonomo e trasparente a tutte le parti coinvolte nella blockchain.

3.1.1 Smart Contracts nei framework di Hyperledger

Quattro dei framework di blockchain di Hyperledger supportano gli smart contracts:

- ***Hyperledger Burrow***
- ***Hyperledger Fabric***
- ***Hyperledger Iroha***
- ***Hyperledger Sawtooth***

In tutti questi framework, il livello degli smart contracts è responsabile del processo delle richieste di transazione e della determinazione della validità delle transazioni attraverso l'esecuzione della logica di business. Ogni framework supporta gli smart contracts in modo leggermente diverso.

Questi quattro framework di Hyperledger offrono supporto per lo sviluppo e l'esecuzione di smart contracts. Gli smart contracts consentono di implementare e automatizzare la logica di business all'interno della blockchain. Ogni framework ha la propria implementazione specifica del livello degli smart contracts, che consente agli sviluppatori di definire e gestire i *smart contracts* in modo personalizzato.

3.2 Smart Contracts in Hyperledger Burrow

Hyperledger Burrow è una macchina di smart contract permessionata. Fornisce un client di blockchain modulare con un interprete di smart contract permessionato costruito secondo le specifiche della *Ethereum Virtual Machine* (EVM), con alcune estensioni e alcuni cambiamenti ancora da incorporare. **Hyperledger Burrow** accoppia il suo motore di esecuzione EVM con il motore di consenso Tendermint tramite un'interfaccia applicazione-consenso chiamata ABCI. Lo stato dell'applicazione consiste in tutti gli account, l'insieme di validatori e il registro dei nomi. Gli account in **Hyperledger Burrow** hanno permessi e contengono o il codice degli smart contract o corrispondono a una coppia di chiave pubblica-privata. Una transazione che chiama il codice degli smart contract in un determinato account attiva l'esecuzione del codice di quell'account in una macchina virtuale permessionata[1].

Lo stato dell'applicazione consiste in tutti gli account, l'insieme di validatori e il registro dei nomi incorporato in **Hyperledger Burrow**. Una transazione che chiama il codice degli smart contract in un determinato account attiva l'esecuzione del codice di quell'account in una macchina virtuale permessionata.

3.2.1 Funzioni Native Sicure e livello di Permesso

Le funzioni native sicure stabiliscono le regole di base che tutti gli account e tutto il codice degli smart contract devono seguire. Non risiedono come codice EVM, ma sono esposte all'EVM permessionato tramite contratti di interfaccia. L'accesso è regolato attraverso le funzioni native sicure e l'accesso dipende dall'esecuzione di tutto il codice degli smart contract.

Hyperledger Burrow prevede un framework di funzioni native sicure che supporta l'utilizzo di codice in linguaggio nativo per prestazioni e sicurezza migliori. Le funzioni native sicure possono essere esposte all'EVM permessionato all'interno di **Hyperledger Burrow**. Inoltre, possono essere strutturate per migliorare le prestazioni degli smart contract e fornire una gamma di funzioni a livello privilegiato alle applicazioni dell'ecosistema, che dovrebbero essere sviluppate nativamente ed esposte all'EVM permessionato. Sono in corso sforzi per sistematizzare ciò e aggiungere funzionalità avanzate per supportare una vasta gamma di utenti.

Hyperledger Burrow include un livello di permesso basato sulle capacità e in evoluzione. La rete viene avviata con un insieme iniziale di account con permessi e un insieme predefinito globale di permessi. I partecipanti alla rete con le autorizzazioni corrette pos-

sono modificare i permessi di altri account inviando un tipo di transazione appropriato alla rete. Questa transazione viene valutata dai validatori di rete prima che i permessi vengano aggiornati sull'account di destinazione. Attraverso l'EVM, possono essere sfruttati ulteriori meccanismi di autorizzazione basati su ruoli attraverso i ruoli di Hyperledger Burrow su ciascun account. I ruoli possono essere aggiornati tramite transazioni discrete o smart contract.
Inoltre, **Hyperledger Burrow** offre la possibilità agli smart contract all'interno dell'**EVM permessionato** di modificare il livello di autorizzazione e i ruoli degli account. Una volta che un contratto con questa funzionalità è stato distribuito su una blockchain, un partecipante alla rete con le autorizzazioni appropriate può concedere al contratto tale capacità.

3.2.2 EVM permessionato

Questa macchina virtuale è progettata per osservare le specifiche delle operazioni di Ethereum e affermare che sono stati concessi i permessi corretti. Ad ogni esecuzione viene assegnata una quantità arbitraria ma finita di gas, ovvero la tassa di esecuzione per ogni operazione eseguita su Ethereum. Ciò garantisce che l'esecuzione venga completata entro un periodo di tempo finito.

Le transazioni devono essere formulate in un formato binario che può essere elaborato dal nodo della blockchain utilizzando un'interfaccia binaria dell'applicazione (ABI). Una serie di strumenti open source provenienti da Monax e dalla comunità Ethereum consentono agli utenti di compilare, distribuire e collegare smart contract compilati per l'EVM permessionato e di formulare transazioni che richiamano gli smart contract.

L'EVM permessionato stesso è progettato e implementato come una funzione senza stato per transizionare in modo deterministico e verificabile lo stato dell'EVM data una transazione. Questo pacchetto di codice potrebbe essere integrato in diversi progetti Hyperledger. Ad esempio, le famiglie di transazioni estensibili in Hyperledger Sawtooth consentono di considerare l'EVM permessionato come un processore di transazioni nel framework del registro permessionato di Sawtooth.

3.2.3 Gateway, Firma e Interfacce

Hyperledger Burrow espone endpoint RESTful e JSON-RPC per permettere ai client di interagire con la rete di blockchain e lo stato dell'applicazione, sia inviando transazioni che interrogando lo stato corrente dell'applicazione. I WebSocket consentono a componenti di interfacciarsi e sottoscriversi agli eventi. Questo è particolarmente prezioso poiché il motore di consenso e il motore dell'applicazione degli smart contract possono fornire risultati definitivamente finalizzati alle transazioni dopo ogni blocco.
Hyperledger Burrow accetta transazioni formulate e firmate dal lato client e mette a disposizione un'interfaccia per la firma remota. Le soluzioni di firma esterne sono cruciali per gli utenti di Hyperledger Burrow, poiché consentono ai nodi della blockchain di funzionare su hardware di consumo.
Hyperledger Burrow utilizza anche interfacce di avvio e runtime, principalmente tramite file letti dal nodo della blockchain all'avvio. Naturalmente, Burrow include anche una chiamata di procedura remota (RPC) che consente l'interfacciamento con il nodo durante l'esecuzione.

3.3 Smart Contracts in Hyperledger Fabric

Un smart contract in Hyperledger Fabric è un programma chiamato *chaincode*. Il chaincode può essere scritto in Go, JavaScript (node.js) e, eventualmente, in altri linguaggi di programmazione come Java che implementano un'interfaccia prescritta. Il chaincode, che inizializza e gestisce lo stato del registro attraverso transazioni inviate dalle applicazioni[1], viene eseguito in un contenitore Docker sicuro, isolato dal processo del peer che lo approva. Di solito, un chaincode gestisce la logica aziendale su cui i membri della rete sono concordi. Lo stato creato da un chaincode è limitato esclusivamente a quello specifico e non può essere accessibile direttamente da un altro. Tuttavia, con le autorizzazioni appropriate, un chaincode nella stessa rete ne può richiamare un altro per accedere al suo stato.

Ci sono due tipi di chaincode da considerare:

- **Chaincode di Sistema**: gestisce tipicamente transazioni legate al sistema come la gestione del ciclo di vita e la configurazione delle politiche. Tuttavia, l'API del chaincode di sistema è aperta agli utenti per implementare anche le proprie esigenze applicative

- **Chaincode di Applicazione**: gestisce gli stati delle applicazioni sul registro, inclusi asset digitali o record di dati arbitrari.

3.3.1 Chaincode di Applicazione

Analizzando più nel dettaglio i chaincode applicativi, si può dire come questi inizino con un pacchetto che racchiude metadati critici su loro stessi, includendo il nome, la versione e le firme delle controparti per garantire l'integrità del codice e dei metadati. Questo pacchetto viene quindi installato sui nodi di rete delle controparti.
Un membro appropriato della rete (come controllato dalla configurazione delle politiche) attiva il chaincode inviando una transazione di istanziazione alla rete. Se la transazione viene approvata, il chaincode entra in uno stato attivo in cui può ricevere transazioni dagli utenti tramite applicazioni lato client.
Tutte le transazioni del chaincode che vengono convalidate vengono aggiunte al registro condiviso. Queste transazioni possono quindi modificare lo stato del mondo di conseguenza. In qualsiasi momento dopo che un chaincode è stato istanziato, può essere aggiornato attraverso una transazione di aggiornamento.
Utilizzando il Chaincode per Sviluppare Contratti Aziendali e Applicazioni Decentralizzate
Esistono generalmente due modi per sviluppare contratti aziendali in Hyperledger Fabric:

- Codificare contratti individuali in istanze indipendenti di chaincode.

- Utilizzare un unico chaincode per gestire tutti i contratti (di determinati tipi) e avere API che gestiscono il ciclo di vita di quei contratti. Il secondo approccio è probabilmente più efficiente.

Utilizzando il Chaincode per Definire e Gestire Asset gli utenti di Hyperledger Fabric possono anche utilizzare il chaincode per definire gli asset e la logica che li gestisce.
Nella maggior parte delle soluzioni blockchain, esistono due approcci popolari per definire gli asset:

- Il modello UTXO (unspent transaction output) senza stato, in cui i saldi degli account sono codificati in registri di transazioni passate.
- Il modello degli account, in cui i saldi degli account sono conservati nello spazio di archiviazione dello stato nel registro.

Entrambi gli approcci hanno vantaggi e svantaggi. Hyperledger Fabric non richiede l'uno o l'altro, ma si assicura che entrambi gli approcci siano facili da implementare.

3.4 Smart Contracts in Hyperledger Indy

Hyperledger Indy non ospita smart contracts. Invece di memorizzare dati nel registro e fornire accesso a tali dati tramite smart contracts, Indy consente agli utenti di possedere i dati e condividerli in modo da preservare la loro privacy[1].
Le identità di Hyperledger Indy possono essere referenziate negli smart contracts di altri sistemi. Ciò consente ad Indy di fornire a qualsiasi sistema di registro distribuito un sistema di identità decentralizzato di prim'ordine.
Hyperledger Indy supporta plugin che consentono il supporto di nuove transazioni senza dover modificare i componenti principali del codice sorgente. Un esempio potrebbe essere la creazione di una semplice criptovaluta su Indy.

3.5 Smart Contracts in Hyperledger Iroha

Hyperledger Iroha supporta gli smart contracts per consentire la definizione e l'esecuzione di logica aziendale all'interno della rete. Gli smart contracts in Iroha sono scritti utilizzando il linguaggio di programmazione C++.
Gli smart contracts in Iroha sono implementati come plugin che vengono eseguiti all'interno del nodo Iroha. Questi plugin possono interagire con il ledger e manipolare i dati dello stato.
Per sviluppare smart contracts in Iroha, è necessario creare un nuovo plugin che implementi l'interfaccia fornita da Iroha per gli smart contracts. Questa interfaccia definisce i metodi e le funzionalità che devono essere implementati per consentire l'esecuzione degli smart contracts all'interno del nodo.
Una volta che lo smart contract è stato implementato come plugin, può essere installato e attivato sui nodi Iroha della rete. Una transazione che richiede l'esecuzione di uno smart contract può essere inviata alla rete Iroha, e il nodo eseguirà lo smart contract corrispondente per elaborare la transazione.
Gli smart contracts in Iroha possono accedere ai dati presenti nel ledger e possono anche emettere nuove transazioni per aggiornare lo stato o interagire con altri smart contracts.
È importante notare che Hyperledger Iroha supporta gli smart contracts solo nel contesto dei plugin C++. Altri linguaggi di programmazione potrebbero non essere supportati direttamente e richiederebbero l'implementazione di un'apposita infrastruttura per il supporto degli smart contracts[1].

3.6 Smart Contracts in Hyperledger Sawtooth

Hyperledger Sawtooth supporta due tipi di smart contracts: contratti installati (*installed smart contracts*) e contratti on-chain. Gli sviluppatori possono scegliere tra sette linguaggi per lo sviluppo degli smart contracts in Sawtooth[2].

3.6.1 Contratti Installati con Famiglie di Transazioni

Al fine di limitare i rischi associati a linguaggi di programmazione completamente programmabili, Sawtooth specifica delle semantiche di transazione fisse. Queste semantiche sono implementate tramite famiglie di transazioni che supportano solo operazioni specifiche consentite. In questo contesto, una famiglia di transazioni può essere considerata come un'applicazione distribuita.
Un esempio semplice è la famiglia di transazioni *IntegerKey*, che fornisce solo tre operazioni: incremento, decremento e impostazione. Con sole tre operazioni e senza cicli, questa famiglia contribuisce a prevenire eventuali problemi intenzionali o accidentali nello script delle transazioni.
Un altro esempio è la famiglia di transazioni *Settings*, che può essere utilizzata per controllare la rete blockchain stessa, inclusi aspetti come il tipo di consenso utilizzato e il tempo interno dei blocchi.
Un esempio più complesso che blocca la sintassi arbitraria è la famiglia di transazioni *supply chain*. Le semantica di questa famiglia includono circa 20 operazioni necessarie per tracciare la provenienza e altre informazioni contestuali di qualsiasi asset, ma non includono ulteriori operazioni che potrebbero essere utilizzate in modo improprio, né intenzionalmente né per errore.
Qualsiasi famiglia di transazioni può essere distribuita con Hyperledger Sawtooth, purché supporti l'API delle famiglie di transazioni. Questa è un'API semplice che supporta alcune operazioni come la lettura dello stato per recuperare informazioni dal registro e la scrittura dello stato per aggiornare il registro.
Le famiglie di transazioni possono essere scritte in quasi tutti i linguaggi, tra cui C++, Go, Java, JavaScript, Python, Rust e Solidity tramite Seth. Alcune delle famiglie di transazioni esistenti che supportano l'API includono *Blockinfo*, *Identity*, *IntegerKey*, *Settings*, *Smallbank*, *Validator registry* e *XO*.
Il concetto di famiglie di transazioni consente alle aziende di scegliere il livello di versatilità e rischio più adatto per la propria rete. Un vantaggio del concetto di famiglia di transazioni, rispetto alle transazioni on-chain, è che un bug super critico può influire solo sul processo della famiglia di transazioni. Gli altri validatori e tutte le altre famiglie di transazioni possono continuare a funzionare. Al contrario, un bug super critico eseguito on-chain potrebbe bloccare l'intero nodo.

3.6.2 Contratti On-Chain con la Famiglia di Transazioni Seth

I contratti on-chain sono gestiti collegando la Hyperledger Burrow Ethereum Virtual Machine (EVM) al nodo validator di Hyperledger Sawtooth. Una volta fatto ciò, è possibile scrivere smart contracts utilizzando il codice *Solidity*.

4 Conclusioni

In conclusione, il progetto Hyperledger mette a disposizione un'infrastruttura open-source scalabile e modulare. Fornisce ai suoi utenti un insieme di frameworks e tools che possono rispondere ad esigenze di natura diversa basati sulla tecnologia blockchain.
I diversi progetti nati a partire da Hyperldger strizzano l'occhio alle features di scalabilità, efficienza e finalità in quanto, a differenza del capostipite Bitcoin, non implementano in nessuna casistica la $Proof\ of\ Work$ (PoW) come algoritmo di consenso, garantendo mediamente performance migliori.
Inoltre, i framework di Hyperledger che supportano gli Smart Contracts, consentono di personalizzare la gestione di quest'ultimi.
La caratteristica open-source e la possibilità di personalizzare i framework in base alle proprie necessità lo rende appetibile per diverse applicazioni aziendali, come illustrato nei casi d'uso.

Riferimenti bibliografici

[1] Smart Contracts in Hyperledger, https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf

[2] Hyperledger Sawtooth official documentation, https://sawtooth.hyperledger.org/docs/1.2/

[3] An Introduction to Hyperledger https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf

[4] Design Philosophy and Consensus in Hyperledger, https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

[5] A Review on Consensus Algorithm of Blockchain, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8123011

[6] https://ieeexplore-ieee-org.ezproxy.biblio.polito.it/document/9210358

[7] Blockchain System Defensive Overview for Double-Spend and Selfish Mining Attacks: A Systematic Approach, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9308934

[8] The Byzantine Generals Problem, https://lamport.azurewebsites.net/pubs/byz.pdf

[9] Proof-of-Elapsed-Time Consensus with Distributed Coordination for Blockchain Networks, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9472787

[10] Evaluating Proof-of-Work Consensus Protocols' Security, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8835227

[11] RBFT: Redundant Byzantine Fault Tolerance, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6681599

[12] Blockchain Consensus Protocols in the Wild, https://arxiv.org/pdf/1707.01873.pdf

[13] A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8416470

[14] The Honey Badger of BFT Protocols, https://eprint.iacr.org/2016/199.pdf

[15] Leveraging Intel SGX Technology to Protect Security-Sensitive Applications, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8548184

WELCOME TO DECENTRALAND

Alex Carluccio, Samuele Longo, Veronica Orciuoli, Lorenzo Spinardi

Politecnico di Torino

Dipartimento di Scienze Matematiche

Corso di Laurea in Ingegneria Matematica

Blockchain e Criptoeconomia

Welcome To Decentraland

Professore:

Prof. Danilo Bazzanella

Autori:

Carluccio Alex s302373
Longo Samuele s305202
Orciuoli Veronica s303496
Spinardi Lorenzo s305725

Anno accademico 2022/2023

Contents

1 Il Metaverso **3**
1.1 Perchè il Metaverso è importante? 3
1.2 Storia del Metaverso 3

2 Introduzione a Decentraland **4**
2.1 Storia 5

3 Come funziona Decentraland? **6**
3.1 Entriamo nel metaverso 8
3.2 MANA e LAND 9
3.3 Acquistare "terra" in Decentraland 10
3.4 Architettura 10

4 Andamento e prezzo **11**

5 DAO **12**

6 Differenze con un altro metaverso: The Sandbox **13**

7 Pro e Contro **14**
7.1 Pro 14
7.2 Contro 15

8 Esplorando il metaverso **15**
8.1 OpenSea: Museo di NFT 16
8.2 Decentraland Metaverse Fashion Week 2023 18

9 Giochi su Blockchain **19**
9.1 Come si differenziano i Blockchain games dai giochi tradizionali? 19
9.2 I 10 migliori giochi basati su blockchain 20
9.2.1 The Sandbox 20
9.2.2 Axie Infinity 21
9.2.3 Enjin Coin 21
9.2.4 Illuvium 22
9.2.5 STEPN 22
9.2.6 Treasure 23

9.2.7 My Neighbor Alice 23
9.2.8 Mobox 24
9.2.9 Vulcan Forged 24

10 Il futuro di Decentraland **25**

1 Il Metaverso

Il metaverso è un mondo virtuale in cui miliardi di persone vivono, lavorano, fanno shopping, imparano e interagiscono l'una con l'altra, tutto dal comfort del proprio divano nel mondo reale.
In questo mondo, i computer che venivano utilizzati per connettersi ad una rete di informazioni sono diventati portali per un mondo virtuale tridimensionale tangibile, simile alla vita reale, popolato da avatar che si spostano liberamente da una esperienza all'altra. Per ora il Metaverso non esiste, ma potrebbe svilupparsi sulla nuova infrastruttura del Web3.

1.1 Perchè il Metaverso è importante?

Il termine "Metaverso" è diventato di uso comune quando Facebook ha ribattezzato la sua identità aziendale in Meta nell'ottobre 2021 e ha annunciato piani per investire almeno 10 miliardi di dollari.
Oltre a Meta, giganti come Google, Microsoft, Nvidia e Qualcomm stanno investendo miliardi nel progetto. La società di consulenza manageriale McKinsey & Company ha previsto con ottimismo che l'economia del metaverso potrebbe raggiungere i 5 trilioni di dollari entro il 2030.
Oggi, le aziende usano il termine "Metaverso" per riferirsi a molti e diversi tipi di ambienti online migliorati. Questi spaziano dai videogiochi online a posti di lavoro virtuali, come Mesh di Microsoft o Horizon Workrooms di Meta, fino a spogliatoi e sale operatorie virtuali.

1.2 Storia del Metaverso

Figure 1: Copertina di Snow Crash, versione Italiana

Il termine "Metaverso" venne coniato da Neal Stephenson in una sua novella in stile cyberpunk del 1992 intitolata "Snow Crash" (Figura 1). Nel libro, il metaverso, viene descritto come un posto immaginario all'interno del quale gli sviluppatori possono creare di tutto, reso disponibile al mondo intero grazie ad una rete in fibra ottica ed accessibile tramite degli occhiali per la realtà virtuale (VR).

2 Introduzione a Decentraland

Decentraland (Figura 2) è una piattaforma decentralizzata costruita sulla blockchain di Ethereum che dà vita a un mondo digitale in cui i membri possono vivere, creare esperienze, generare e monetizzare i propri contenuti. Alla fine di dicembre 2021, ci sono più di 800.000 utenti registrati e circa 500.000 utenti attivi mensili.

Ma chi ha creato Decentraland? [7] Gli informatici argentini Esteban Or-

Figure 2: Decentraland

dano e Ari Meilich sono i padri fondatori di Decentraland.
Il metaverso, in realizzazione dal 2015, raccolse più di 24 milioni di dollari (86,260 ETH) ad agosto 2017, mentre in una ICO vendette più di un miliardo di MANA (il token ERC-20 del progetto), ad un prezzo compreso tra 0.024$ e 0.04$. I "pacchetti" di 1000 token ciascuno vennero esauriti in soli 35 secondi.
Nel dicembre del 2017 fu organizzata l'asta della "Genesis City": vennero

Figure 3: Genesis City

venduti 90.000 riquadri di terreno (LAND), per 1000 token MANA l'uno (circa 20), appartenenti alla prima area del metaverso.
Ogni LAND è un token non fungibile (NFT) e 40.000 furono usati per creare "distretti" a tema, proposti dalla community di Decentraland.
A marzo 2018, fu poi rilasciato il Decentraland Marketplace, così da rendere disponibile per i giocatori la compravendita di appezzamenti LAND della Genesis City, oltre a dare occasione di esplorare l'area nella mappa del metaverso.
I tre aspetti di Decentraland, aperto, decentralizzato e guidato dalla comunità, sono la spinta alla base del progetto Genesis.City map (Figura 3). Il progetto è stato il favorito di una sovvenzione DAO nel 2022, con un rinnovo recente [8].
Si può osservare come il mondo di Decentraland sia la combinazione di due tecnologie: realtà virtuale e blockchain. Infatti, la realtà virtuale permette a chiunque di vagare per Genesis City e la blockchain è responsabile di rendere tutte le transazioni trasparenti e affidabili.

2.1 Storia

Decentraland [5] è nata come una proof-of-concept per l'assegnazione della proprietà di beni immobili digitali agli utenti su una blockchain. Questo immobile digitale è stato inizialmente implementato come un pixel su una griglia 2D infinita.
Risultava come una griglia 2D infinita, dove ogni pixel conteneva metadati che identificavano il proprietario e descrivevano il colore del pixel.
L'esperimento è stato intitolato: l'età della pietra di Decentraland.
Alla fine del 2016, il team ha iniziato a sviluppare l'Età del bronzo (Figura 4),

un mondo virtuale in 3D suddiviso in appezzamenti di terreno. Il proprietario di ogni appezzamento poteva associarlo a un file con un hash riferimento, utilizzando una blockchain Bitcoin modificata. Da questo riferimento, gli utenti del mondo virtuale potevano utilizzare una Distributed Hash Table (DHT) e BitTorrent per scaricare il file contenente il lotto, il quale definisce i modelli e le texture da visualizzare in quel luogo.

Figure 4: Età del bronzo: le strutture create dalla comunità intorno l'appezzamento di Genesis, situato alle coordinate (0,0).

La successiva versione di Decentraland, l'età del ferro, crea un'esperienza sociale con un'economia guidata dai livelli esistenti di proprietà della terra e di distribuzione dei contenuti.
Nell'età del ferro gli sviluppatori possono creare applicazioni su Decentraland, distribuirle ad altri utenti e monetizzarle.
L'età del ferro implementa le comunicazioni peer-to-peer, un sistema di scripting per contenuti interattivi e un sistema di pagamenti veloci in criptovaluta per le transazioni nel mondo. Un livello di comunicazione è essenziale per le esperienze sociali: Decentraland realizza questo obiettivo con una rete P2P.
Il sistema di scripting è lo strumento che i proprietari del terreno utilizzano per descrivere il comportamento e le interazioni degli oggetti 3D, dei suoni e delle applicazioni in esecuzione sui terreni.
Infine, un sistema di pagamento con commissioni ridotte è fondamentale per sviluppare un'economia in un ambiente rapido come quello virtuale.

3 Come funziona Decentraland?

Le blockchain sono database decentralizzati distribuiti tra le macchine di una rete. Le transazioni sono raggruppate in "blocchi" ed elaborate in sequenza

per formare una catena di eventi.
Ethereum è una delle blockchain più note: la più grande differenza dalle altre, come Bitcoin, è che utilizza la blockchain come archivio non solo per record di transazioni valutarie, bensì può memorizzare informazioni più complesse per distinguere diversi tipi di token o persino gestire token unici con caratteristiche specifiche.
Decentraland [4] utilizza la blockchain di Ethereum per schedare la proprietà delle risorse digitali e altri oggetti negoziabili che possono essere proiettati su una scena 3D. La blockchain non viene utilizzata per memorizzare la posizione del giocatore, la disposizione dello scenario, o altro che può cambiare in tempo reale mentre un giocatore interagisce. Queste informazioni vengono registrate localmente sulla macchina di ogni giocatore o su un server privato appartenente al proprietario dello scenario. Gli sviluppatori di ogni scena devono scegliere quali informazioni vale la pena archiviare sulla blockchain e cosa archiviare invece su un server privato.
I token Ethereum sono detenuti dai wallet, il quale può contenere vari token, inclusi Ether, MANA, LAND e altri token che possono essere utilizzati da giochi o esperienze in Decentraland.
Per utilizzare il Marketplace (Figura 5) o per accedere a Decentraland, bisogna utilizzare un wallet integrato nel browser web, di conseguenza quelli consigliati sono i seguenti:

- Metamask
- Trezor/Ledger hardware wallets

Ogni wallet ha una chiave pubblica e una privata. L'hash della chiave pubblica è l'indirizzo univoco del wallet, utilizzato per instradare le transazioni e identificare un giocatore. La chiave privata viene utilizzata dal wallet per firmare ogni transazione che si inoltra alla rete e certificare che è stata effettivamente inviata dall'utente. La chiave privata viene utilizzata anche per ripristinare il wallet nel caso in cui la password venga persa o dimenticata.

In Decentraland, le identità dei giocatori sono costruite attorno ai wallet. Siccome le chiavi pubbliche sono univoche, si possono utilizzare per identificare un utente. I Token differenti possono dare ad un giocatore un avatar unico, un abito, permessi per entrare in luoghi che scelgono di limitare l'accesso ecc.
Un contratto è costituito sia da un codice che da dati, i quali risiedono su un indirizzo specifico sulla blockchain di Ethereum. Un contratto non può

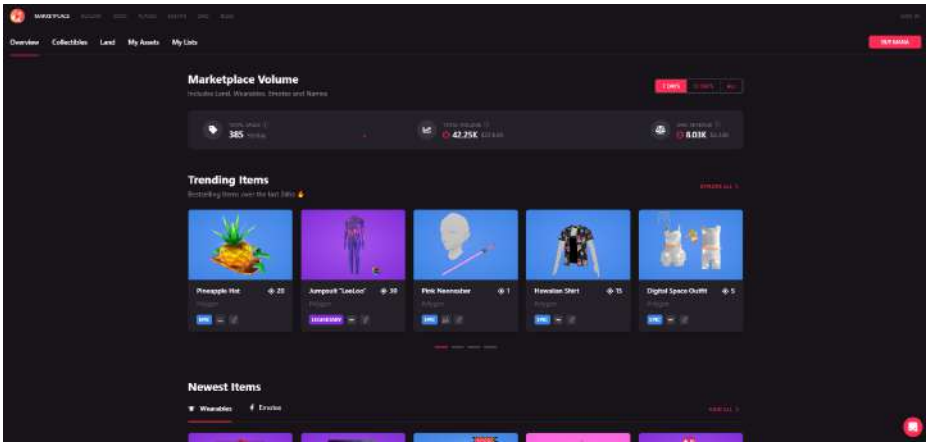


Figure 5: Marketplace

attivare alcuna azione da solo o in base a un evento temporale. Tutte le azioni eseguite da uno smart contract derivano sempre da una transazione che chiama una delle funzioni del contratto. È possibile utilizzare gli smart contracts per condizionare le transazioni in base a condizioni personalizzate. Ad esempio, i giocatori potrebbero scommettere sul risultato di una partita e i pagamenti corrispondenti avverrebbero non appena il risultato della partita viene comunicato al contratto. L'intero codice di uno smart contract è pubblico a chiunque voglia leggerlo. Ciò consente agli sviluppatori di creare regole verificabili pubblicamente.
Tutti i gettoni sono definiti da uno smart contract che ne specifica le caratteristiche. Decentraland ha scritto e gestisce una serie di smart contracts: i token LAND e MANA sono definiti rispettivamente dai contratti LANDregistry e MANAtoken. L'indirizzo di ogni contratto creato da Decentraland si trova in Decentraland smart contracts. È possibile leggere il codice completo di ciascuno di questi contratti, poiché si tratta di informazioni pubbliche sulla blockchain. È possibile trovare il contratto per nome su Etherscan e leggerne il contenuto.

3.1 Entriamo nel metaverso

Decentraland (Figura 6) viene paragonato spesso a Second Life, con la differenza che quest'ultimo non è basato su una blockchain. Infatti, i linden, la moneta di Second life, non sono criptovalute.

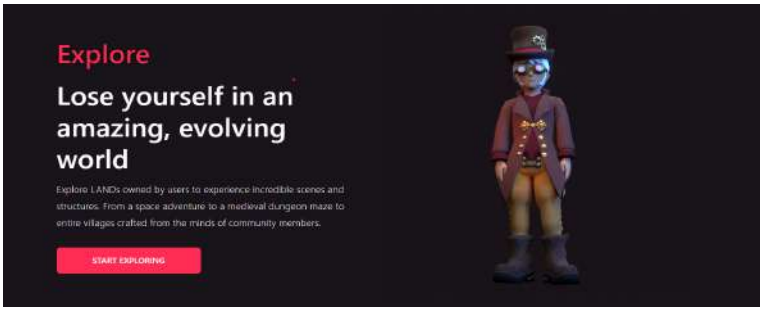


Figure 6: Decentraland.org

Nella schermata del login (Figura 7) si cominciano a vedere ulteriori differenze: nel cosidetto web 1.0 l'utente si loggava tramite username e password, attualmente nel web 2.0 l'utente può loggarsi tramite google, facebook, ecc. e nel web3 esiste ora "collega il tuo wallet".

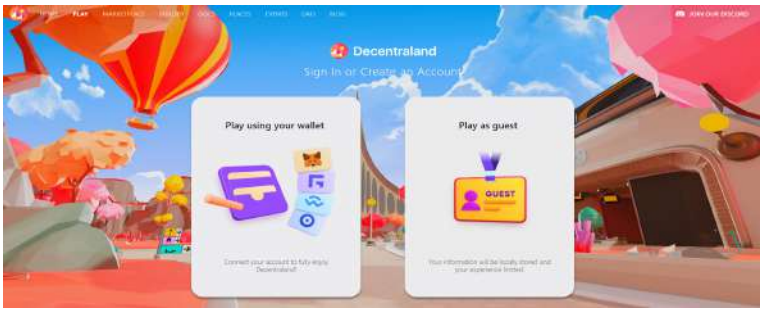


Figure 7: Pagina login su decentraland.org

3.2 MANA e LAND

Ci sono due token nel mondo di Decentraland: il primo è il token MANA, il secondo è LAND [4].
I possessori di token MANA possono partecipare alla governance del protocollo e possono acquisire lotti di terreno virtuali all'interno di Decentraland. Questo token è stato creato seguendo lo standard ERC-20 di Ethereum, quindi può essere facilmente integrato nelle piattaforme DeFi, DEX e altri dApps di Ethereum, permettendone un rapido scambio.
Inoltre, Decentraland ha limitato l'esistenza dei token MANA a un totale di

2.194.460.527 token, in modo da renderli più preziosi man mano che aumenta l'utilizzo della piattaforma.
Il secondo token è un token non fungibile che segue lo standard ERC-721. Ogni token LAND identifica in modo univoco le proprietà di un appezzamento di terreno di proprietà di un utente Decentraland. Per acquisire token LAND, l'utente deve scambiare i propri token MANA con token LAND, un'azione che brucia gettoni MANA, rendendolo più raro e prezioso.
Data questa relazione, anche l'esistenza dei token LAND è limitata. Inoltre, quando si tengono insieme due token LAND (due pacchi adiacenti), allora si sta tenendo un token Estate. Questo tipo di token è importante perché i token MANA, LAND e Estate possono essere usati nella governance Decentraland.

3.3 Acquistare "terra" in Decentraland

Ogni LAND su Decentraland misura 16x16 metri quadrati ed è rappresentato come un NFT. Il numero di appezzamenti di terreno su Decentraland è limitato a 90.000, il che contribuisce a creare scarsità. Chiunque può acquistare, affittare o vendere terreni su Decentraland tramite OpenSea, un marketplace NFT, o tramite il Marketplace ufficiale di Decentraland.

3.4 Architettura

Il protocollo di Decentraland [5] è formato da tre layers:

- Layer di consenso: tieni traccia della proprietà della terra e del suo contenuto.
- Layer del contenuto del terreno: scarica le risorse utilizzando un sistema di distribuzione decentralizzato.
- Layer in tempo reale: consente agli utenti di connettersi tra loro.

La proprietà della terra è stabilita a livello di consenso e il contenuto della terra è referenziato tramite un hash al contenuto del file. Da questo riferimento il contenuto può essere scaricato da BitTorrent o IPFS. Il file scaricato contiene una descrizione di oggetti, trame, suoni e altri elementi necessari per il rendering della scena. Inoltre, contiene l'URL di un server per coordinare le connessioni tra gli utenti P2P che stanno esplorando il tile contemporaneamente. In Figura 8 possiamo osservare un diagramma delle fasi che gli utenti

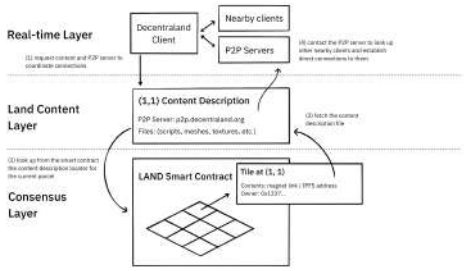


Figure 8: Il protocollo di Decentraland per utenti simultanei in un mondo virtuale decentralizzato.

di Decentraland eseguono per l'esperienza di un mondo virtuale condiviso in a modo decentrato.

4 Andamento e prezzo

Decentraland (MANA) ad oggi possiede una capitalizzazione di mercato di 799.75M EUR. Il volume di trading in 24 ore è di circa 59.20M EUR. Il prezzo

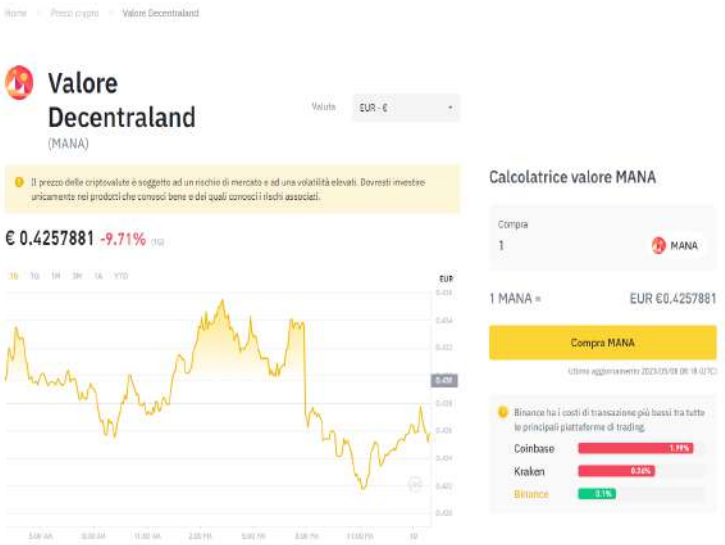


Figure 9: Decentraland andamento e prezzo in tempo reale.

ad Aprile 2023 è oscillato tra 0.49 EUR e 0.63 EUR [1].
Dal suo lancio tramite una ICO nel 2017 ha avuto il suo picco di prezzo di 4.32 EUR e una capitalizzazione di mercato pari a 7.9 miliardi di EUR a fine Novembre 2021. Dopo questa data ha subito un veloce calo fino a quando ha iniziato a stabilizzarsi, seguendo l'andamento delle principali criptovalute Bitcoin ed Ethereum.

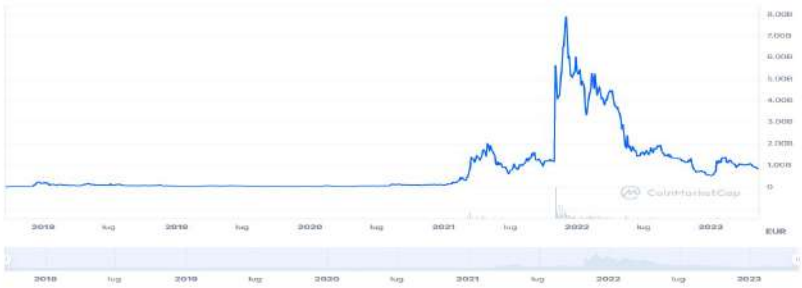


Figure 10: Decentraland andamento del prezzo dal lancio sul mercato.

5 DAO

Decentraland è il primo mondo virtuale completamente decentralizzato. È sempre stato parte della visione originale consegnare il controllo alle persone che creano e giocano in questo spazio virtuale. Il Decentraland DAO è un tool utilizzato dai possessori di MANA e LAND per prendere decisioni all'interno del mondo virtuale. Gli utenti, attraverso il DAO, hanno a disposizione il controllo delle politiche create per determinare il comportamento del mondo: ad esempio, quali tipi di oggetti indossabili sono consentiti (o non consentiti) dopo il lancio del DAO, la moderazione dei contenuti, la politica di LAND e le aste. Per evitare le gas-fee per la realizzazione di una proposta, è possibile effettuarla off-chain (ovvero al di fuori della governance della blockchain) per poi essere eventualmente approvata ed inserita nella blockchain. Le votazioni si svolgono sull'interfaccia di governance di Decentraland DAO, gestita da Aragon.
Inoltre, le proposte con i relativi voti associati vengono memorizzate in IPFS tramite l'utilizzo di Snapshot, una piattaforma di voting che consente di votare in maniera gratuita senza l'utilizzo di gas.

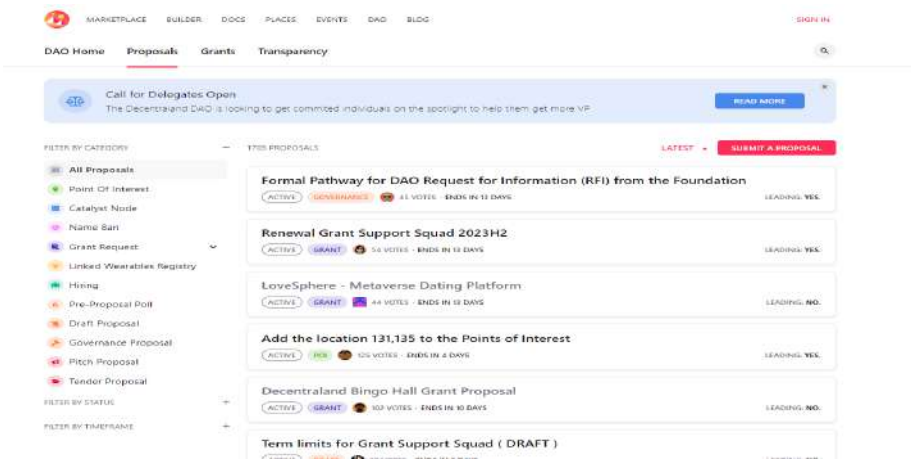


Figure 11: Decentraland DAO proposals.

6 Differenze con un altro metaverso: The Sandbox

Un altro metaverso che vale la pena citare è senza dubbio The Sandbox il quale è basato su Ethereum, e allo stesso modo l'economia interna si basa sui non fungible token. Servono infatti a comprare e possedere terreni (chiamati LAND come in Decentraland), così come altri oggetti di personalizzazione (dagli accessori alle skin per il proprio avatar). Il token utilizzato per la compravendita in questo caso è SAND.

- La prima fra le differenze tra Decentraland e The Sandbox è l'obiettivo dei metaversi. Nel primo caso abbiamo un "metaverso sociale" pensato per far interagire le persone come nel mondo offline, ma accorciando i limiti geografici. È il metaverso giusto per ospitare eventi ispirati a quelli IRL (in real life) come mostre o sfilate di moda. The Sandbox invece punta tutto sul gaming e il play-to-earn. Sia proponendo dei videogiochi che spronando gli utenti a creare i propri.

- Decentraland è stato il primo a sviluppare un mondo virtuale come prodotto principale creando un metaverso blockchain 3D, ed è stato anche il primo a rendere pubblico un proof of concept funzionante. Al contrario, Sandbox esegue ancora una versione Alpha.

- Sandbox ha un'offerta immobiliare maggiore rispetto a Decentraland,

con oltre 150.000 appezzamenti che gli utenti possono raggruppare in proprietà. Più precisamente in The Sandbox ci sono 166.464 LAND, mentre in Decentraland sono circa 90 mila.

- La maggior parte degli utenti trova più facile accedere a Sandbox poiché offre più opzioni per interagire con la piattaforma.
  Ad esempio, puoi accedere a The Sandbox collegandoti tramite il tuo wallet Metamask, e-mail o account di social media. Decentraland, d'altra parte, consente l'accesso solo collegando un wallet.

- Per quanto riguarda la grafica, Decentraland ha uno stile realistico simile a videogiochi come The Sims. Mentre The Sandbox propone lo stile della pixel art, anche se a colpo d'occhio può sembrare "spigolosa" l'esperienza di gioco è estremamente immersiva.

Nonostante le differenze tra Decentraland e The Sandbox, entrare nei due metaversi crypto su Ethereum è ugualmente semplice.

7 Pro e Contro

7.1 Pro

- Un metodo differente per comprare, creare o vendere proprietà, in questo caso di natura digitale.

- Maggiore interazione sociale. La possibilità di socializzare in un mondo virtuale può aiutare a costruire e mantenere relazioni con altri personaggi. Inoltre, la ricerca ha dimostrato che l'interazione sociale in un metaverso può portare a maggiori sentimenti di benessere e soddisfazione (Wang et al., 2012).

- Un altro potenziale vantaggio dei metaversi è che possono fornire esperienze di apprendimento avanzate, come ad esempio la partecipazione all'interno di giochi ed eventi creati dagli utenti stessi.

- Un altro vantaggio è che come metaverso può fornire maggiori opportunità di creatività ed espressione personale. Ad esempio, gli utenti possono creare i propri avatar, che sono rappresentazioni digitali di se stessi, e progettare i propri ambienti virtuali.

7.2 Contro

- Gli item di cui si è in possesso non sono "tangibili" ed hanno una commerciabilità limitata.
- La distribuzione di contenuti attraverso una rete P2P presenta due problemi principali:
  - la velocità di download: il recupero di un file da un sistema di archiviazione distribuita DHT o peer-to-peer è tradizionalmente troppo lento. In particolare, in un'applicazione grafica come Decentraland, gli utenti saranno contrari all'uso di un sistema che non carica l'esperienza in modo rapido;
  - la disponibilità: garantire che i contenuti siano sufficientemente distribuiti nella rete senza perdite. Tuttavia, IPFS e l'imminente protocollo FileCoin stanno affrontando questi problemi.

8 Esplorando il metaverso

C'è un intero mondo digitale di opportunità da scoprire all'interno di Decentraland. Nel metaverso basato sulla proprietà di LAND ci sono molti luoghi da esplorare.
Per entrare nei territori di Decentraland basterebbe un'email, ma l'esperienza sarebbe limitata. Per entrare in modo più immerso nell'universo Decentraland si può usare un crypto wallet come Metamask. Dopo aver creato il proprio avatar e aver scelto il tipo di conformazione fisica, l'abbigliamento e gli accessori, si viene proiettati nella piazza principale, chiamata Genesis Plaza. Intorno i grandi pilastri mostrano le attività che si possono fare.
In qualsiasi momento premendo il tasto X (explore),si può scegliere un'altra destinazione.
Il metaverso Decentraland è diviso in distretti, aree virtuali che condividono un tema comune. In particolare, possiamo vedere tre tipi di distretto: i *quartieri pubblici*, aperti a tutti gli utenti e destinati all'uso generale e all'esplorazione; i *Distretti privati*, sono di proprietà di singoli utenti o organizzazioni e accessibili solo a coloro a cui è stata concessa l'autorizzazione dal proprietario; ed infine *distretti sponsorizzati*, che sono creati e gestiti da sponsor, generalmente aziende o organizzazioni che utilizzano Decentraland

come piattaforma per il marketing o la promozione del marchio. Ogni distretto ha il proprio insieme di regole e regolamenti, stabiliti dal proprietario o dallo sponsor del distretto. Inoltre, la principale differenza tra i tre tipi di distretti si basa sul livello di accesso e controllo dato agli utenti e sullo scopo del distretto.

L'area Aetheria (cyberpunk) è la più grande, con 8.008 pezzi LAND, ma anche 6.776 di Vegas City e 6.485 di Dragon City sono impressionanti. Ci sono aree nel sistema per tutti. E l'obiettivo di un luogo può spaziare dall'avventura allo yoga e oltre.
Come la vita stessa, sta all'utente determinare cosa vuole dal mondo,
nell'universo Decentraland è anche possibile semplicemente socializzare, incontrando altre persone. Si può incontrare persone che la pensano allo stesso modo mentre ci si gode la vita notturna dei club o persino delle taverne.
Chi ha un'inclinazione più artistica amerà parlare di arte nel quartiere dei musei. Continuando ad esplorare si può entrare in distretti dedicati a gallerie d'arte vitrtuali dove sono esposte alcune opere di noti cripto artisti che si possono acquistare.
Decentraland ha la possibilià di utilizzare il marketplace OpenSEA.

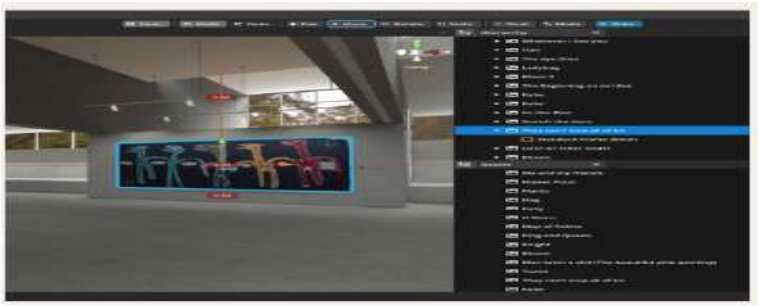


Figure 12: Galleria d'arte virtuale.

8.1 OpenSea: Museo di NFT

OpenSEA è il marketplace per NFT fondato nel dicembre 2017 da Devin Finzer e Alex Atallah, ispirati dai CryptoKitties. Questi ultimi sono stati introdotti nel 2017 quando nacque una DApp sulla blockchain di Ethereum,

un gioco basato sull'allevamento di gattini sotto forma di NFT. La proprietà verificabile degli NFT, creati "accoppiando" i gattini, ha aperto alla possibilità di monetizzare l'impegno dei giocatori. Questi gattini, infatti, potevano essere venduti in cambio di criptovalute.
I fondatori presentano le potenzialità della tecnologia blockchain come motivazioni che li hanno spinti alla creazione della piattaforma. Nella loro opinione, gli NFT costituiscono un tassello fondamentale in una nuova forma di economia, decentralizzata e basata sulla proprietà dei contenuti digitali, così da restituire libertà e potere agli utenti. Acquistare e vendere su Internet è ormai esperienza comune, e Opensea funziona come qualsiasi e-commerce, con l'unica differenza che i token non fungibili possono essere coniati (mintati) sulla piattaforma stessa, impossibile per i beni fisici. I valori principali che OpenSEA mira a garantire sono:

1. Fiducia e sicurezza: Opensea si impegna nel proteggere creatori e collezionisti di NFT, così da conservare un clima di fiducia. L'esperienza è supportata da strumenti, linee guida e servizi di assistenza, così da introdurre qualsiasi tipo di utente al nuovo mondo della blockchain.

2. Inclusività e accessibilità: su Opensea chiunque può diventare un autore di NFT, non ci sono barriere all'entrata.

3. Ampiezza e varietà: è il marketplace per NFT più popolare, offrendo il catalogo più vario e ricco in assoluto. Gli utenti possono navigare tra migliaia di progetti crypto, un'offerta talmente ampia da giustificare il nome di "mare aperto".

Questi principi, affiancati all'innovazione, hanno condotto Opensea alla valutazione di oltre 13 miliardi di dollari nel 2022.
All'interno della piattaforma gli NFT sono divisi per categoria, come collezionabili, fotografia, domini NFT ed addirittura oggetti del metaverso (come gli asset di The Sandbox).
Non è necessario essere registrati per esplorare opensea.io, ma per acquistare, vendere, creare o mettere tra i "preferiti" un NFT c'è bisogno di un account. Inoltre, non bastano un nome utente e una password, ma sarà necessario possedere un wallet crypto, essenziale per inviare, ricevere e conservare criptovalute, dunque anche per operare con gli NFT. Su openSEA si può acquistare in 3 modi:

- "Compra ora": alcuni pezzi sono in vendita ad un prezzo fissato e, come in ogni e-commerce, possono essere comprati in qualsiasi momento.
- Aste: si possono organizzare vere e proprie aste per vendere NFT, a cui chiunque può partecipare facendo un'offerta. Il venditore può accettare qualsiasi delle offerte ricevute prima della chiusura dell'asta, oppure a tempo scaduto l'NFT andrà al miglior offerente.
- Offerte: E' possibile fare offerte anche per oggetti non in vendita, presenti nelle collezioni di altri utenti su Opensea, oppure offrire una somma diversa rispetto al prezzo "compra ora" fissato dal venditore.

Che cos'è un POAP in Decentraland? Quando partecipi agli eventi Decentraland, potresti ricevere uno speciale token Proof Of Attendance Protocol (POAP). Questi token funzionano con la catena laterale Gnosis Chain Etherium. È essenzialmente simile a un biglietto nel mondo fisico, con il quale si può accedere a eventi virtuali. I token di prova di presenza sono un piccolo pezzo di storia digitale. Ogni token POAP è unico grazie alle qualità ereditate dalla blockchain. Se stai pianificando un evento, puoi creare i tuoi token POAP. Il Decentraland Foundation ha impostato un server accessibile specifico per la creazione di POAP da parte dei membri Decentraland. In Decentraland è stato creato anche il Distretto del Lusso, sviluppato da Metaverse Group, dove i marchi di moda globali hanno esposto le loro vetrine virtuali. Nei vari distretti si possono organizzare eventi, che attirano molti cittadini di DCL, eccone un esempio.

8.2 Decentraland Metaverse Fashion Week 2023

La moda è stata una delle prime industrie a riconoscere l'incredibile potenziale del Metaverso e del Web3. Questo perché il Metaverso crea opportunità per così tante aree della moda, dal design alla vendita al dettaglio. Il settore della moda e il metaverso possono unire il mondo virtuale e quello fisico.
Questo presenta enormi opportunità per marchi, designer e rivenditori di raggiungere i consumatori ovunque e in qualsiasi momento, attraverso la realtà aumentata.
Il tema della moda nel metaverso e come quest'ultima possa essere un'ulteriore opportunità di sviluppo dei mondi virtuali è stato trattato nella seconda edizione della Metaverse Fashion Week, svoltasi tra il 28 e il 31 marzo 2023.

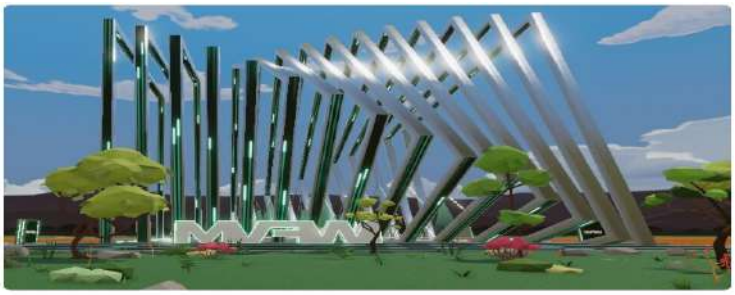


Figure 13: Distretto del Lusso.

La prima edizione, nel 2022, ha visto oltre 100mila partecipanti, 7 milioni di media impression, 460 testate giornalistiche che hanno coperto l'evento e oltre 165 mila wearable, oggetti e indumenti da indossare nel metaverso, presentati dalle case di moda. Infatti, tutte le principali case di moda stanno già investendo nella produzione 3D.
La MVFW 2023 ha inoltre dimostrato il potenziale di interoperabilità tra metaversi open source, quest'anno infatti, la MVFW si è svolta in più metaversi, in quanto oltre ai pionieri Decentraland e UNXD, il marketplace digitale del lusso, essa è stata realizzata in collaborazione con i metaversi Spatial e OVER.[14]

9 Giochi su Blockchain

9.1 Come si differenziano i Blockchain games dai giochi tradizionali?

Per quanto riguarda i giochi tradizionali le risorse sono di proprietà e controllate dallo sviluppatore del gioco, non sono trasferibili tra i giochi e la cronologia dei giocatori è difficile da tracciare. Invece, per quanto riguarda i giochi Blockchain le risorse sono di proprietà e controllate dal giocatore, possono essere scambiate tra i giochi e la cronologia dei giocatori viene registrata continuamente, consentendo agli sviluppatori di creare contenuti personalizzati.
Siccome i dati dei giocatori sono archiviati su una blockchain, risultano essere pubblici. Ciò significa che qualsiasi altro giocatore può accedere e utilizzare

tali dati. Inoltre, i giocatori possono acquistare risorse di gioco direttamente da altri giocatori anziché tramite i negozi in-game e potrebbero anche ottenere risorse di gioco da un servizio di deposito a garanzia, il che significa che gli sviluppatori di giochi non possono fare affidamento sulla costruzione di modelli di business basati sulle tariffe del mercato. Di conseguenza, non possono impedire ai giocatori di rivendere gli articoli.

9.2 I 10 migliori giochi basati su blockchain

La definizione di "top 10" di giochi è di per sè molto difficile in quanto spesso si considerano molti aspetti soggettivi. In questo caso, la classifica è stata realizzata analizzando esclusivamente il "Market Cap" di ciascun gioco. Grazie a Chainplay è stato infatti possibile ordinare in ordine decrescente i giochi in base alla loro capitalizzazione di mercato.

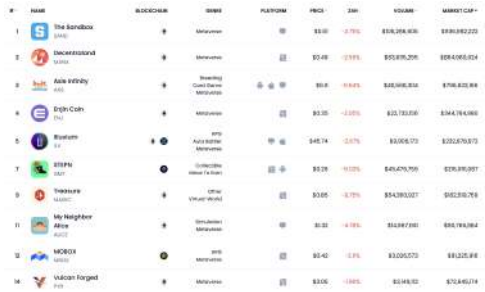


Figure 14: Classifica Top 10 Giochi ottenuta dal sito 'chainplay.gg'

Come è possibile vedere in Figura 14, al secondo posto troviamo Decentraland, ma analizziamo i restanti titoli.

9.2.1 The Sandbox

The Sandbox [13] è composto da tre elementi che uniti offrono agli utenti un'esperienza completa per la produzione di contenuti (UGC User Generated Content). Sono offerti anche ulteriori strumenti che aiutano i creatori a proteggere i loro contenuti, soggetti a diritto d'autore, attraverso blockchain e contratti intelligenti.
Gli elementi sono:

- **VoxEdit** è pacchetto semplice da utilizzare e gratuito per la creazione di NFT e modellazione 3D. I voxel sono pixel quadrati 3D simili a

blocchi di costruzione e possono essere manipolati per creare qualsiasi cosa.

- **Marketplace** consente agli utenti di caricare, pubblicare e vendere le loro creazioni. Quest'ultime vengono prima caricate in una rete IPFS per fornire uno storage decentralizzato e quindi registrate sulla blockchain per dimostrare la proprietà. Una volta fatto questo, le creazioni diventano ASSET che possono essere venduti facendo una prima offerta di vendita sul marketplace, dove i potenziali acquirenti possono acquistarli.

- **Game Maker** consente a chiunque di creare giochi 3D gratuitamente. Non è richiesto alcun codice grazie a strumenti di scripting visivi ad alto livello.

9.2.2 Axie Infinity

Axie Infinity [2] è un universo di gioco online incentrato su creature simili a Pokémon chiamate Axies. I giocatori possono collezionare Axies con la possibilità di combattere, accoppiare, collezionare, allevare e costruire regni per i propri Axies.
Ciò che differenzia Axie Infinity da altri giochi è la sinergia che ha stabilito tra il gioco online standard e la blockchain. Il gioco, basato su Ethereum, utilizza un design che consente ai giocatori di possedere i propri asset virtuali e al gioco di premiare i giocatori che riescono a raggiungere un livello avanzato di abilità.
Per iniziare, gli utenti devono completare un processo di configurazione multistep per connettere il loro wallet al proprio account Axie Infinity. Una volta fatto ciò il giocatore può interagire con il mercato digitale. Per giocare, gli utenti hanno bisogno di 3 Axies. Quando il giocatore ha 3 Axies, può scaricare l'applicazione e iniziare a giocare. Ci sono molte sfumature intorno al costo di un Axie poiché il prezzo varia in base a fattori come: la rarità, l'esperienza, gli attributi e il tipo.

9.2.3 Enjin Coin

Enjin Coin [6] è un progetto di Enjin, un'azienda che fornisce un ecosistema di prodotti di gioco basati su blockchain. L'offerta principale di Enjin è

la Enjin Network, una piattaforma di gioco sociale attraverso cui gli utenti possono creare siti web e clan, chattare e gestire negozi di oggetti virtuali.
Enjin consente agli sviluppatori di giochi di creare token per gli oggetti del gioco sulla blockchain Ethereum. Utilizza Enjin Coin, un token per supportare gli asset digitali emessi utilizzando la sua piattaforma, il che significa che gli oggetti possono essere comprati, venduti e scambiati con valore nel mondo reale. Enjin Coin è stato annunciato per la prima volta nel luglio 2017 e lanciato sulla blockchain Ethereum a giugno 2018.
Ogni asset creato con la piattaforma Enjin contiene ENJ, una risorsa di creazione che viene bloccata all'interno degli NFT e rimossa dalla circolazione.

9.2.4 Illuvium

Illuvium [9] è un gioco di battaglie fantasy open-world play-to-earn in stile Pokémon, costruito sulla blockchain Ethereum. Spesso considerato il primo gioco AAA su Ethereum, Illuvium cerca di offrire fonte di intrattenimento sia per i giocatori casual che per i fan hardcore di DeFi attraverso una serie di funzionalità di raccolta e trading.
Il mondo di Illuvium è abitato da creature note come Illuvial, che possono essere catturate dai giocatori che le sconfiggono in battaglia e le curano. Da quel momento diventano una parte fedele della collezione del giocatore e possono essere utilizzate in battaglia contro altri avventurieri come parte del gameplay di auto battler di Illuvium.
Il gioco è una fusione tra un gioco di esplorazione open-world e un gioco di battaglie PVP. I giocatori possono trascorrere il loro tempo esplorando le vastità del mondo di gioco o costruendo il loro team di potenti bestie.
Illuvium è in fase di sviluppo dal 2020 ed è stato creato da un team globale di oltre 40 persone. Il token ILV ha diverse utilità all'interno dell'ecosistema di Illuvium. È il token principale utilizzato per ricompensare i giocatori per i loro successi in-game, garantisce ai giocatori la loro quota della Illuvium Vault e viene utilizzato per partecipare alla governance del gioco tramite l'organizzazione autonoma decentralizzata (DAO) di Illuvium.

9.2.5 STEPN

Stepn [12] è il primo gioco di token non fungibili, basato sulla blockchain Solana, che sta rivoluzionando il concetto di guadagno attraverso l'attività

fisica. È un'app lifestyle che combina l'AR con la tokenizzazione di attività quotidiane come l'esercizio fisico. Gli utenti possono guadagnare criptovalute camminando, correndo o facendo jogging con le sneakers NFT, essenzialmente un paio di sneakers virtuali che determinano quanto tempo ci si può allenare e quanto si può guadagnare. Lo scopo di Stepn è motivare le persone a muoversi ed esercitarsi premiandole.
Non solo i giocatori possono guadagnare token mentre si esercitano, ma possono raccogliere scrigni del tesoro durante le loro sessioni.

9.2.6 Treasure

Treasure [15] è un ecosistema governato dalla community che funge da ponte tra diversi giochi, diventando una "console" di gioco decentralizzata. Questo concetto è riflesso nel nome della sua piattaforma principale, Bridgeworld. Come suggerisce il nome, essa funge da ponte tra mondi virtuali o giochi.
La piattaforma Treasure mira a fornire alle comunità un supporto completo per costruire e sviluppare i propri giochi.
Le leggende o trame di ciascun nuovo gioco vengono integrate sotto l'ombrello di Treasure. Questi giochi condividono alcune risorse simili, tra cui MAGIC, la valuta nativa della piattaforma.
L'altra piattaforma principale di Treasure, Smolverse, ha lanciato Smol Brains, un gruppo di popolari NFT in evoluzione. Combinati con gli NFT di Bridgeworld e elencati sul mercato di Treasure, Trove, i due progetti hanno guidato il 10% del volume totale su OpenSea all'inizio del 2022. OpenSea è attualmente il più grande mercato digitale al mondo per gli NFT.

9.2.7 My Neighbor Alice

My Neighbor Alice [11] è un gioco di costruzione multiplayer in cui chiunque può acquistare e possedere isole virtuali, collezionare e costruire oggetti e incontrare nuovi amici. Unisce il meglio dei due mondi: una trama divertente per i giocatori occasionali e un ecosistema per i giocatori che desiderano collezionare e scambiare NFT.
Ogni giocatore è rappresentato da un avatar, che è possibile modificare installando diversi elementi. Nel gioco, si possono acquistare appezzamenti di terreno virtuali da Alice o dal marketplace. L'offerta di terreni nell'universo è limitata e ogni pezzo di terra è rappresentato sotto forma di token NFT. Ci sono elementi di gioco che possono essere inseriti nel gioco e che possono

essere acquistati sul marketplace, come: case, animali, verdure, decorazioni o oggetti cosmetici per l'avatar.
Il token Alice è la valuta principale del gioco e consente ai giocatori di effettuare tutte le operazioni necessarie.

9.2.8 Mobox

Mobox [10] è una piattaforma di gioco basata su blockchain decentralizzata che utilizza il modello play-to-earn (P2E) e opera sulla Binance Smart Chain (BSC). La piattaforma di gioco crittografico Mobox offre tre diversi tipi di gioco, insieme a token non fungibili (NFT) e caratteristiche di finanza decentralizzata (DeFi). Il token MOBOX nativo è essenziale per l'acquisto, la vendita e il trading della gamma di NFT "MOMO" di Mobox e per partecipare al mining di MOMO. Inoltre, il token MOBOX sblocca funzionalità bonus e consente ai giocatori di acquistare attrezzature di alto livello e asset in-game.
Oltre a cio l'ecosistema di gioco, essendo play-to-earn, premia i giocatori per la loro partecipazione e abilità. Con il farming, la creazione di NFT, diversi flussi di reddito e opzioni di gioco, Mobox è uno dei progetti di gioco crittografico di maggior successo nell'ecosistema della Binance Smart Chain (BSC).

9.2.9 Vulcan Forged

Progettato come un ecosistema facile da giocare e da costruire, Vulcan Forged [16] è un progetto che promuove lo sviluppo di giochi blockchain supportando gli sviluppatori attraverso i suoi programmi di incubazione e crowdfunding. Vulcan Forged è un punto di riferimento per gli appassionati di giochi blockchain dove possono accedere a giochi popolari e a un vasto mercato NFT per comprare e vendere asset digitali in-game. L'intero ecosistema è alimentato dal suo token di utilità, staking e pagamento PYR.
Il PYR, compatibile con ERC20 e Matic/Polygon, è una valuta cross-platform che può essere utilizzata nei giochi che fanno parte dell'ecosistema di Vulcan Forged. L'azienda ha anche lanciato il suo scambio decentralizzato chiamato VulcanDex. Gli NFT possono esistere su più blockchain. Attualmente, la principale catena utilizzata è Vechain.
Vulcan Forged si vanta di rimuovere il gas e la crittografia per gli sviluppatori di giochi che utilizzano la loro piattaforma e offre supporto a qualsiasi

terza parte con una semplice idea per trasformarla in realtà. I membri della comunità hanno creato i loro giochi con il supporto di base, tra cui Coddle Pets, Block Babies e GeoCats. Ad oggi, molti altri progetti di gioco hanno iniziato a utilizzare l'ecosistema di Vulcan Forged.

10 Il futuro di Decentraland

Nel 2022 Decentraland si è concentrato sulla crescita e il miglioramento della piattaforma, con l'obiettivo di mantenere un protocollo aperto e un bene pubblico. Sono state aggiunte molte funzionalità, è stata rilasciata una versione per desktop, sono stati organizzati nuovi eventi a livello di piattaforma, attirando molti nuovi cittadini di DCL, e la comunità è stata ulteriormente responsabilizzata a contribuire e rivendicare la proprietà di Decentraland, in particolare con tutti i cambiamenti nella piattaforma di governo DAO.
L'obiettivo principale dichiarato nel "Manifesto di Decentraland per il 2023" consiste nella crescita della comunità di creatori di Decentraland, rendendo la creazione in DCL più accessibile a tutti e fornendo ai creatori migliori strumenti per aiutarli a liberare la loro creatività in Decentraland. Tanto che, il 2023 è denominato "Year of the Creators". [3]
I creatori della comunità DCL sono parte integrante dell'ecosistema di Decentraland; essi sono descritti come gli artisti che conferiscono a un mondo virtuale basato sul codice il suo colore e la sua forma. I creators infatti creano l'atmosfera del mondo,i suoni, le esperienze da vivere, i vestiti virtuali che indossano gli avatar, gli Emotes, ovvero le animazioni degli avatar che li rendono espressione degli utenti e molto altro ancora. In definitiva, i creatori sono coloro che danno vita a Decentraland.
Un creatore può essere chiunque si coinvolga, contribuisca, partecipi, crei, costruisca o implementi. Dall'organizzazione di eventi, alla progettazione di vestiti virtuali e Emotes, alla costruzione con l'SDK (software development kit) o al contributo al codice di DCL, tutto quel lavoro è svolto dai creatori.
Decentraland è una piattaforma per l'espressione creativa dei propri utenti e per questo motivo punta a migliorare e facilitare l'esperienza ai creators, attraverso nuove funzionalità, come per esempio l'introduzione di scenari che attivano le animazioni degli avatar oppure "smart wearables", ovvero vestiti dotati di codice che permettono all'utente di vedere nuovi contenuti, e fornendo strumenti e risorse accessibili che possono essere utilizzati per creare tutto ciò che si immagina in Decentraland.

Come fanno esattamente i creators a creare nuovi contenuti per e in Decentraland? La risposta più significativa è una discussione a sé stante. Ma la risposta breve può essere ristretta ai due strumenti di creazione più cruciali: The Builder e SDK.

Figure 15: Decentraland SDK.

Il Builder è uno strumento online progettato per aiutare a creare e pubblicare scene Decentraland. Una delle cose migliori dello strumento è che non è nemmeno necessario installarlo poiché The Builder è un'app Web. È progettato per essere facile da configurare, utilizzare e padroneggiare. Esso fornisce agli utenti una vasta libreria di modelli predefiniti e contenuti su cui basarsi, ed è implementato all'interno di un'interfaccia facile da usare.
The Decentraland SDK porta la funzionalità di The Builder al livello successivo. Per questo strumento è necessaria una certa esperienza di programmazione: i programmatori possono importare modelli, scrivere programmi e persino creare giochi che possono esistere nel più ampio universo Decentraland. Naturalmente, non tutti i programmatori sono esperti nella modellazione 3D: troveranno suggerimenti nella documentazione per utilizzare modelli prefabbricati. Inoltre, i documenti contengono informazioni sufficienti per iniziare a imparare la modellazione 3D.
In conclusione, si può affermare che Decentraland sia diventato rapidamente un gioco di successo con un futuro roseo con molte opportunità di crescita, dovute a diversi fattori come la collaborazione con diversi marchi e aziende importanti, la possibilità di sviluppare applicazioni innovative grazie al suo linguaggio di scripting e alla flessibilità della piattaforma e la continua evoluzione tecnologica che punta ad avere: questi aspetti stanno portando ad un'espansione della comunità, la quale potrebbe favorire una sempre maggiore diversità di contenuti e interazioni, oltre alla crescita dell'economia

virtuale basata sulla creazione e lo scambio di asset digitali.
Naturalmente, il futuro di qualsiasi progetto dipende da molti fattori, tra cui l'adozione da parte degli utenti, la concorrenza sul mercato e l'evoluzione delle tecnologie. Tuttavia, con il suo concetto innovativo e una solida base di utenti e sviluppatori, Decentraland sembra avere un potenziale significativo per prosperare come una delle principali piattaforme di realtà virtuale basate su blockchain.

Bibliografia

[1] In: *www.coinmarket.com* (2023).

[2] "Axie Infinity Whitepaper". In: *https://whitepaper.axieinfinity.com/* (2023).

[3] "Decentraland 2023 Manifesto: Year of the Creators". In: *www.Decentraland.org* (2023).

[4] "Decentraland docs". In: *www.Decentraland.org* (2023).

[5] "Decentraland: white paper". In: *www.Decentraland.org* (2023).

[6] "Enjin Coin Whitepaper". In: *https://enjin.io/whitepaper* (2023).

[7] "Esteban Ordano e Ari Meilich: all'origine di Decentraland". In: *https://academy.youngplatform.com/* (2023).

[8] "Genesis.City: A Dynamic Bird's-eye View of Decentraland". In: *www.Decentraland.org* (2023).

[9] "Illuvium Whitepaper". In: *https://www.docs.illuvium.io/* (2023).

[10] "Mobox Whitepaper". In: *https://faqen.mobox.io/* (2023).

[11] "My Neighbor Alice Whitepaper". In: *https://www.myneighboralice.com/s/My-Neighbor-Alice-Whitepaper-final.pdf* (2023).

[12] "Stepn Whitepaper". In: *https://whitepaper.stepn.com/* (2023).

[13] "The Sandbox Whitepaper". In: *https://www.sandbox.game/en/about/* (2023).

[14] "Tradition and Innovation Collide: Decentraland Meta- verse Fashion Week 2023". In: *www.Decentraland.org* (2023).

[15] "Treasure Whitepaper". In: *https://docs.treasure.lol/about-treasure/readme* (2023).

[16] "Vulcan Forged Whitepaper". In: *https://docs.vulcanforged.com/* (2023).

CBDC

UN'INNOVAZIONE NEI PAGAMENTI DIGITALI

Enrico Bonsignorio, Daniele Di Marco, Ilaria Palumbo, Rachele Pierri

POLITECNICO DI TORINO

Corso di Laurea Magistrale in Ingegneria Matematica

Blockchain e criptoeconomia

CBDC:
un'innovazione nei pagamenti digitali

Prof. Danilo Bazzanella

Prof. Andrea Gangemi

Enrico Bonsignorio s295507

Daniele Di Marco s296623

Ilaria Palumbo s302642

Rachele Pierri s305728

Anno accademico 2022/2023

Indice

Introduzione 1

1 Caratterizzazione delle CBDC 3
1.1 Definizione e caratteristiche di CBDC 3
1.2 Tipologie di CBDC 5
1.2.1 Classificazione in base al grado di accessibilità 5
1.2.2 Classificazione in base alla gestione delle transazioni 6
1.2.3 Classificazione in base all'architettura 7
1.3 Obiettivi delle CBDC 8

2 Le motivazioni delle banche centrali per l'emissione di una CBDC 10
2.1 I sistemi di pagamento 10
2.2 Il ruolo delle banche centrali 11
2.2.1 Un possibile scenario: CBDC come valuta per i depositi pubblici presso le banche centrali 12

3 Vantaggi e svantaggi delle CBDC rispetto alle valute tradizionali e alle criptomonete 14
3.1 Le criptomonete e le valute tradizionali 14
3.2 Vantaggi e svantaggi rispetto alle valute tradizionali 15
3.2.1 Vantaggi e svantaggi rispetto alle criptomonete 16
3.3 Impatto ambientale delle CBDC 17

4 L'esperienza di alcuni paesi nel lancio di una CBDC: Cina e Europa 19
4.1 Il caso Cina 19
4.1.1 Caratteristiche chiave dell' e-CNY 20
4.2 In Europa 23
4.2.1 Ragioni per l'emissione 23
4.2.2 Potenziali effetti di un euro digitale 24
4.2.3 Considerazioni legali e design tecnologico 25
4.2.4 Lavori futuri 25

Conclusioni 27

Bibliografia 29

Introduzione

Il concetto di denaro, negli ultimi anni, sta subendo una trasformazione significativa e le valute digitali stanno emergendo come una possibile evoluzione delle forme di pagamento tradizionali. L'avvento delle criptomonete ha infatti aperto la strada a nuove forme di pagamento digitali, con tutte le loro potenzialità e limitazioni.

Tra queste, le Central Bank Digital Currency (d'ora in poi chiamate come CBDC) potrebbero rappresentare un ulteriore passo avanti nella digitalizzazione delle transazioni finanziarie.

In questo elaborato verrà quindi presentato il concetto di denaro elettronico con le proprietà che lo contraddistinguono. Inizialmente si definisce la nozione di CBDC specificandone le caratteristiche e descrivendo le diverse tipologie. Verranno infatti analizzate tre classificazioni distinte tra loro e come queste possono essere combinate insieme. Al termine di questo capitolo si identificano i principali obiettivi delle CBDC.

Nel secondo capitolo vengono presentate le motivazioni che hanno spinto le banche centrali ad avvicinarsi al mondo delle valute digitali. L'utilizzo delle CBDC potrebbe contribuire al miglioramento dei sistemi di pagamento attuali, ridefinendo il ruolo delle banche centrali in questo nuovo contesto.

Invece, nel capitolo successivo, viene presentata una panoramica generale dei vantaggi e svantaggi delle CBDC rispetto alle monete fiat ora vigenti e alle attuali criptomonete. Si evince come le CBDC si inseriscano in una posizione intermedia tra di esse, a causa del fatto che non si deduce mai uno sbilanciamento tra i pro e contro presentati. Il capitolo si conclude con una presentazione dei possibili vantaggi ambientali che l'emissione di una CBDC potrebbe apportare.

Infine, verranno analizzati i casi reali della Banca Centrale Cinese e dell'Europa. La Cina è stata la prima grande potenza economica mondiale ad emettere sul mercato una valuta digitale, la quale verrà presentata studiandone l'architettura,

analizzando il ruolo dello Stato nella sua emissione e le conseguenze a livello internazionale. Per quanto riguarda l'Europa, gli studi attuali risultano essere ancora in una fase embrionale e dunque verranno esposte solo alcune possibilità prese in considerazione dalla BCE.

Capitolo 1

Caratterizzazione delle CBDC

1.1 Definizione e caratteristiche di CBDC

Le CBDC rappresentano una forma di valuta digitale emessa dalle banche centrali dei paesi, con l'obiettivo di trasformare il modo in cui le persone scambiano valore e conducono le loro transazioni finanziarie.

Viene quindi introdotta l'idea di una nuova forma digitale di denaro rilasciata e controllata dalle banche centrali.

Avendo dato la definizione formale di CBDC, possiamo delinearne le caratteristiche:

1. **Accessibilità**: Le CBDC sono progettate per essere accessibili a tutti, garantendo l'uguaglianza di accesso ai servizi finanziari digitali. Ciò implica che le

CBDC dovrebbero essere utilizzabili tramite strumenti di pagamento digitali come portafogli elettronici o carte di pagamento;

2. **Efficienza**: Questa caratteristica è strettamente legata alla convenienza del sistema di pagamento e alla somiglianza con i pagamenti in contanti. La decisione prioritaria è quindi delineare i ruoli della Banca Centrale e degli altri intermediari finanziari coinvolti;

3. **Anonimato e sicurezza**: Verrebbe garantita trasparenza sull'ammontare delle transazioni, assicurando comunque che le transazioni siano sicure e che le informazioni personali siano adeguatamente protette. La CBDC avrà comunque l'autorità per poter approfondire ogni transazione ritenuta sospetta;

4. **Flessibilità e scalabilità**: Le CBDC dovrebbero essere progettate in modo flessibile e scalabile per adattarsi alle esigenze e alle evoluzioni del sistema finanziario;

5. **Resilienza**: La solidità delle operazioni di rete è una dimensione chiave che deve essere presa in considerazione. Bisogna decidere se basare la CBDC su infrastrutture bancarie tradizionali o su Distributed Ledger Technology (DLT). Tale scelta influenza profondamente la struttura e la gestione della governance dell'infrastruttura, che può essere centralizzata o decentralizzata;

6. **Interoperabilità**: Tale dimensione deve essere valutata al fine di garantire la possibilità di interazione tra diversi sistemi di pagamento e infrastrutture finanziarie esistenti, facilitando l'integrazione delle CBDC.

1.2 Tipologie di CBDC

Possiamo suddividere le tipologie di CBDC in base a diverse caratteristiche.

1.2.1 Classificazione in base al grado di accessibilità

Le CBDC possono espandere le funzionalità della valuta esistente, rendendo più efficienti i pagamenti e fungendo da sostituto digitale del denaro. Il grado in cui CBDC può effettivamente offrire questi vantaggi dipenderà dal suo design.

Valutando quindi il grado di accessibilità, le tipologie di CBDC sono:

- **CBDC retail** (al dettaglio): Si tratta di una forma di CBDC accessibile direttamente al pubblico. Tra la tante opzioni di pagamento già in uso per le transazioni quotidiane (pagamento in contanti, credito, addebito, ecc.), le CBDC offrirebbero una nuova scelta per le transazioni digitali, i pagamenti istantanei peer-to-peer e le transazioni fisiche. Potrebbero potenzialmente ridurre i costi e diversificare i canali di pagamento;
- **CBDC wholesale** (all'ingrosso): Sono riservate alle istituzioni finanziarie, come le banche commerciali e le istituzioni finanziarie non bancarie. I pagamenti all'ingrosso si basano sui sistemi di pagamento nazionali e le transazioni sono generalmente condotte tramite compensazione interbancaria utilizzando la valuta della banca centrale. Il concetto di CBDC potrebbe facilitare un accesso più ampio e diversificato delle istituzioni a pagamenti di alto valore e potrebbe favorire la nascita di una nuova infrastruttura finanziaria all'ingrosso;
- **CBDC cross-border**: Le CBDC potrebbero stabilire relazioni monetarie più dirette a livello internazionale, ridurre i rischi, migliorare le inefficienze, rafforzando al contempo la concorrenza nei conti internazionali e favorendo l'integrazione e l'inclusività dei mercati finanziari.

Figura 1.1: CBDC retail e wholesale.

1.2.2 Classificazione in base alla gestione delle transazioni

L'accessibilità alla CBDC è una delle caratteristiche chiave di una valuta virtuale. Le differenze principali risiedono nella struttura dei dati e nel processo di autenticazione e trasferimento di fondi.

Ci possono essere due modi diversi in cui un consumatore può accedere ai suoi token digitali:

- **Modello account-based**: La proprietà è collegata a un'identità, quindi chiunque può verificare il proprietario dell'account. Questo schema presuppone che ogni utente abbia un conto identificato da una chiave univoca associata alla sua identità, come negli odierni conti bancari. Per effettuare una transazione si deve dimostrare la propria identità e quando si verifica una transazione o un trasferimento di fondi, il record viene aggiornato aumentando o diminuendo la posizione del conto nel database.
- **Modello token-based**: La proprietà è collegata a una prova che si ottiene attraverso l'uso di una PKI (Public Key Cryptography Infrastructure). Semplicemente con una firma digitale, un individuo è in grado di dimostrare il possesso della sua CBDC. Questo modello mira a garantire un'accessibilità più ampia e meno complessa rispetto al modello basato su account, potendo anche garantire migliori funzionalità di privacy per l'utente. D'altra parte, può presentare dei problemi, soprattutto legati alla gestione delle chiavi crittografiche da parte degli utenti. Infatti, nel caso di una soluzione non detentiva (dove l'utente è l'unico responsabile della gestione delle chiavi), se l'utente perdesse le sue chiavi private, non avrebbe più accesso ai suoi fondi, senza una terza parte che possa intervenire per aiutarlo a ripristinare i fondi. Questo problema può essere limitato costruendo schemi di protezione chiave. Un'altra grossa problematica è trovare il giusto compromesso tra privacy e normativa.

Figura 1.2: Modello account-based e token-based.

1.2.3 Classificazione in base all'architettura

La definizione dell'architettura alla base delle CBDC dipende fortemente dalla scelta del ruolo operativo che deve essere assunto dalla Banca Centrale e dagli altri intermediari finanziari coinvolti.

Ciò che differenzia le possibili architetture riguarda principalmente la struttura dei sinistri e delle scritture detenute dalla Banca Centrale e le responsabilità operative degli attori della rete. Esistono tre diversi tipi di architettura:

- **Direct issuance** (emissione diretta): Questo modello è il più semplice e centralizzato, infatti è la Banca Centrale che tiene traccia di tutti i rendiconti finanziari e di tutte le transazioni al dettaglio ed emette la CBDC direttamente agli utenti finali. Viene quindi eliminata la dipendenza da intermediari, ma si presentano problemi che possono rappresentare una minaccia in termini di affidabilità, velocità ed efficienza del il sistema di pagamento. In ogni caso la Banca Centrale è l'unica istituzione che gestisce i servizi di pagamento;

Figura 1.3: CBDC diretta.

- **Two-tiered issuance** (emissione a due livelli): Questo modello è quello che meglio riflette lo stato dell'attuale sistema finanziario, dove gli intermediari privati sono parte integrante del sistema. Il grande vantaggio risiede nel fatto che tutte le operazioni di interfaccia con i consumatori al dettaglio non sono di competenza della Banca Centrale. Infatti, quest'ultima emette la CBDC a una rete di intermediari finanziari autorizzati che diventano poi responsabili della distribuzione al pubblico. La principale debolezza sta nel fatto che il modello non sarebbe in grado di risolvere gli attuali problemi di fiducia nei confronti delle istituzioni private. Per questo motivo, il modello di emissione indiretta pone problemi normativi e dovrebbe prevedere polizze assicurative nei confronti dei depositi;

- **Hybrid model** (modello ibrido): Quest'ultimo combina gli elementi chiave dei modelli precedenti. Infatti, in questo modello rimane la pretesa nei confronti della Banca Centrale, ma c'è la partecipazione delle istituzioni private a supporto dell'operatività del sistema. L'elemento chiave è che i crediti sono tenuti dalla Banca Centrale separatamente dal registro dei fornitori di servizi

Figura 1.4: CBDC indiretta o a due livelli.

di pagamento. In questo modo, se l'istituto privato dovesse fallire, il sistema garantirebbe la portabilità degli asset digitali e la Banca Centrale potrebbe gestire il trasferimento della relazione del cliente ad un fornitore che gli consenta di tornare ad operare.

Figura 1.5: CBDC ibrida.

1.3 Obiettivi delle CBDC

Le CBDC sono una risposta a fenomeni decentralizzati come criptomonete e token privati, affrontando la necessità di supervisione normativa e stabilità finanziaria promuovendo al contempo l'innovazione. Proprio per questo, sono state sviluppate con una serie di obiettivi chiave, che riflettono le sfide e le opportunità offerte dalla crescente digitalizzazione delle transazioni finanziarie.

Ovviamente, gli obiettivi delle CBDC possono variare a seconda delle politiche e delle circostanze specifiche di ogni paese, ma, in generale, esistono diversi obiettivi comuni che possono essere identificati. Ecco alcuni dei principali:

1. **Innovazione finanziaria**: Le CBDC possono favorire l'innovazione finanziaria, consentendo lo sviluppo di nuovi servizi e modelli di business basati sulla tecnologia blockchain e su smart contract. Ciò potrebbe portare a stimolare la crescita economica.

2. **Efficienza dei pagamenti**: Le CBDC sono progettate per migliorare l'efficienza dei sistemi di pagamento, consentendo transazioni più rapide, sicure e convenienti.

3. **Controllo monetario**: Le CBDC offrono alle banche centrali un maggiore controllo sulla politica monetaria. Consentono alle autorità di monitorare le transazioni finanziarie in tempo reale e di adottare misure più rapide ed efficaci per regolare l'offerta di moneta e gestire l'economia.

4. **Competizione con valute digitali private**: L'emissione di una CBDC può essere una risposta alle valute digitali private come le criptovalute, offrendo un'alternativa controllata e regolamentata che preservi la sovranità monetaria dello Stato.

Capitolo 2

Le motivazioni delle banche centrali per l'emissione di una CBDC

2.1 I sistemi di pagamento

La richiesta di pagamenti in forma digitale, in particolare nell'ambito delle vendite al dettaglio, negli ultimi anni è cresciuta in modo esponenziale.
La pandemia di COVID-19 ha accelerato la necessità di digitalizzazione, rendendo l'utilizzo del contante nella vita quotidiana sempre meno rilevante: secondo la Banque de France, solo il 28% dell'importo delle transazioni nei punti vendita viene effettuato in contanti ed il trend è in diminuzione anno dopo anno (dato relativo a Gennaio 2021).

Per sostenere questo cambiamento e migliorare l'efficienza dei sistemi di pagamento, le banche centrali stanno esplorando il potenziale di nuove tecnologie, in particolare quelle basate sulla tecnologia blockchain. Inoltre il rapido avanzamento della Cina in questo ambito ha stimolato le principali banche centrali a muoversi nella stessa direzione, per evitare una situazione di svantaggio nel contesto del mercato globale.

Più in generale, la necessità di migliorare il sistema bancario era già presente in alcuni paesi per altri motivi: i servizi bancari per molte persone sono poco accessibili a causa di limitazioni geografiche e costi elevati. Costruire un sistema totalmente digitale e accessibile tramite internet permetterebbe ad un numero notevolmente più alto di persone di beneficiare dei servizi finanziari e di partecipare

all'economia globale.

Per i suddetti motivi, le banche centrali di tutto il mondo hanno iniziato la loro esplorazione nel mondo delle valute digitali già nel 2014. La Bank of International Settlements (BIS) riferisce che nel gennaio 2021 l'86% delle banche centrali intervistate stava esplorando i casi d'uso di una CBDC. Diversi paesi hanno sperimentato, stanno attualmente implementando o stanno emettendo CBDC, tra cui l'Ecuador (2014-2018), le Bahamas (Sand Dollar nel 2019), la banca centrale dei Caraibi orientali (D-Cash nel 2020), Cina (Yuan digitale nel 2020), Venezuela (Petro-Dollaro nel 2018) e Nigeria (e-Naira nel 2021).

Mentre i casi incentrati sulla vendita al dettaglio sono stati inizialmente predominanti, le banche centrali hanno riconosciuto anche il ruolo delle CBDC all'ingrosso e l'impatto che avrebbero sull'intero sistema economico. I casi principali di CBDC all'ingrosso consistono nell'aumentare l'efficienza dei pagamenti interbancari transfrontalieri e della negoziazione e regolamentazione dei titoli interbancari, contribuendo alla stabilità nei mercati finanziari e quindi alla diminuzione dei rischi.

Uno degli scopi principali, comunicato dalle banche centrali, è infatti quello di avere un sistema che minimizzi rischi e costi, per una totale inclusione finanziaria. In particolare, insieme a banche di tutto il mondo, la BIS ha stabilito tre principi chiave richiesti da una CBDC:

- Promozione dell'innovazione e dell'efficienza;
- Sostenimento della stabilità monetaria e finanziaria;
- Coesistenza con valute fiat e criptomonete.

2.2 Il ruolo delle banche centrali

L'idea di sviluppare le CBDC ha sollevato diversi interrogativi riguardanti il ruolo delle banche centrali, l'accesso diretto alle passività bancarie da parte degli utenti e, soprattutto, come dovrebbe essere strutturata l'intermediazione bancaria in uno scenario di questo genere.

Attualmente, le banche centrali adottano un sistema di gestione dei pagamenti basato su una gerarchia che permette di gestire il grande numero di conti correnti intestati agli individui in base alla tecnologia disponibile. Questi sistemi sono stati progettati in un contesto molto diverso da quello attuale, quindi lo sviluppo tecnologico degli ultimi anni permette di pensare a metodi innovativi di gestione della moneta. Generalmente, il settore finanziario ha sempre accolto velocemente le

novità, ma a livello di gestione dei pagamenti le cose sono rimaste sempre immutate: la banca centrale funge da intermediario primo e possiede un libro mastro centralizzato, il quale tiene conto di tutte le movimentazioni che avvengono nell'economia e al quale solo pochi soggetti muniti di licenza possono accedervi.
In particolare, le top-tier banks sono quegli istituti finanziari che possono avere un conto presso una banca centrale, le lower-tier banks invece sono quelle che possono accedere al sistema centrale solo attraverso i servizi offerti da una banca top-tier. Gli individui invece non possono detenere soldi presso una banca centrale direttamente, ma devono rivolgersi ad una di queste due tipologie di banca.
Le banche centrali hanno quindi dotato le banche commerciali della funzione di gestione dei conti correnti degli individui e delle aziende, che possono accedere al sistema di pagamenti esclusivamente attraverso il deposito bancario.

In questo contesto, l'adozione delle nuove tecnologie basate sulla blockchain potrebbe permettere l'accesso diretto ai depositi presso le banche centrali a tutti i soggetti presenti nel sistema economico.

2.2.1 Un possibile scenario: CBDC come valuta per i depositi pubblici presso le banche centrali

In questo scenario le autorità centrali non avrebbero più il compito di mantenere aggiornato il libro mastro, dato che avverrebbe tutto in modo automatico attraverso un protocollo crittografato formato da nodi che operano in simbiosi tra loro fino alla validazione della transazione da parte di tutti (ovvero mediante l'utilizzo della tecnologia blockchain). I conti di regolamento presso le banche centrali saranno equiparabili a dei wallets, nei quali saranno contenute le chiavi crittografate e le CBDC detenute. Tutto questo sistema richiederà il permesso di operare alla banca centrale, in modo tale da poter riconoscere, se necessario, i soggetti coinvolti nel sistema.

Ma quali vantaggi avrebbero le banche centrali nel permettere a tutti i soggetti di detenere soldi presso i loro conti?
La prima motivazione riguarda sicuramente la possibilità di rendere l'economia il più possibile basata sull'utilizzo della moneta digitale. Un secondo vantaggio riguarda la competizione tra i soggetti interessati al trasferimento di queste monete: l'apertura del sistema verso tutti aumenterebbe la competizione perchè subentrerebbero nuovi agenti economici, oltre alle banche commerciali attualmente operanti, quindi i costi di transazione diminuirebbero portando ad un miglioramento dei servizi offerti e quindi vantaggi per i soggetti coinvolti.

Quest'apertura al pubblico potrebbe aiutare anche nella gestione delle crisi sistemiche. In particolare, l'utilizzo da parte delle banche centrali di un libro mastro distribuito comporterebbe la possibilità di accedere in ogni momento al sistema.
I sistemi attualmente utilizzati non sono accessibili in qualsiasi momento, ma soprattutto non permettono un accesso trasparente ai flussi di denaro che hanno luogo nell'economia. La possibilità di analizzare come e dove il denaro viene trasferito permetterebbe uno studio migliore e una maggiore comprensione delle cause scatenanti le crisi, quindi la possibilità di controllare il rischio sistemico.
L'utilizzo di un libro mastro distribuito permetterebbe alle banche centrali anche di competere direttamente con i soggetti privati che hanno emesso moneta elettronica fino a questo momento e che hanno adottato questo sistema di regolamento. Nonostante la banca centrale non rientri direttamente nella gestione dei pagamenti, avrebbe la possibilità di supervisionare le transazioni lasciando libertà di azione ai soggetti, evitando in ogni caso che avvengano scenari rischiosi per l'economia.

Dal punto di vista delle banche commerciali, uno scenario di questo genere causerebbe delle perdite significative. Un aumento dei depositi presso le banche centrali da parte dei consumatori si tradurrebbe in una diminuzione dei depositi presso gli istituti bancari attualmente operanti; questo calo di soldi a disposizione degli istituti di credito provocherebbe una diminuzione dimensionale del sistema bancario, quindi della possibilità per le banche di erogare prestiti ai propri clienti, diminuendo quindi il credito aggregato dell'intera economia.
Per ridurre questo impatto negativo è però possibile pensare a delle soluzioni attuabili dalle autorità creditizie. Le alternative dovrebbero andare ad aumentare la possibilità di erogazione del credito: ad esempio si potrebbero ridurre i requisiti di riserva o imporre una tassa sull'uso di CBDC.

Nonostante siano chiari i benefici a livello di controllo e di concorrenza, è necessario considerare i costi per implementare un sistema di questo genere. Le banche centrali dovranno munirsi di server abbastanza potenti per immagazzinare e gestire continuamente l'ammontare di informazioni che vengono scambiate. Il costo iniziale per la creazione di questo nuovo sistema gestionale sarà quindi elevato, in quanto dovrà essere istituita e mantenuta una struttura adatta allo scopo.

Capitolo 3

Vantaggi e svantaggi delle CBDC rispetto alle valute tradizionali e alle criptomonete

3.1 Le criptomonete e le valute tradizionali

In precedenza si è detto che le CBDC sono valute digitali emesse dalle banche centrali, che possono essere utilizzate come mezzo di pagamento e riserva di valore. Esse differiscono dalle criptomonete per il fatto che sono emesse da un'autorità centrale, e quindi non sono soggette alla volatilità dei mercati e alla manipolazione da parte di soggetti terzi. Tuttavia, le CBDC presentano anche alcuni svantaggi rispetto alle valute tradizionali, come la mancanza di anonimato delle transazioni e la possibile violazione della privacy.

In questo capitolo, si esploreranno i vantaggi e gli svantaggi delle CBDC rispetto alle valute tradizionali e alle criptomonete, analizzando i loro impatti sul sistema finanziario, sull'economia e sulla società nel suo complesso. In particolare, si porrà particolare attenzione sulla loro sicurezza, sulla loro accessibilità, sulla loro stabilità, sulla loro scalabilità e sulla loro interoperabilità.

Prima di tutto, è necessario capire, anche se già noto, cosa sono le valute tradizionali e le criptomonete.
Una criptomoneta è una moneta digitale che, a differenza delle monete tradizionali, non esiste in forma fisica e non è controllata né gestita da alcuna autorità

centrale. Le informazioni sulle transazioni sono memorizzate in un registro digitale decentralizzato, basato tipicamente sulla tecnologia blockchain.
Invece, una valuta tradizionale è un mezzo di scambio accettato e riconosciuto da un governo o da una comunità, utilizzato per effettuare transazioni finanziarie e misurare il valore dei beni e dei servizi.

Dopo aver chiarito meglio di cosa si sta parlando possiamo esplorare i pro e i contro delle CBDC.

3.2 Vantaggi e svantaggi rispetto alle valute tradizionali

I vantaggi delle CBDC rispetto alle valute tradizionali sono:

- **Efficienza delle transazioni**: Le transazioni con CBDC possono essere più veloci rispetto ai metodi di pagamento tradizionali, come i bonifici bancari, poiché le CBDC possono essere trasferite istantaneamente e in modo diretto tra le parti coinvolte.
- **Riduzione dei costi**: L'utilizzo delle CBDC potrebbe ridurre i costi associati alle transazioni finanziarie, come le commissioni di elaborazione dei pagamenti e i costi delle transazioni transfrontaliere.
- **Inclusione finanziaria**: Le CBDC potrebbero favorire l'inclusione finanziaria, consentendo alle persone senza possibilità di usufruire di servizi bancari o non collegate a servizi finanziari tradizionali di accedere a strumenti di pagamento digitali sicuri e convenienti.
- **Trasparenza e sicurezza**: Le CBDC possono offrire una maggiore trasparenza e sicurezza rispetto alle valute tradizionali. Poiché le transazioni con CBDC sono registrate su una blockchain o un registro distribuito, possono essere tracciate in modo accurato, riducendo il rischio di frodi e attività illegali.

Invece, gli svantaggi delle CBDC rispetto alle valute tradizionali sono:

- **Privacy**: L'implementazione delle CBDC potrebbe sollevare preoccupazioni sulla privacy delle transazioni finanziarie. Poiché le CBDC sono digitali e tracciate, le autorità finanziarie possono potenzialmente accedere a informazioni dettagliate sulle transazioni degli individui.
- **Stabilità finanziaria**: L'introduzione delle CBDC potrebbe avere implicazioni sulla stabilità finanziaria di un paese. È importante che le politiche monetarie e fiscali siano attentamente considerate per mitigare gli eventuali rischi sistematici

- **Dipendenza tecnologica**: L'adozione delle CBDC richiede infrastrutture tecnologiche solide e sicure. Ciò potrebbe comportare una maggiore dipendenza dalle tecnologie digitali e potenzialmente escludere coloro che non hanno accesso o competenze per utilizzarle.

3.2.1 Vantaggi e svantaggi rispetto alle criptomonete

Nell'introduzione del capitolo abbiamo definito anche le criptomonete, qui di seguito vengono riportate i vantaggi delle CBDC rispetto alle altre criptomonete:

- **Supporto governativo**: Le CBDC sono emesse e supportate da una banca centrale o da un'autorità governativa, il che conferisce loro un'autorità e una stabilità istituzionale che molte criptovalute decentralizzate non hanno. Questo può aumentare la fiducia degli utenti e facilitare l'adozione delle CBDC.

- **Stabilità dei prezzi**: A differenza delle criptovalute decentralizzate, le CBDC possono essere progettate per mantenere una stabilità dei prezzi, agganciandole a una valuta tradizionale o utilizzando meccanismi di gestione della volatilità. Ciò riduce il rischio di grandi fluttuazioni di valore che possono essere associati ad altre criptovalute.

- **Regolamentazione finanziaria**: Poiché le CBDC sono emesse e regolate da un'autorità finanziaria centrale, possono essere sottoposte a norme e regolamenti finanziari esistenti, come la KYC (Know Your Customer) e la AML (Anti Money Laundering), che possono contribuire a prevenire attività illegali e frodi finanziarie.

Ed ora gli svantaggi delle CBDC, rispetto alle altre criptomonete:

- **Decentralizzazione e autonomia**: Molti sostenitori delle criptovalute apprezzano la natura decentralizzata e l'autonomia che le monete digitali offrono. Le CBDC, d'altra parte, sono ancora controllate da un'autorità centrale, il che può essere considerato come una limitazione della libertà finanziaria.

- **Innovazione tecnologica**: Le criptovalute decentralizzate, come Bitcoin ed Ethereum, hanno spinto l'innovazione tecnologica nel settore delle transazioni finanziarie e degli smart contract. Le CBDC potrebbero non essere in grado di offrire la stessa flessibilità e potenziale di sviluppo tecnologico delle criptovalute decentralizzate.

- **Privacy e anonimato**: Mentre alcune criptovalute, come Bitcoin, offrono un certo grado di anonimato nelle transazioni, le CBDC potrebbero richiedere una maggiore trasparenza e tracciabilità delle transazioni, a scapito della privacy finanziaria degli utenti.

È importante sottolineare che le caratteristiche specifiche delle CBDC possono variare a seconda del paese e delle politiche adottate, di cui mostreremo qualche esempio nel capitolo successivo.

3.3 Impatto ambientale delle CBDC

Di seguito si presenta un importante tema, l'impatto ambientale, dove le Central Bank Digital Currency (CBDC) potrebbero offrire alcuni vantaggi rispetto alle valute tradizionali e dunque, giocare un ruolo fondamentale per contribuire in positivo all'attuale situazione climatica. Ecco alcuni punti da considerare:

- **Riduzione del consumo di carta**: Le CBDC sono digitali e non richiedono l'utilizzo di carta moneta. L'eliminazione o la riduzione dell'uso di denaro fisico può contribuire a ridurre la domanda di carta moneta, il che potrebbe avere un impatto positivo sull'ambiente in termini di risparmio di risorse naturali e riduzione dell'inquinamento legato alla produzione e allo smaltimento di carta.

- **Riduzione delle emissioni di carbonio**: L'adozione delle CBDC potrebbe ridurre la necessità di trasportare e distribuire fisicamente denaro, che richiede il consumo di carburante per il trasporto e può contribuire alle emissioni di carbonio. Utilizzando le CBDC, le transazioni finanziarie possono essere gestite in modo digitale, riducendo la necessità di spostamenti fisici di valuta e, di conseguenza, le emissioni di carbonio associate.

- **Efficienza energetica**: Le CBDC possono essere gestite su infrastrutture digitali, come blockchain o registri distribuiti. Queste tecnologie possono essere progettate per essere efficienti dal punto di vista energetico, riducendo l'impatto ambientale rispetto ai processi tradizionali basati su carta o sistemi legacy. Tuttavia, è importante notare che l'efficienza energetica delle CBDC dipenderà dalla tecnologia specifica utilizzata per implementarle.

Dunque, è importante considerare che l'implementazione delle CBDC potrebbe richiedere l'utilizzo di risorse tecnologiche, come server e infrastrutture di rete, che possono a loro volta avere un impatto ambientale in termini di consumo di energia elettrica. È quindi cruciale che l'adozione delle CBDC venga bilanciata con misure per ridurre l'impatto ambientale, come l'utilizzo di fonti di energia rinnovabile e l'implementazione di tecnologie sostenibili.

In sintesi, sebbene le CBDC potrebbero offrire alcuni vantaggi in termini di impatto ambientale rispetto alle valute tradizionali, è necessario considerare attentamente l'intero ciclo di vita delle CBDC e adottare misure per garantire che la loro implementazione sia ecologicamente sostenibile.

Le CBDC sono simili alle criptomonete sotto alcuni aspetti, ma ci sono anche differenze significative. Mentre entrambe sono forme di valute digitali, le CBDC, come è stato detto in precedenza, sono emesse e regolate da una banca centrale, mentre le criptomonete come Bitcoin e Ethereum sono decentralizzate e non sono controllate da un'autorità centrale.
Ciò significa che le CBDC non soddisfano pienamente tutti i requisiti tipici delle criptomonete, come la decentralizzazione, l'anonimato delle transazioni e l'assenza di un'autorità centrale che le controlli. Comunque se non ricoprono al cento per cento la definizione di criptomoneta non è da intendere per forza come fattore negativo poiché esse sono emesse dalle banche centrali con l'obiettivo di integrare il sistema finanziario tradizionale con l'innovazione tecnologica, offrendo al contempo un certo grado di sicurezza, stabilità e controllo governativo.

In sostanza, le CBDC si collocano in una posizione intermedia tra le valute tradizionali e le criptomonete. Incorporano alcune delle caratteristiche delle criptomonete, come l'uso di tecnologie di registro distribuito (come la blockchain) per garantire la sicurezza delle transazioni, ma mantengono il controllo centrale delle banche centrali e la regolamentazione governativa. E' importante ribadire che le CBDC sono ancora in fase di sviluppo e sperimentazione da parte di diverse banche centrali in tutto il mondo. Attualmente, non esiste un modello standard o un'implementazione definitiva delle CBDC, ma ci sono molti studi e progetti in corso per esplorarne le possibilità e valutarne gli impatti potenziali.

Nel capitolo successivo, esploreremo più in dettaglio le caratteristiche specifiche delle CBDC già implementate o in via di sviluppo, analizzando i casi concreti della Cina e dell'Europa.

Capitolo 4

L'esperienza di alcuni paesi nel lancio di una CBDC: Cina e Europa

4.1 Il caso Cina

La Cina è stata sicuramente la prima grande economia a emettere una valuta digitale, chiamata e-CNY (o yuan digitale), che attraverso un'interfaccia di tipo "account-based" è disponibile sia ai cittadini che ai turisti.

La CBDC cinese è caratterizzata da un'architettura ibrida con due livelli che si occupano della distribuzione e della circolazione.
Nel primo livello (quello per la distribuzione), la Banca Centrale (PBOC) fornisce la moneta digitale alle istituzioni sottostanti (le sei più grandi banche e due banche digitali) chiamate anche Operatori Autorizzati o Istituzioni di secondo livello. Queste si occupano poi di far circolare la moneta digitale ai partecipanti del retail market, incluso il grande pubblico.

Le Istituzioni di secondo livello sono anche i fornitori dei portafogli digitali, perciò un utente ha bisogno di chiamare in causa loro in caso voglia aprire un e-wallet.
Altre banche e aziende formano le cosiddette "Istituzioni di livello 2.5", che forniscono agli utenti la possibilità di pagare con yuan digitali e ulteriori opportunità, ma nessun servizio di exchange.
Un'importante caratteristica dello yuan digitale è il disaccoppiamento con i conti bancari. Infatti, gli e-wallet possono essere utilizzati per sfruttare semplici funzioni senza dover aprire necessariamente un conto "tradizionale". In questo modo, anche

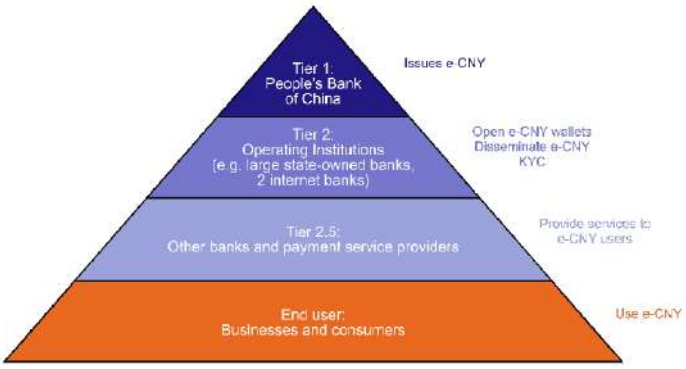


Figura 4.1: Architettura della CBDC cinese.

i turisti stranieri possono sfruttare le potenzialità della CBDC semplicemente aprendo un wallet scaricando l'applicazione.

L'anonimato è uno dei principali punti di forza della CBDC cinese. Infatti, come da accordi con la Banca Centrale Cinese, il sistema di valuta digitale "non fornisce informazioni a terzi o altre agenzie governative se non diversamente stabilito da leggi e regolamenti". La Banca Centrale conosce l'identità degli utenti, in modo da permetterne la corretta verifica nell'applicazione, ma le transazioni condotte attraverso essa trasmettono sono l'ID del wallet, senza che nessuno possa sapere l'identità della persona. Ciò significa che gli utenti saranno in grado di "nascondere" il loro identificativo rendendo più difficile alle piattaforme online la raccolta di dati.

4.1.1 Caratteristiche chiave dell' e-CNY

L'approccio cinese alle CBDC può essere compreso in termini di tre caratteristiche principali dell'e-CNY: il ruolo dello stato, il possibile uso oltre confine della moneta e gli sforzi proattivi della Cina nello studio internazionale delle CBDC.

Il ruolo dello stato

L'e-CNY è un'iniziativa portata avanti dallo stato, indicata nel 14-esimo piano quinquiennale cinese, ed è considerata come parte centrale di una riforma finanziaria. Il governo è proattivo riguardo le potenzialità della CBDC, così come i governi locali che stanno concedendo finanziamenti ai residenti per provare l'e-CNY. Il concetto legale di moneta si basa sul potere dello Stato di regolare il sistema monetario e la CBDC riguarda il "rapporto fondamentale tra denaro, Stato e diritto".

L'approccio della Cina alle CBDC può essere visto come la faccia di una medaglia che ha le criptovalute sull'altro lato. Esse infatti operano fuori dalla giurisdizione dello stato e mirano alla decentralizzazione del potere che tipicamente gli spetta. Di conseguenza, la Cina non permette lo sviluppo parallelo di criptovalute decentralizzate e della CBDC.

Nel 2020, la Banca Centrale cinese propose di confermare il corso legale dell'e-CNY e contemporaneamente vietò e impose multe per la produzione, circolazione e vendita di valute sostitutive in forma digitale e fisica. Più recentemente inoltre, la Cina ha vietato tutte le attività riguardanti le valute digitali private attraverso un avviso emesso da dieci agenzie tra cui la Corte Suprema del Popolo.

L'e-CNY è gestito secondo un modello centralizzato ma è considerato addirittura "ipercentralizzato". Secondo un governatore della PBOC, la gestione centrale dell'e-CNY è significativa per diversi motivi:

1. Mantenere il ruolo della valuta fiat e l'autorità di emettere valuta;
2. Migliorare l'efficienza dei sistemi di pagamento e migliorare la trasmissione della politica monetaria;
3. Garantire la stabilità finanziaria (ad esempio attraverso l'uso di big data e intelligenza artificiale per inibire le attività illecite).

La CBDC rafforzerebbe il ruolo dello stato, che include le agenzie collegate (ad esempio, le autorità fiscali) e fornirebbe alla Banca Centrale uno stretto controllo centralizzato sulla moneta digitale. In primo luogo, la PBOC è al centro del funzionamento del sistema e-CNY, inclusa la cura dell'emissione e dello smaltimento di CBDC. Inoltre, l'uso dell'e-CNY richiede il download dell'app della PBOC.
In secondo luogo, la PBOC svolge un ruolo di primo piano nella regolamentazione e nella definizione di regole e standard relativi alla CBDC. La PBOC supervisiona anche lo scambio e la circolazione della moneta (inclusa la regolamentazione antiriciclaggio) e regola gli operatori autorizzati e altre istituzioni commerciali, oltre ad essere responsabile della definizione delle regole per i portafogli e-CNY e della gestione del loro ecosistema.

Il possibile uso oltre confine

La PBOC ha enfatizzato l'importanza di esplorare i possibili pagamenti oltre confine attraverso la CBDC. Ad esempio, l'imminente programma pilota di Hong Kong per l'uso dell'e-CNY comporterà l'utilizzo in alcuni contesti come lo shopping e la ristorazione per alcuni singoli utenti di Hong Kong e per i cittadini che vivono nella Greater Bay Area.

La Banca Centrale è anche coinvolta nel progetto Multiple CBDC Bridge, un progetto di "co-creazione" (sviluppato con Hong Kong, Thailandia e Emirati Arabi Uniti) di una CBDC wholesale che esplora le capacità della DLT e si concentra sui pagamenti transfrontalieri in più valute.
Il miglioramento dei pagamenti internazionali è uno dei principali obiettivi della CBDC cinese. La PBOC crede che essa sia tecnicamente pronta per un utilizzo oltre confine e le banche ne stanno cominciando a sperimentare l'uso attraverso programmi pilota.

La Cina, per esplorarne le potenzialità, sta utilizzando tecnologie esistenti e nuove. In particolare, i suoi sforzi si concentrano spesso sulla finanza, la tecnologia e lo sviluppo delle infrastrutture. In relazione alla finanza, la Cina si impegna con i sistemi finanziari esistenti, tra cui SWIFT, il sistema globale di messaggistica finanziaria.
Per quanto riguarda la tecnologia, tra i nuovi meccanismi studiati, spicca la Blockchain. Il PBOC Digital Currency Institute (DCI) sta sviluppando una piattaforma blockchain per la finanza commerciale e anche l'iniziativa promossa dal governo, la Blockchain Service Network (BSN) potrebbe aiutare a promuovere la CBDC.

Proattività nello studio internazionale della CBDC

La Cina sembra svolgere un ruolo attivo nella formulazione di standard emergenti relativi al CBDC in varie sedi e organizzazioni. Ad esempio, il governo cinese ha chiesto al G20 di affrontare lo sviluppo degli standard e dei principi CBDC affrontando al contempo i vari rischi e le sfide. Di conseguenza, la Cina è rappresentata nel Future of Payments Working Group, che deriva dalla tabella di marcia del G20 per migliorare i pagamenti transfrontalieri, con la PBOC che partecipa attivamente allo sviluppo di standard internazionali.
Inoltre, all'International Telecommunication Union (ITU), la Cina guida la ricerca e la standardizzazione dell'ecosistema CBDC e dell'architettura di riferimento.

In aggiunta, la Cina propone diversi principi internazionali per la progettazione di CBDC, affrontando varie questioni tra cui l'uso internazionale di CBDC e il monitoraggio e la condivisione delle informazioni. La Cina sembra proporre i principi di "nessuna interruzione", "conformità" e "interconnettività" per la regolamentazione della CBDC che prevede l'uso transfrontaliero della CBDC.
Il primo requisito di "nessuna interruzione" significa che la CBDC di uno stato non dovrebbe interrompere la sovranità monetaria di altri stati e la loro stabilità finanziaria, così come la protezione dei consumatori e competizione leale.
Il secondo requisito è la conformità, attraverso il quale si richiede che i pagamenti

oltre confine effettuati attraverso la valuta digitale debbano essere conformi alle leggi di tutte le giurisdizioni coinvolte.
L'ultimo requisito è l'interconnettività: i pagamenti transfrontalieri dovrebbero, invece di utilizzare un'unica CBDC per le transazioni su entrambi i lati del confine, prevedere l'interoperabilità tra i sistemi CBDC nazionali di diverse giurisdizioni e tra i sistemi CBDC nazionali e i sistemi di pagamento esistenti. Infatti la PBOC preferisce un sistema dove la valute digitali nazionali vengono convertite in altre valute quando i pagamenti oltrepassano i confini.

4.2 In Europa

Sicuramente, rispetto alla Cina, l'Europa è indietro nell'ambito CBDC poiché si è ancora in una fase di studio in cui si ragiona sulla possibile introduzione di un euro digitale che affiancherebbe le banconote e le monete, ampliando la scelta delle persone su come pagare.
La Banca Centrale Europea vorrebbe rispondere alla crescente domanda di pagamenti elettronici sicuri e affidabili e l'euro digitale rappresenta sicuramente la miglior innovazione possibile.
Il 2 ottobre 2020 la BCE ha pubblicato il "Report on digital euro", documento che esamina l'emissione di una CBDC dalla prospettiva dell'Eurosistema.

4.2.1 Ragioni per l'emissione

Un euro digitale potrebbe supportare gli obiettivi dell'Eurosistema fornendo ai cittadini accesso a una forma sicura di moneta in un mondo digitale in rapida evoluzione.

Diversi scenari potrebbero rendere necessaria l'emissione di un euro digitale e, tra di essi, un euro digitale potrebbe rappresentare un'opzione valida per realizzare gli obiettivi connessi alle funzioni fondamentali di banca centrale e alle politiche economiche generali dell'UE, a condizione che sia configurato per soddisfare i requisiti specifici di ogni scenario. Un euro digitale potrebbe essere emesso:

- Per sostenere la digitalizzazione dell'economia europea e l'indipendenza strategica dell'UE;
- Per rispondere al significativo declino del ruolo del contante come mezzo di pagamento;
- Se vi fosse un considerevole potenziale per il diffuso utilizzo di CBDC estere o sistemi di pagamento digitale privati nell'area dell'euro;

Figura 4.2: Obiettivi dell'euro digitale.

- Come nuovo canale di trasmissione della politica monetaria;
- Per mitigare i rischi dovuti alla normale erogazione di servizi di pagamento;
- Per promuovere il ruolo internazionale dell'euro;
- Per favorire il miglioramento dei costi complessivi e dell'impronta ecologica dei sistemi monetario e dei pagamenti.

4.2.2 Potenziali effetti di un euro digitale

L'Eurosistema configurerebbe un euro digitale in modo da evitare possibili implicazioni indesiderate per l'assolvimento del proprio mandato, per il settore finanziario e per l'economia in generale.
L'euro digitale dovrebbe essere strutturato in modo da evitare potenziali conseguenze indesiderate derivanti dalla sua emissione, limitando effetti avversi sulla politica monetaria e sulla stabilità finanziaria ma anche sull'offerta di servizi da parte del settore bancario, e in modo da mitigare i possibili rischi.
L'uso eccessivo di un euro digitale come forma di investimento e il rischio associato di improvvise ampie riallocazioni dai depositi bancari all'euro digitale andrebbero evitati. Un euro digitale dovrebbe essere disponibile tramite intermediari vigilati, mentre i rischi connessi al progetto informatico (ad esempio, ritardi e costi inattesi) andrebbero minimizzati.

Inoltre, la valuta digitale dovrebbe essere un mezzo efficiente per realizzare gli obiettivi dell'Eurosistema rispetto a soluzioni alternative. Le condizioni per il suo

uso all'esterno dell'area dell'euro andrebbero definite e i servizi in euro digitale dovranno essere estremamente resilienti a minacce informatiche.

4.2.3 Considerazioni legali e design tecnologico

L'Eurosistema deve affrontare una serie di importanti questioni legali relative all'euro digitale, fra cui la base giuridica dell'emissione, le implicazioni giuridiche dei diversi impianti teorici e l'applicabilità della legislazione dell'UE all'Eurosistema in quanto emittente.

L'infrastruttura back-end per l'offerta di un euro digitale potrebbe essere accentrata (tutte le operazioni registrate presso la banca centrale) oppure parzialmente decentrata (alcune responsabilità attribuite agli utenti e agli intermediari vigilati). Indipendentemente dall'approccio, l'infrastruttura back-end dovrebbe essere controllata in definitiva dalla banca centrale.

Le soluzioni per l'accesso degli utenti finali all'infrastruttura dell'euro digitale potrebbero essere basate su hardware o software, oppure su una loro combinazione. In ogni caso, le soluzioni di accesso front-end necessitano senza dubbio di un'autenticazione sicura per identificare dell'utente.

Le soluzioni per gli utenti finali e gli eventuali sistemi privati coinvolti nella prestazione di servizi in euro digitale dovrebbero disporre di un'interfaccia con l'infrastruttura back-end della banca centrale, in modo da assicurare la massima protezione dal rischio di creazione ingiustificata di unità di euro digitale senza la sua autorizzazione.

4.2.4 Lavori futuri

Per ottenere risposte significative alle questioni aperte sollevate nel rapporto, verso la metà del 2021 l'Eurosistema ha avviato un progetto per l'euro digitale, iniziato con una fase di indagine e che si concluderà verso la fine del 2023.

Prima di poter prendere in considerazione l'emissione di un euro digitale infatti, è ritenuta necessaria una valutazione esaustiva ed equilibrata sulle sfide di un euro digitale e sul suo potenziale in relazione a opzioni alternative. Le opinioni delle istituzioni, dei cittadini e dei professionisti fornirebbero indicazioni preziose per la valutazione, anche attraverso una consultazione pubblica.

Inoltre, la sperimentazione pratica è necessaria per sottoporre a test le funzionalità e studiarne la fattibilità tecnica, nonché la capacità di rispondere alle esigenze dei

potenziali utenti. La sperimentazione dovrebbe coinvolgere il settore privato e i potenziali utenti nella misura necessaria, senza pregiudicare eventuali decisioni né impegnare l'Eurosistema a fornire un euro digitale.

Figura 4.3: Progetto dell'euro digitale.

Conclusioni

L'idea delle CBDC poggia sul voler creare un'alternativa valida alle valute digitali emesse da privati, introducendo nel sistema il controllo da parte di un'autorità.
La creazione di una digital currency da parte delle banche centrali permetterà quindi alle stesse di esercitare un maggiore controllo, che potrebbe essere visto come una forma di fiducia maggiore da parte del pubblico.
Infatti, nonostante un iniziale scetticismo riguardo alla loro emissione, come mostrato in figura 4.4, si può notare un aumento significativo dei pareri positivi a partire dal 2018.

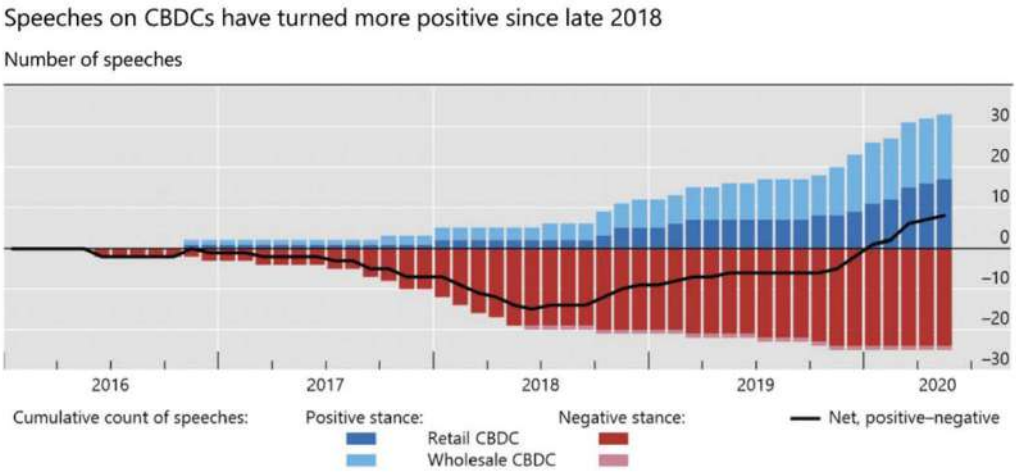


Figura 4.4: Evoluzione delle menzioni positive e negative delle CBDC.

D'altra parte, viene meno l'idea alla base della tecnologia blockchain, ovvero la decentralizzazione, con conseguente assenza di un'autorità centrale.

Il dubbio che rimane riguarda le tempistiche con cui le CBDC potrebbero svilupparsi. Infatti, l'affiancamento di una moneta elettronica a quelle già in uso richiederebbe tempi di adattamento molto lunghi.

In ogni caso esse rappresentano un'evoluzione inevitabile nel mondo dei pagamenti e andranno ad affiancare e in seguito (probabilmente) a sostituire i contanti cogliendo i lati positivi sia delle criptovalute che delle monete fiat.

Bibliografia

[1] Heng Wang. «China's Approach to Central Bank Digital Currency». In: Vol. 18 (forthcoming) (feb. 2022).

[2] PwC. «Central Bank Digital Currency». In: (2020).

[3] Vijak Sethaput e Supachate Innet. «Blockchain application for central bank digital currencies (CBDC).» In: (2022).

[4] European Central Bank. «Report on digital euro». In: (ott. 2020).

[5] European Central Bank. «Central Bank Digital Currency: functional scope, pricing and controls». In: (dic. 2021).

[6] European Central Bank. «Central bank digital currency and bank intermediation». In: (mag. 2022).

[7] George Calle e Daniel Eidan. «Central Bank Digital Currency: an innovation in payments». In: (apr. 2020).

[8] Alisa DiCaprio, Willy Lim e Laurence Eckford. «The future of financial liquidity: CBDCs and Automated Market-Making». In: (apr. 2020).

SOLANA

Michele Masiello, Abdelouahab Moubane, Elisa Salvadori, Filippo Scaramozzino

Blockchain E Criptoeconomia
Solana

Masiello Michele (294949), Moubane Abdelouahab (305716),
Elisa Salvadori (302630), Filippo Scaramozzino (312856)

Indice

1 Introduzione **3**
1.1 SOL . . . 3
1.2 Real Time Carbon Data . . . 4
1.3 La curva ellittica di Solana . . . 5

2 Architettura **7**
2.1 Nodi . . . 7
2.2 Cluster . . . 7

3 Proof of History (PoH) **9**

4 Protocollo di consenso **12**
4.1 Sincronizzazione . . . 12
4.1.1 Transazioni . . . 13
4.2 Rotazione del leader . . . 14
4.3 Fork . . . 14
4.4 Voti, Costi e Reward . . . 15
4.4.1 Voti . . . 15
4.4.2 Staking . . . 15
4.4.3 Costi e Reward . . . 16
4.4.4 Slashing . . . 18

5 Casi d'uso **19**
5.1 DeFi 19
5.2 Applicazioni aziendali 19
5.3 NFT 20
5.3.1 Star Atlas 20

Conclusioni **22**

Sommario

Questa tesina si pone l'obiettivo di introdurre i concetti principali della blockchain Solana e di elencarne i più famosi casi d'uso.
In particolare si concentrerà sul protocollo di consenso utilizzato e sull'algoritmo innovativo: Proof of History.

1 Introduzione

Le fonti utilizzate per questa sezione sono: [1], [2], [3], [4], [5].
Solana è una blockchain pubblica nata come un progetto open-source della fondazione Solana (2020) e si propone come una blockchain che risolve il trilemma delle blockchain (di Vitalik Buterin, il fondatore di Ethereum), ovvero ambisce ad essere una blockchain scalabile, sicura e decentralizzata.
Secondo il fondatore di Ethereum, una blockchain non può possedere tutte e tre le proprietà sopra descritte, ma ne sacrifica una per favorire le altre due, come ad esempio Bitcoin che risulta essere sicura e decentralizzata ma perde invece in scalabilità, per questo motivo le soluzioni più comuni sono le blockchain layer 2 o lo sharding.
Dal sito di Solana al momento di scrittura di questa tesina (20 maggio 2023) possiamo contare 1823 nodi validatori che mantengono la blockchain decentralizzata e sicura lavorando in modo indipendente e una media di 4379 transazioni per secondo.

L'idea di Solana nasce dal whitepaper di Anatoly Yakovenko (2017), in cui viene descritto un nuovo algoritmo: Proof of History, un modo per tenere traccia del tempo, tra computer che non si fidano l'un l'altro.
Anatoly si rese conto che i sistemi blockchain senza orologi, come Bitcoin ed Ethereum (quando usava la PoW), faticassero a superare le 15 transazioni al secondo in tutto il mondo e non sarebbero mai passati a essere un sistema di pagamento globale come quelli centralizzati, ad esempio Visa che raggiunge picchi di 65.000 transazioni al secondo.

Utilizzando una terminologia Web3 Solana è una layer 1 chain perchè fornisce la struttura di una rete blockchain, sulla base della quale altre reti (layer 2) possono essere costruite.
Alcuni esempi di layer 1 includono Bitcoin e Ethereum.
Solana è simile alla blockchain di Ethereum perchè offre sia Token (SOL) e anche un meccanismo distribuito per eseguire smart contracts e connettere applicazioni decentralizzate (dApps).
Guardando più in dettaglio la sua architettura notiamo alcune idee innovative e la sua missione di competere contro Ethereum.

1.1 SOL

La moneta nativa di Solana è SOL, può essere passata ai nodi di un cluster in cambio dell'esecuzione di un programma on-chain, o della validazione del suo output.
L'altra moneta nativa di Solana è Lamport, che equivale a 0.000000001 SOL.

Per ricevere o inviare quantitativi di SOL si deve predisporre di un wallet (una collezione di chiavi pubbliche e private).

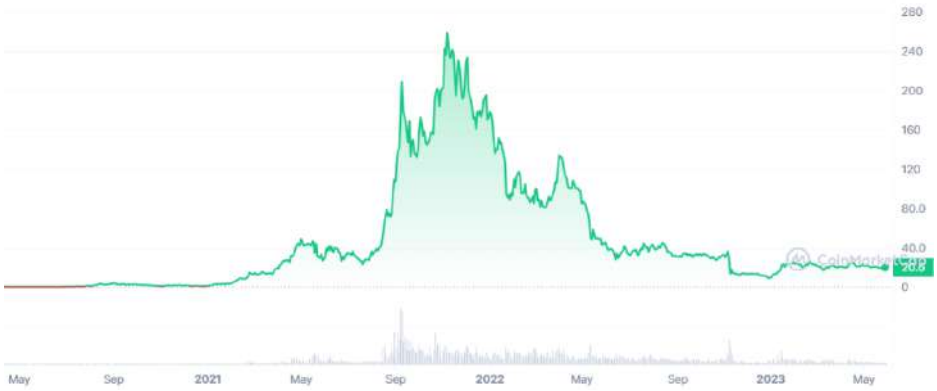


Figura 1: Grafico del prezzo della cryptovaluta SOL in EUR (Euro) fino al 29 maggio 2023 [1].

1.2 Real Time Carbon Data

Il sistema ibrido di consenso di Solana (PoH e PoS) e altre innovazioni di questa blockchain minimizzano il suo impatto ambientale. Solana è infatti la prima blockchain layer 1 a permettere di eseguire gli smart contract e ad avere un sistema di tracciamento delle emissioni in tempo reale.

Il sistema di tracciamento è stato sviluppato in collaborazione con Trycarbonara, e integra il software direttamente sui nodi della blockchain. Infatti le misurazioni cambiano in base al throughput di ogni singolo validatore (online e offline). In particolare i dati che vengono estratti e misurati sono:

- Misurazione dell'emissione dei nodi RPC;
- Granularità delle emissioni a livello di server che incorpora la geolocalizzazione dei validatori e dei nodi RPC;
- Emissioni marginali o consequenziali basate sull'impatto incrementale delle emissioni dovute alla nuova domanda, in relazione alla distribuzione complessiva dell'offerta di rete. Questo quadro può essere utile per valutare l'impatto ambientale delle modifiche e delle ottimizzazioni del consumo energetico e tiene conto del mix di energia rinnovabile delle diverse fonti di elettricità;
- Emissioni incorporate basate sulla produzione, il trasporto e la gestione del fine vita dell'infrastruttura hardware della rete Solana;
- Power Usage Effectiveness (PUE) che descrive l'efficienza complessiva di un data center.

Dal sito [5] si possono vedere i dati dell'impatto ambientale di Solana. Inoltre la Figura 2 e la Figura 3 mostrano l'impronta ecologica di una transazione in Solana rispetto ad altri consumi comuni.
Possiamo quindi notare che una transazione Solana consuma meno energia di una ricerca di Google.

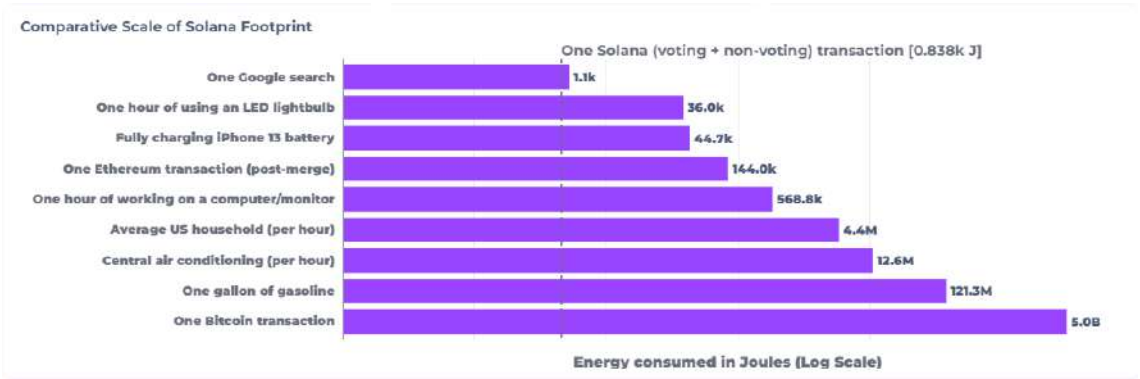


Figura 2: Grafico comparativo dell'impronta di Solana.

Energy Usage Comparison of Solana Transaction

Number of Solana Transaction(s)	Equivalent to
1.3	One Google search
43.48	One hour of using an LED lightbulb
53.96	Fully charging iPhone 13 battery
173.91	One Ethereum transaction (post-merge)
686.96	One hour of working on a computer/monitor
5,318.15	Average US household (per hour)
15,217.39	Central air conditioning (per hour)
146,521.74	One gallon of gasoline
6,043,478.26	One Bitcoin transaction

Figura 3: Confronto consumo di energia di una transazione Solana.

1.3 La curva ellittica di Solana

Solana usa Curve25519 e la rispettiva firma Ed25519.
Curve25519 è una curva di Edwards, un particolare tipo di curve ellittiche, la firma associata è detta EdDSA.

L'EdDSA (*Edwards-curve Digital Signature Algorithm*) è una variante del sistema di firma di Schnorr usando le curve di Edwards.
I vantaggi con EdDSA sono i seguenti:

- EdDSA offre prestazioni elevate su una varietà di piattaforme;
- Non è richiesto l'utilizzo di un numero casuale univoco per ogni firma;
- È più resistente agli attacchi del canale laterale;

- EdDSA usa piccole chiavi pubbliche di 32 byte e firme di 64 byte nel caso di Ed25519;
- Le formule sono "complete", cioè valide per tutti i punti della curva, senza eccezioni. Ciò elimina la necessità per EdDSA di eseguire costose convalide di punti su valori pubblici non attendibili;
- EdDSA fornisce resilienza alle collisioni, il che significa che le collisioni delle funzioni hash non rompono questo sistema.

Quella che segue è una descrizione semplificata di EdDSA, ignorando i dettagli della codifica e della scelta dei parametri.
Uno schema di firma EdDSA si basa sulla scelta di:

- un campo finito $\mathbb{F}_q$, dove q è un numero primo;
- una curva ellittiva E su $\mathbb{F}_q$ il cui gruppo $E(\mathbb{F}_q)$ ha cardinalità $Card(E(\mathbb{F}_q)) = 2^c l$, dove l è un numero primo grande e 2^c è detto cofattore;
- indichiamo con $B \in E(\mathbb{F}_q)$ un generatore di ordine l;
- una funzione hash H con output di $2b$ bit, dove $2^{b-1} > q$, in modo che gli elementi di $\mathbb{F}_q$ e i punti della curva $E(\mathbb{F}_q)$ possono essere rappresentati da stringhe di b bit. Questi parametri sono comuni a tutti gli utenti dello schema di firma EdDSA. La sicurezza dello schema EdDSA dipende in modo critico dalle scelte dei parametri, ad eccezione dellla scelta del generatore.

Una chiave pubblica EdDSA è un punto della curva $A \in E(\mathbb{F}_q)$, codificato in b bit.

Una firma EdDSA su un messaggio M tramite chiave pubblica A è la coppia (R, S), codificata in $2b$ bit, di un punto della curva $R \in E(\mathbb{F}_q)$ e un numero intero $0 < S < l$ soddisfacente la seguente equazione di verifica:

$$2^c SB = 2^c R + 2^c H(R||A||M)A.$$

Una chiave privata EdDSA è una stringa k di b bit che viene scelta in modo casuale. La corrispondente chiave pubblica $A = sB$, dove $s = H_{0,\ldots,b}(k)$ che è il numero intero in little-indian dei primi b bit non significativi di $H(k)$. La firma su un messaggio M è (R, S), dove $R = rB$ e $r = H(H_{b,\ldots,2b-1}(k)||M)$, e $S = r + H(R||A||M)s \pmod{l}$. Questo soddisfa l'equazione di verifica:

$$2^c SB = 2^c(r + H(R||A||M)s)B = 2^c rB + 2^c H(R||A||M)sB = 2^c rB + 2^c H(R||A||M)A.$$

Come anticipato nel caso di Solana, Ed25519 è lo schema di firma EdDSA che usa la hash SHA-512 e curva Curve25519 dove:

- $q = 2^2 55 - 19$;
- $l = 2^2 52 + 27742317777372353535851937790883648493$ e $c = 3$;
- H è SHA-512.

2 Architettura

Le fonti per questa sezione sono: [6]

2.1 Nodi

La blockchain Solana ha solo due tipi di nodi, sono entrambi nodi validatori ma hanno delle differenze:

- Nodi di consenso, i nodi di consenso forniscono due funzioni essenziali per il funzionamento della blockchain: creano e propongono al resto della rete nuovi blocchi, oppure votano sulla validità di nuovi blocchi proposti da altri nodi della rete. Ogni nodo di consenso verifica in modo indipendente ogni messaggio presente in un blocco prima di votarne la validità.

- Nodi RPC (Remote Procedure Call): i nodi RPC possono offrire API, o altri servizi per fornire una comoda interfaccia per gli utenti o le applicazioni.
  I nodi RPC, come i nodi di consenso, verificano tutti i nuovi blocchi e le modifiche alla rete. La differenza sostanziale con i nodi di consenso è che i nodi RPC non votano.

Dopo aver descritto i tipi di nodi presenti in Solana, possiamo aggiungere che tali nodi sono raggruppati in cluster.

2.2 Cluster

Un cluster in Solana è un insieme di nodi validatori che cooperano per gestire le transazioni e mantenere l'integrità del ledger.
Quando due cluster condividono lo stesso blocco di genesi, provano a convergere, altrimenti ignorano la reciproca esistenza. Le transazioni inviate al cluster sbagliato vengono ignorate.

Un nodo validatore riceve tutte le istanze dal leader e vota per confermare se queste istanze sono valide. Dopo aver votato salva le istanze, ma appena avrà osservato un numero sufficiente di copie, elimina la propria.

La conferma di una transazione è definita come il tempo che intercorre tra il timestamp di una nuova istanza e il momento in cui si riscontra la supermajority[1] dei voti.

Solana ruota i leader dei cluster a intervalli fissi, chiamati slot. Ogni leader può produrre istanze solo durante lo slot assegnatogli. Le transazioni sono poi divise in batch in modo da poter inviare transazioni a più nodi senza doverne fare tante copie quanti sono i nodi, ogni nodo poi condividerà il proprio batch con gli altri per ricostruire tutte le transazioni.
Se, ad esempio, il leader avesse bisogno di inviare 60 transazioni a 6 nodi, suddividerebbe quella raccolta di 60 in batch di 10 transazioni e ne invierebbe una a ciascun nodo.

[1] $\frac{2}{3}$ dei validatori pesati tramite il loro stake (ovvero la quantità di token SOL usati come garanzia per partecipare alla validazione dei blocchi).

Per valutare le prestazioni di un cluster si usano due metriche: il numero medio di transazioni al secondo che la rete può sostenere (TPS) e quanto ci mette una transazione a essere confermata dalla supermajority del cluster (Tempo di conferma).

Un'altra importante novità di Solana è la Turbine Block Propagation: ogni nodo di un cluster invia i dati che riceve solo al suo vicinato (neighborhoods), i nodi del vicinato diffondono i dati ad altri nodi vicini e così via, fino a quando il blocco non raggiunge l'intera rete. In questo modo ogni nodo comunica con un piccolo insieme di nodi.
La turbine block propagation permette quindi una diffusione rapida e affidabile dei blocchi all'interno della rete Solana, consentendo una maggiore scalabilità e un alto throughput di transazioni. Questo contribuisce a garantire che la rete Solana possa gestire un gran numero di transazioni in modo efficiente e sicuro.

3 Proof of History (PoH)

Le fonti per questa sezione sono: [18].
La Proof of History fornisce un modo per verificare crittograficamente il passaggio di tempo tra due eventi. Usa una funzione crittograficamente sicura, scritta in modo tale che l'output non può essere previsto dall'input e deve essere completamente eseguita per generare l'output. La funzione viene richiamata in modo ricorsivo, usando l'output precedente come nuovo input, registrando ogni volta l'output e quante volte è stata chiamata. L'output può essere ricomputato e verificato da altri computer.
I dati, o una hash di essi, possono essere aggiunti nello stato della funzione. La registrazione dello stato, dell'indice e dei dati fornisce un timestamp, garantendo che i dati siano stati prodotti prima della generazione dell'hash successivo nella sequenza.

Vediamo come funziona nel dettaglio la PoH:

PoH Sequence

Index	Operation	Output Hash
1	sha256("any random starting value")	hash1
200	sha256(hash199)	hash200
300	sha256(hash299)	hash300

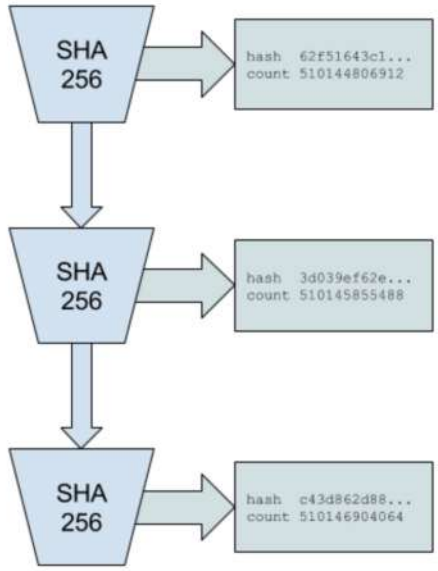


Figura 4: Sequenza di PoH.

Nella Figura 4 si vede come, data in input una stringa casuale, viene calcolato l'output chiamando una funzione (in questo caso sha256, ma è possibile utilizzarne altre), l'output così generato viene a sua volta usato come input. Ad ogni chiamata si registrano il numero di volte in cui è stata chiamata la funzione e l'output di tale hash. A meno di collisioni della funzione hash, si può verificare che effettivamente è passato del tempo tra index 1 (hash1) e index 300 (hash300), poichè non c'è modo di calcolare l'output all'iterazione 300 senza prima calcolare l'output di ogni iterazione partendo dalla stringa casuale iniziale.

La sequenza di hash può essere usata anche per documentare che un dato è stato creato prima della creazione di un particolare indice della hash.
La hash di un particolare dato combinato con la hash precedente funziona da tamestamp per tale dato, poichè può essere stata calcolata solo dopo che quel particolare

dato è stato inserito.

POH Sequence

Index	Operation	Output Hash
1	sha256("any random starting value")	hash1
200	sha256(hash199)	hash200
300	sha256(hash299)	hash300
336	sha256(append(hash335, photograph1_sha256))	hash336
400	sha256(hash399)	hash400
500	sha256(hash499)	hash500
600	sha256(append(hash599, photograph2_sha256))	hash600
700	sha256(hash699)	hash700

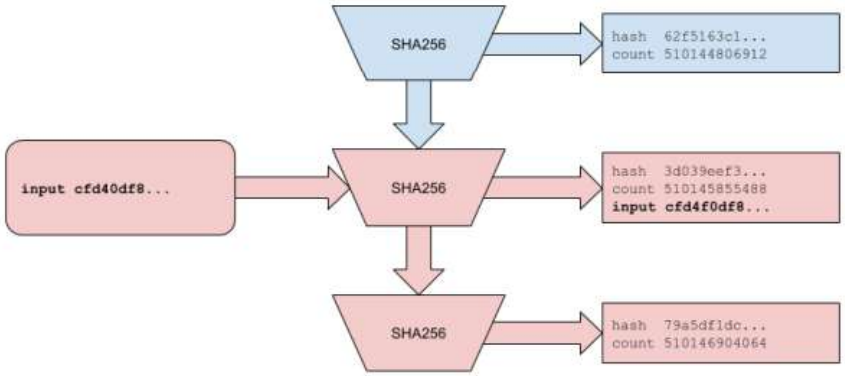


Figura 5: Sequenza di PoH con inserimento di eventi.

Nella Figura 5 si nota come l'aver inserito due dati all'interno della sequenza fa cambiare tutti i valori successivi (i dati possono essere inseriti così come sono o si può calcolare la hash di essi), fino a che la funzione è priva di collisioni sarà impossibile calcolare l'output finale sapendo solamente quale dato sarà inserito nella sequenza.

È possibile sincronizzare le sequenze di PoH dei generatori ricostruendo l'ordine di tutti gli eventi.

Come si nota nella Figura 6 e nella Figura 7, per evitare attacchi da generatori malintenzionati, si può firmare l'evento concatenato con l'ultima hash considerata valida.

La PoH permettere quindi di stabilire un ordine cronologico affidabile degli eventi all'interno della blockchain. Poiché l'ordine degli eventi è già stabilito attraverso i timestamp, i nodi possono elaborare in parallelo le transazioni senza dover attendere la conferma di altri nodi. Ciò consente un aumento significativo delle capacità di transazione della rete e consente la scalabilità.
Inoltre, rispetto ai meccanismi di consenso tradizionali, come PoW, che richiedono notevoli quantità di energia per risolvere complessi calcoli computazionali, PoH è notevolmente più efficiente dal punto di vista energetico.

PoH Sequence A

Index	Data	Output Hash
10		hash10a
20	Event1 = sign(append(event1 data, hash10a), Client Private Key)	hash20a
30	Event2 = sign(append(event2 data, hash20a), Client Private Key)	hash30a
40	Event3 = sign(append(event3 data, hash30a), Client Private Key)	hash40a

Figura 6: Sequenza di PoH con firma.

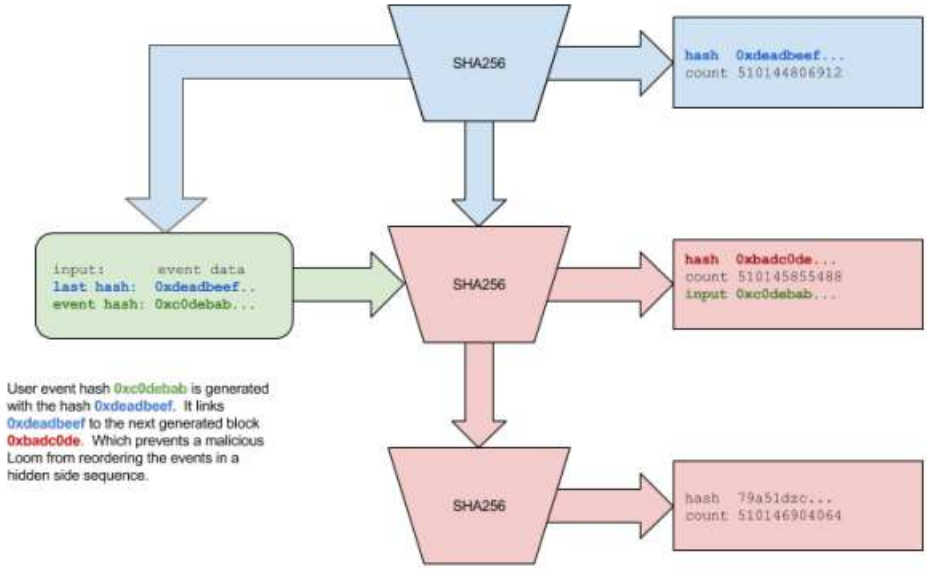


Figura 7: Sequenza di PoH con input una referenza a una precedente hash.

4 Protocollo di consenso

Le fonti per questa sezione sono: [18], [7], [8], [9], [10], [11], [12], [13].
La Proof of History non è un protocollo di consenso ma viene utilizzata per migliorare la Proof of Stake.
La Proof of Stake viene infatti utilizzata per confermare la sequenza di PoH generata, per votare e selezione il prossimo generatore di PoH e per punire comportamenti inappropriati.
I validatori della rete Solana devono possedere e bloccare una quantità di token SOL come garanzia per partecipare al processo di consenso, inoltre vengono selezionati per proporre e convalidare i blocchi sulla base del loro saldo di token SOL bloccati. La selezione dei validatori viene eseguita utilizzando un algoritmo di selezione casuale ponderato in base alla quantità di token bloccati. Questo meccanismo di selezione casuale ponderato aiuta a garantire la sicurezza della rete e impedisce attacchi da parte di partecipanti malevoli.
Il consenso di Solana combina quindi il Proof of History per stabilire un ordine affidabile degli eventi e il Proof of Stake per selezionare i validatori responsabili della convalida dei blocchi. Questa combinazione consente a Solana di raggiungere un alto throughput e una maggiore scalabilità, consentendo alla rete di elaborare un gran numero di transazioni in modo efficiente.
Il generatore di PoH firma lo stato a intervalli predefiniti, ogni validatore conferma tale firma pubblicando la propria firma dello stato. Il voto è un semplice voto favorevole, senza un voto contrario. Se la maggioranza si è espressa come favorevole entro un tempo limite, allora questo ramo è considerato come valido.

4.1 Sincronizzazione

La sincronizzazione affidabile è la ragione principale dell'alto traffico di dati che solana è in grado di ottenere. Le blockchain tradizionali si sincronizzano sulla base di grossi blocchi di dati, in questo modo una transazione deve aspettare una quantità di tempo per essere processata, questa quantità di tempo è chiamata "Block Time". Nel consenso della Proof of Work il tempo da aspettare per validare i blocchi è molto grande, dell'ordine della decina di minuti, mentre nel consenso Proof of Stake non c'è questa restrizione, ma senza timestamp un validatore non può determinare l'ordine dei blocchi. La soluzione più comune è quella di contrassegnare ogni blocco con un wallclock timestamp, ma risulta essere accurato solo entro un'ora o due, inoltre ogni nodo fa affidamento solo al suo personale orologio e non conosce informazioni sugli altri.

Solana, come abbiamo visto in precenza, utilizza una tecnica differente, la Proof of History (PoH): i nodi leader mettono una marca temporale sui blocchi con metodi crittografici per dimostrare che una certa quantità di tempo è passata dall'ultima validazione. Il blocco viene poi condiviso agli altri nodi.
Questa sincronizzazione permette di partizionare i blocchi in transazioni più piccole dette entries.

4.1.1 Transazioni

In particolare, si può riassumere il flusso delle transazioni nel seguente modo:

1. Le tansazioni vengono processate dal leader corrente;
2. Il leader filtra solo le transazioni valide;
3. Il leader esegue le transazioni valide e aggiorna il suo stato;
4. Il leader organizza le transazioni in entries;
5. Il leader trasmette le entries e una firma dell'ultimo stato ai nodi validatori;
6. I validatori trasmettono le entries agli altri nodi del vicinato;
7. I validatori validano la transazione eseguendola nel loro stato;
8. I validatori calcolano l'hash dello stato;
9. Ad uno specifico conteggio di tick della PoH, i validatori trasmettono il proprio voto al leader:
   (a) Il voto è quindi la firma dell'hash dello stato computata in un determinato conteggio di tick della Proof of History (PoH).
   (b) I voti sono propagati via gossip.
10. Il leader esegue i voti, come fa con le transazioni, e li diffonde al resto della rete;
11. I validatori osservano il proprio voto e quello di tutti gli altri validarori del cluster.

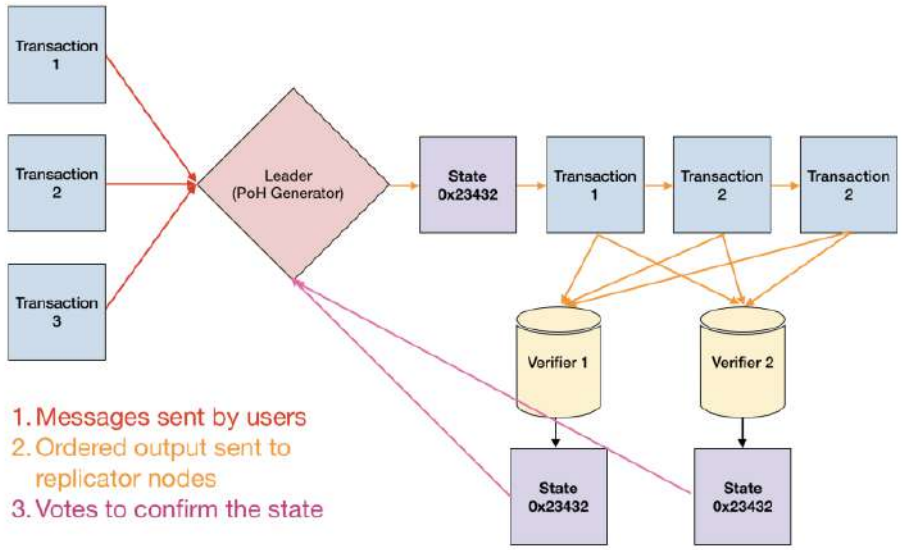


Figura 8: Flusso delle transazioni nella rete.

Dai siti [7] e [8] si può notare la struttura dei blocchi e delle transazioni.

Figura 9: Blocco 194088588.

Figura 10: Esempio di transazione (del blocco 195772030).

4.2 Rotazione del leader

Ad ogni istante, un cluster si aspetta che un solo validatore produca istanze nel libro mastro. Inoltre solo il leader produce la sequenza di Proof of History donando alla rete una prova del passaggio del tempo.
Avendo solo un leader per ogni intervallo di tempo, tutti i validatori sono in grado di replicare copie identiche del libro mastro, lo svantaggio di avere un solo leader è che un leader malintenzionato potrebbe censurare voti e transazioni. Dal momento che la censura non può essere distinta dalla perdita di pacchetti di dati sulla rete, il cluster non può semplicemente eleggere un singolo nodo alla posizione di leader per un tempo indefinito.
Per evitare queste problematiche, il cluster fa ruotare il leader tra i diversi nodi: utilizzando l'altezza dei tick della PoH, Solana genera un ordine casuale e ponderato basato sul peso dello stake dei nodi. Quando il validatore riceve una transazione firmata può essere sicuro che quella transazione è stata prodotta dal leader.

4.3 Fork

Il protocollo Solana non attende che tutti i validatori concordino su un nuovo blocco prodotto prima che venga prodotto il blocco successivo.
Per questo motivo, è abbastanza comune che due blocchi diversi siano concatenati allo stesso blocco genitore, quindi avvengono delle fork.

Le fork si generano quando un leader successivo, non avendo osservato l'ultimo slot di voto, avvia il proprio slot.
Per ovviare a questo problema, i validatori devono votare su una di queste fork e raggiungono un accordo su quale blocco utilizzare attraverso un algoritmo di consenso.
Il punto fondamentale da tenere a mente è che quando ci sono fork concorrenti, solo una fork verrà finalizzato dal cluster e i blocchi abbandonati nelle fork concorrenti verranno tutti scartati.
Più dettagliamente, ogni validatore manda il suo voto su una fork, il voto impegna il validatore per un periodo di tempo detto lockout period, durante il quale il validatore non è autorizzato a cambiare fork.
Ogni voto successivo sulla stessa fork raddoppia la durata del lockout period. Dopo un certo numero di voti configurato dal cluster (attualmente 32), la durata del periodo di blocco raggiunge il cosiddetto max lockout. Fino al raggiungimento del max lockout, il validatore ha la possibilità di attendere fino al termine del lockout period e quindi votare su un'altra fork. Quando vota su un'altra fork, esegue un'operazione chiamata rollback, in base alla quale lo stato torna indietro nel tempo a un checkpoint condiviso e quindi salta in avanti fino alla punta della fork su cui ha appena votato. La distanza massima che una fork può arretrare è chiamata rollback depth.
Questo sistema permette alla blockchain di convergere sulla ramificazione più lunga, quindi quella più votata e utilizzata, che sarà considerata come 'vera'.

4.4 Voti, Costi e Reward

4.4.1 Voti

Un validatore riceve le istanze da un leader e ne vota la validità, gli altri nodi possono verificare la firma del validatore tramite la sua chiave pubblica e, qualora ci fosse evidenza che un nodo validatore ha usato la sua chiave privata per firmare transazioni incorrette, allora lo stake di esso può essere compromesso (il peso del voto del validatore rappresenta tutte le quote delegate (delegated stake) e così anche le ricompense).

4.4.2 Staking

Facendo lo staking dei token SOL, uno staker aiuta a proteggere la rete e guadagna ricompense mentre lo fa, delegando i token ai validatori che elaborano le transazioni e gestiscono la rete.
La delega dello stake è un modello finanziario a rischio condiviso e ricompensa condivisa che può fornire rendimenti ai possessori di token delegati per un lungo periodo.
Ciò si ottiene allineando gli incentivi finanziari dei possessori di token (delegatori) e dei validatori a cui delegano.
Maggiore è lo stake delegato a un validatore, più spesso questo validatore viene scelto per scrivere nuove transazioni nel libro mastro. Più transazioni scrive il validatore, più premi guadagnano il validatore e i suoi deleganti.
I validatori che configurano i loro sistemi per essere in grado di elaborare più transazioni guadagnano proporzionalmente più premi e perché mantengono la rete in esecuzione il più velocemente e agevolmente possibile.

I validatori sostengono costi per l'esecuzione e la manutenzione dei loro sistemi, e questo

viene trasferito ai deleganti sotto forma di una commissione raccolta come percentuale dei premi guadagnati.
Dal momento che i validatori guadagnano più ricompense magggiore è la quota loro delegata, possono competere tra loro per offrire la commissione più bassa per i loro servizi.

4.4.3 Costi e Reward

Non esiste una quantità minima rigorosa di SOL richiesta per eseguire un validatore su Solana.
Tuttavia, per partecipare al consenso, è necessario un conto di voto che abbia una riserva, esente da storage rent, di 0,02685864 SOL. La votazione richiede anche l'invio di una transazione di voto per ogni blocco concordato dal validatore, che può costare fino a 1,1 SOL al giorno.

Gli staker vengono premiati per aver contribuito a convalidare il libro mastro. Lo fanno delegando il loro stake ai nodi validatori.
Sia il validatore che lo staker hanno bisogno di qualche incentivo economico per fare la loro parte. Il validatore deve essere ricompensato per il suo hardware e lo staker deve essere ricompensato per il rischio che la sua quota venga tagliata.
L'idea generale è che il validatore possieda un account Vote. L'account Vote tiene traccia dei voti del validatore, conta i crediti generati dal validatore e fornisce qualsiasi stato aggiuntivo specifico del validatore. L'account Vote non è a conoscenza di alcuno stake a esso delegato e non ha staking weight.
Un account Stake separato (creato da uno staker) nomina un account Vote a cui è delegata la quota. Le ricompense sono proporzionali alla quantità di lamport messi in stake.
L'account Stake è di proprietà solo dello staker. Una parte dei lamport immagazzinati in questo conto è lo stake.

Quindi, per diventare un validatore Solana, è necessario depositare/bloccare una certa quantità di SOL in un contratto. Questi SOL non saranno accessibili per un periodo di tempo specifico. La durata precisa del periodo di blocco dello staking non è stata determinata.

Il sistema cripto-economico di Solana è progettato per promuovere un'economia sana e autosufficiente a lungo termine con incentivi, per i partecipanti, allineati con la sicurezza e il decentramento della rete.
Le commissioni di transazione sono trasferimenti da partecipante a partecipante usati come motivazione e compensazione per l'inclusione e l'esecuzione di una transazione proposta.

Le piccole commissioni pagate per elaborare le istruzioni sulla blockchain di Solana sono note come "commissioni di transazione".
Solana è una delle reti più economiche ed efficienti sul mercato, con una media di 0,00025 dollari per transazione.
Sin dal lancio, Solana ha adottato un approccio fisso alle commissioni di transazione,

con commissioni per singola transazione pari a 0,000005 SOL.
Tuttavia, la situazione è cambiata di recente, poiché è stata introdotta una commissione aggiuntiva, che consente di dare la priorità a determinate transazioni a un costo aggiuntivo.
Una commissione normale è il costo per effettuare transazioni sulla rete di Solana,la commissione aggiuntiva (chiamata anche commissione prioritaria) è una commissione opzionale che consente agli utenti di aumentare le proprie transazioni rispetto ad altri utenti, con tempi di esecuzione più rapidi.
Ecco come viene calcolata la quota di priorità in base alla documentazione di Solana.

> "La commissione di priorità viene calcolata moltiplicando le unità di calcolo massime richieste per il prezzo dell'unità di calcolo (specificato in incrementi di 0,000001 lamport per unità di calcolo), arrotondato per eccesso al lamport più vicino."

La commissione di priorità rappresenta circa un quinto di tutte le commissioni pagate sulla rete in dollari, sebbene tale numero varia di giorno in giorno in modo considerevole.
Per consultare valore aggiornati è possibile visitare direttamente il sito di Solana.

Man mano che ogni transazione (che contiene una o più istruzioni) viene inviata attraverso la rete, viene elaborata dall'attuale leader. Una volta confermata come transazione globale, questa commissione di transazione viene pagata alla rete per aiutare a sostenere il design economico della blockchain di Solana.
Le commissioni di transazione offrono molti vantaggi nel design economico di Solana. Principalmente:

- forniscono una compensazione alla rete di validatori per le risorse CPU/GPU necessarie per elaborare le transazioni;
- ridurre lo spam in rete introducendo costi reali per le transazioni;
- fornire la potenziale stabilità economica a lungo termine della rete attraverso un importo minimo di commissione per transazione.

I voti sono eseguiti come delle transazioni, questo significa che i validatori pagano le transaction fee per partecipare al consenso.

Molte attuali economie blockchain (ad esempio Bitcoin o Ethereum) si affidano alle ricompense (reward) per sostenere l'economia a breve termine, e sulle entrate derivanti dalle transaction fee per quella a lungo termine.

Una percentuale fissa (50%) di ogni commissione di transazione viene bruciata (ovvero distrutta). Il resto viene distribuito al leader corrente per quella transazione.
L'intento di questo progetto è mantenere l'incentivo del leader a includere il maggior numero possibile di transazioni entro il tempo del suo slot.
Pur continuando a fornire un meccanismo di limitazione dell'inflazione che protegge dagli attacchi di "evasione fiscale" (ovvero pagamenti di commissioni sul canale laterale).

Le commissioni bruciate possono anche aiutare a prevenire che i validatori malintenzionati censurino le transazioni considerate nella selezione dei fork.
Esempio di un attacco (caso di un fork Proof of History (PoH) con un leader malintenzionato che censura): a causa delle commissioni perse a causa della censura, le commissioni totali distrutte sono inferiori rispetto a un fork onesto comparabile; se il leader censuratore dovesse compensare queste commissioni perse nel protocollo, dovrebbe sostituire le commissioni bruciate nel suo fork personalmente, riducendo così potenzialmente l'incentivo alla censura fin dall'inizio.
Solana è in grado di gestire fino a 65.000 transazioni al secondo.
Il costo delle transazioni è uno dei motivi principali che determina quanto sia attivo un ecosistema blockchain.
Commissioni basse rendono possibili vari casi d'uso della blockchain, come contratti intelligenti, token non fungibili, applicazioni finanziarie decentralizzate e giochi.
Se il costo delle transazioni è proibitivo, questi casi d'uso non hanno alcuna possibilità di emergere o raggiungere un'adozione significativa.
Poiché il costo delle gas fee[2] su Solana è basso, l'attività NFT sulla rete è decollata nell'ultimo anno, con i mercati NFT di Solana come Magic Eden in testa.

4.4.4 Slashing

Su molte reti Proof-of-Stake esiste un meccanismo noto come "slashing" (taglio). Lo slashing è qualsiasi processo mediante il quale una parte delle stake delegato a un validatore viene distrutta come misura punitiva per azioni malintenzionate compiute dal validatore.

Questo meccanismo incentiva i validatori a non intraprendere azioni malevoli (come la creazione di transazioni non valide o la censura di determinati tipi di transazioni o partecipanti alla rete), poiché una minore quantità di stake delegato a un validatore comporta una riduzione delle ricompense accumulate da quel validatore. Essere soggetti allo slashing può anche essere considerato un rischio reputazionale per mantenere la stake attuale o attirare potenziali stake futuri.

Lo slashing rappresenta anche un rischio per i detentori di token, che potrebbero perdere parte dei loro token se hanno delegato a un validatore che viene sottoposto a slashing. La presenza dello slashing potrebbe incentivare i detentori di token a delegare i loro token solo a validatori che considerano affidabili e a non delegare tutti i loro token a un unico o a un numero limitato di validatori.

Su Solana, lo slashing non avviene automaticamente. Se un attaccante causa l'interruzione della rete, può essere soggetto a slashing al momento del riavvio della rete.

[2] Solana utilizza un modello di calcolo basato su consumi energetici noto come "gas". Ogni operazione o transazione su Solana richiede una quantità specifica di gas, che a sua volta richiede il pagamento di una quantità corrispondente di SOL per coprire i costi di calcolo sulla rete.

5 Casi d'uso

Le fonti per questa sezione sono: [14], [15], [16], [17].

5.1 DeFi

Vista la sua natura open source, le alte prestazioni e un'infrastruttura solida, Solana si offre bene per l'utilizzo in applicazioni finanziare decentralizzate (DeFi). La sua architettura scalabile e la velocità offerta nelle transazioni la portano ad essere una scelta condivisa per molti servizi che non presentano intermediari centralizzati.
Le applicazioni DeFi di Solana includono scambi decentralizzati, piattaforme di prestito e prestito *peer-to-peer*[3], protocolli di staking e molto altro. Gli utenti in questo modo possono partecipare attivamente alle transazioni direttamente dal proprio wallet senza dover affidarsi a servizi terzi come banche o intermediari.
Il vantaggio principale, come menzionato prima, è la velocità di transazione elevata che consente una rapida esecuzione degli ordini a favore dell'esperienza d'uso degli utenti. Altro punto a favore sono le commissioni basse che consentono agli utenti di non sostenere costi essessivi.
Solana, poi, supporta anche la tokenizzazione di asset finanziari su blockchain, contentendo a chi partecipa di scambiare criptovalute, titoli e altri beni digitali. In questo modo vengono aperte nuove opportunità per la creazione di mercati finanziari decentralizzati e per l'accesso a nuovi asset che difficilmente sono negoziabili in modo diretto e globale.
Dato l'aumento dell'interesse per le applicazioni DeFi, Solana sta diventando una scelta affidabile per molti sviluppatori che cercano tutte le qualità che quest'ultima possiede: volume di transazioni in grado di gestire molto alto e ambiente scalabile.
In conclusione, Solana sta guadagnando molta popolarità in questo settore ormai sempre in evoluzione verso la decentralizzazione e nuove soluzioni finanziarie innovative.

5.2 Applicazioni aziendali

Come detto prima: Solana è open source, questo le consente di venire usata anche all'interno di molti applicativi aziendali come può essere la tracciabilità delle forniture. Grazie alla natura immutabile e trasparente della blockchain, è possibile creare registri distribuiti che tracciano il percorso delle forniture lungo l'intera catena di approvvigionamento. Ciò aiuta a migliorare la visibilità e l'efficienza delle operazioni aziendali, consentendo di identificare e risolvere rapidamente eventuali problemi o anomalie.
Può anche essere utilizzata per la gestione delle identità digitali. La blockchain può fungere da registro sicuro e affidabile per le identità digitali dei dipendenti, dei clienti e di altre parti interessate. Ciò semplifica i processi di autenticazione e verifica delle identità, riducendo i rischi di frodi e violazioni dei dati.
Un altro possibile utilizzo è la creazione di registri distribuiti per la gestione delle transazioni aziendali. Le transazioni aziendali, come le transazioni finanziarie, contratti o accordi, possono essere registrate in modo immutabile sulla blockchain Solana, garantendo la loro tracciabilità e consentendo la condivisione e la verifica sicura dei dati tra le parti interessate.

[3] Nelle telecomunicazioni indica un'architettura in cui i nodi possono essere sia client che server.

L'utilizzo di Solana nelle applicazioni aziendali può anche includere la creazione di sistemi di voto e governance decentralizzati. La blockchain offre una base affidabile per la registrazione dei voti e delle decisioni aziendali, garantendo la trasparenza e l'integrità del processo decisionale.
In sintesi, Solana offre molte possibilità di utilizzo all'interno delle aziende sfruttando prestazioni elevate e scalabilità. Queste qualità portano quindi a soluzioni innovative che migliorano l'efficienza operativa e migliorano la trasparenza all'interno delle aziende.

5.3 NFT

Gli *NFT*[4] di Solana rappresentano asset digitali unici e indivisibili che vengono registrati e scambiati sulla blockchain di Solana. Gli NFT di Solana sono token crittografici che rappresentano proprietà digitale esclusiva, come opere d'arte digitali, collezionabili, giochi, oggetti virtuali e molto altro.
Grazie alla alta scalabilità, Solana consente ad artisti, creatori ed utenti di scambiarsi NFT in modo facile e veloce.
Questi vengono acquistati, venduti e scambiati all'interno di diverse piattaforme su mercati decentralizzati. Data la trasparenza della blockchain si può facilmente verificare l'autenticità degli NFT creando fiducia e sicurezza per gli acquirenti.
All'interno di Solana si sono venuti a creare diversi contenuti basati su NFT come la creazione di esperienze interattive e giochi. Vengono usati come token all'interno dei giochi consentendo ai partecipanti di accedere a funzioni speciali, ricompense o avere più peso all'interno di decisioni del progetto.
Questo ecosistema è in continua crescita con artisti, creatori e collezionisti che sfruttano le potenzialità della blockchain per esplorare nuovi modelli di business e interazioni digitali.
Riassumendo, gli NFT in Solana sono asset unici che contribuiscono alla crescita continua della blockchain. Le transazioni rapide e le basse tasse favoriscono il loro scambio, favorendo la creazione di nuove forme di espressione artistica e interazione digitale.

5.3.1 Star Atlas

Un esempio di gioco basato sulla blockchain di Solana è Star Atlas.
Gioco di strategia ambientato in un metaverso galattico futuristico, in cui i giocatori possono esplorare, combattere, commerciare e costruire imperi virtuali.
Ciò che rende Star Atlas unico è l'utilizzo della tecnologia blockchain di Solana per garantire la proprietà e la trasferibilità degli asset digitali nel gioco. Gli oggetti virtuali come navi spaziali, terreni, edifici e risorse sono rappresentati come token non fungibili (NFT) sulla blockchain di Solana. Questo permette ai giocatori di possedere e scambiare liberamente gli asset, creando un'economia virtuale con valore reale.
Il gioco si concentra su una varietà di elementi di gameplay, tra cui esplorazione spaziale, combattimenti, economia e gestione delle risorse. I giocatori possono pilotare navi spaziali, partecipare a missioni, commerciare risorse, costruire e gestire basi stellari, formare alleanze e competere per il controllo di territori nel metaverso.
Inoltre, il progetto ha annunciato piani per introdurre un token di utilità chiamato "ATLAS", che sarà utilizzato come mezzo di scambio e governance all'interno del gioco.

[4] Non-Fungible Token

Gli utenti potranno utilizzare il token ATLAS per acquistare oggetti in-game, partecipare alle attività del metaverso e influenzare le decisioni di governance del progetto.
In sintesi, questo gioco è un esempio di come gli NFT che Solana offre possono essere utilizzati all'interno di un videogioco ben sviluppato per creare un gameplay innovativo basato su un'economia virtuale dinamica.

Conclusioni

In conclusione, Solana si propone di risolvere i problemi di scalabilità delle blockchain tradizionali e di offrire un'architettura innovativa, un sistema di tracciamento delle emissioni in tempo reale e transazioni economiche. Con il suo approccio unico, Solana si posiziona come una potenziale alternativa a Ethereum e ad altre blockchain leader nel settore.

Possiamo riassumere la sua decentralizzazione attraverso diverse considerazioni.
Coefficiente di Nakamoto: Il Coefficiente di Nakamoto, una metrica proposta per la prima volta da Balaji Srinivasan, è definito come il numero minimo di nodi che dovrebbero essere compromessi per alterare o interrompere il consenso in una rete, impedendo così la conferma di alcuni o tutti i nuovi blocchi (e quindi le transazioni al loro interno). Nei network di proof of stake, il Coefficiente di Nakamoto rappresenta il numero minimo di nodi necessari per rappresentare almeno il 33,4% del potere di voto.
Su Solana, il coefficiente di Nakamoto è 31. Ciò significa che il numero più basso di validatori che dovrebbero colludere per censurare la rete è 31.

Blockchain	Nakamoto Coefficient (as of 3/7/23)	Nakamoto Coefficient (as of 8/7/22)
SOLANA	31	31
Avalanche	29	28
Ethereum	1	NA
Thorchain	26	27
Binance	7	7
Cosmos	7	7
Osmosis	6	7
NEAR	8	7
Polygon	4	3

Figura 11: Coefficiente di Nakamoto per diverse blockchain che usano un protocollo PoS.

Diversità dei client: Uno dei punti di vulnerabilità più sottovalutati in una blockchain è il software del client del validatore. I client del validatore sono simili a un sistema operativo: sono il software che un validatore utilizza per partecipare alla rete. Il software è scritto dagli esseri umani ed è soggetto a errori. I client potrebbero avere bug o qualcuno di malintenzionato potrebbe riuscire a introdurre un codice dannoso o compromettere il software utilizzato dal client del validatore. Un modo per ovviare a questi problemi consiste nella creazione di client software aggiuntivi, in modo che i validatori abbiano opzioni su quale client del validatore utilizzare.
Inizialmente su Solana c'era un unico client del validatore, originariamente sviluppato da Solana Labs. Nel agosto 2022, Jito Labs ha rilasciato un secondo client del validatore su mainnet. Si tratta di una derivazione del codice di Solana Labs che Jito sta sviluppando in modo indipendente ed è responsabile della sua manutenzione, modifica e distribuzione.

Concentrazione dei Data center: Chiunque può eseguire un nodo Solana. Poiché Solana richiede hardware ad alte prestazioni, gli operatori dei validatori spesso affittano spazio server da data center privati per eseguire i loro nodi.
Il rischio nell'utilizzo di data center privati per eseguire validatori significa che i proprietari dei data center hanno un potere sproporzionato sul funzionamento di una blockchain. È importante che lo stake su una blockchain sia distribuito in modo relativamente equo tra aziende private che affittano spazio server, al fine di ridurre al minimo il rischio che una singola azienda possa compromettere una catena (nel Novembre 2022 il fornitore di server Hetzner ha bloccato i nodi Solana). Al momento, almeno 3 data center dovrebbero colludere per riunire più del 33,3% dello stake e interrompere la rete.

Concentrazione geografica: Infine, una blockchain globale e resiliente deve continuare a funzionare, indipendentemente dagli eventi che si verificano in una determinata parte del mondo.
La rete Solana è ben distribuita geograficamente, nessun paese possiede il 33,3% dello stake attivo totale.

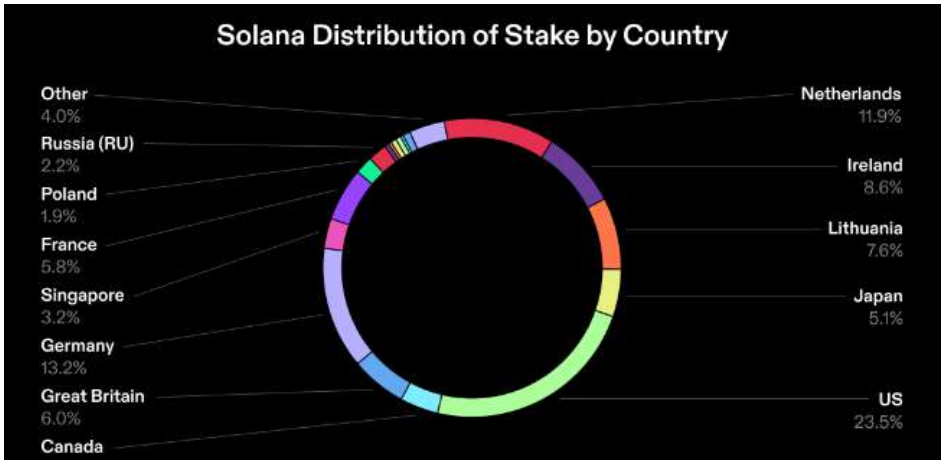


Figura 12: Distribuzione dello stake tra paesi.

Riferimenti bibliografici

[1] URL: https://coinmarketcap.com/currencies/solana/?period=7d.

[2] URL: https://datatracker.ietf.org/doc/html/rfc8032.

[3] URL: https://en.wikipedia.org/wiki/EdDSA.

[4] URL: https://docs.solana.com/introduction.

[5] URL: https://solanaclimate.com/?ref=solana.ghost.io.

[6] URL: https://solana.com/it/news/validator-health-report-march-2023.

[7] URL: https://solscan.io/.

[8] URL: https://solana.fm/blocks?cluster=mainnet-solanafmbeta.

[9] URL: https://docs.solana.com/cluster/overview.

[10] URL: https://docs.solana.com/staking.

[11] URL: https://docs.solana.com/implemented-proposals/staking-rewards.

[12] URL: https://docs.solana.com/economics_overview.

[13] URL: https://coincodex.com/article/24933/solana-gas-fees/.

[14] URL: https://www.criptovaluta.it/solana#:~:text=Permette%20di%20comprare%20e%20vendere,ha%20da%20offrire%20agli%20utenti..

[15] URL: https://thecryptogateway.it/star-atlas-il-metaverso-su-blockchain-solana/.

[16] URL: https://www.maremedia.agency/nft-solana-come-funzionano/.

[17] Singh Shivam. *Solana: Speed and Scale*. independently published, 2022.

[18] Anatoly Yakovenko. *Solana: A new architecture for a high performance blockchain v0.8.13*. URL: https://solana.com/solana-whitepaper.pdf.

POLYGON

E LA POLITICA 110% GREEN

Francesca Portadibasso, Ilaria Panuccio, Giulio Maselli, Iacopo Romano

Blockchain e criptoeconomia

Polygon e la politica 110% green

Francesca Portadibasso, Ilaria Panuccio,
Giulio Maselli, Iacopo Romano

June 2023

Contents

1 Introduzione **3**
1.1 Presentazione di Polygon e del contesto in cui si inserisce 3

2 Problemi di scalabilità delle blockchain **5**
2.1 Problemi di scalabilità delle blockchain, con un focus su Ethereum 5
2.1.1 Polygon Proof-of-Stake (PoS) 6
2.1.2 Polygon zkEVM 6
2.1.3 Polygon Supernets 7

3 Architettura di Polygon **9**
3.1 Spiegazione dell'architettura a *sidechain* di Polygon 9
3.2 Risoluzione dei problemi di scalabilità e congestione della rete . . 9
3.3 Architettura a livelli di Polygon PoS 10
3.3.1 *Smart contracts* di staking su Ethereum 10
3.3.2 Heimdall (livello validatori *Proof of Stake*) 11
3.3.3 Bor (*Block Producer Layer*) 11

4 Sostenibilità ambientale e blockchain **12**
4.1 Problemi ambientali associati alle attività di mining e di elaborazione delle transazioni sulle blockchain 12
4.2 Iniziative sostenibili implementate da alcune blockchain 13
4.2.1 Il progetto "Moss". 14

5 Polygon e l'ecosostenibilità **15**
5.1 Iniziative di sostenibilità di Polygon, con un focus sull'iniziativa "*Polygon Green*" 16
5.2 Polygon supporta l'elaborazione di transazioni "carbon neutral" e utilizza energia rinnovabile 16
5.2.1 Compensazione delle emissioni di carbonio 17
5.2.2 Soluzione di mining "Proof of Stake" 18
5.2.3 Supporto per tecnologie "Layer 2" 18

6 Applicazioni di Polygon **19**
6.1 Applicazioni che possono essere sviluppate su Polygon, con un focus sui vantaggi in termini di sostenibilità ambientale 19

7 Ulteriori commenti e conclusione **20**

8 Bibliografia **21**

1 Introduzione

Polygon rappresenta una rete di blockchain che offre soluzioni di scalabilità compatibili con Ethereum. Noto in precedenza con il nome di Matic Network, il progetto è stato ribattezzato Polygon in seguito alla sua espansione da una singola soluzione ai problemi di scalabilità, quindi come blockchain *Layer 2* (L2) e all'ambizione di creare una rete di reti.
Per ora, è ragionevole assumere che il futuro sia multi-chain. È probabile che non sarà una sola blockchain ad acquisire una dominance completa sul mercato, ma saranno presenti una moltitudine di reti interconnesse, ognuna con le proprie peculiarità, la propria gestione della fiducia, così come prestazioni e sicurezza differenti.
Polygon mira a questo obiettivo: la loro sidechain *Proof of Stake* ha suscitato un certo interesse nella comunità di Bitcoin e delle criptovalute in generale, inoltre il progetto fa parte dell'iniziativa per migliorare la scalabilità di Ethereum.

Si è sentito parlare di Cosmos (una rete centralizzata di blockchain indipedenti) e della sua visione di "internet of blockchains" attraverso l'uso dell'*Inter-Blockchain Communication Protocol* (IBC), dove i messaggi possono spostarsi tra le diverse blockchain che hanno implementato questo protocollo. La visione di Polygon è in parte simile, ma ha adattato questo concetto in modo specifico all'ecosistema Ethereum. L'idea è che gli sviluppatori possano lanciare facilmente le loro soluzioni di *scaling* compatibili con Ethereum o persino blockchain autonome (*stand alone*).

1.1 Presentazione di Polygon e del contesto in cui si inserisce

Polygon è un framework per la creazione di reti blockchain e soluzioni di scalabilità compatibili con Ethereum, da definirsi più come un protocollo che una singola soluzione. Ecco perché una delle principali offerte dell'ecosistema è il **Polygon SDK**, che consente agli sviluppatori di creare queste reti compatibili con Ethereum. Polygon è inoltre concepito come un modo per qualsiasi sviluppatore di creare una rete blockchain dedicata che combini tutte le migliori caratteristiche delle blockchain *stand-alone* (flessibilità, sovranità e scalabilità) con il meglio di Ethereum (sicurezza, esperienza dello sviluppatore, interoperabilità).

Avendo la scalabilità come punto centrale, Polygon si basa su Ethereum proprio perchè mira a superare il limite della scalabilità di questa blockchain. Il protocollo di messaggistica interoperabile e il framework specializzato di Polygon offrono opportunità uniche per sfruttare l'ecosistema popolare e consolidato di Ethereum. Diversi progetti hanno già sfruttato Polygon come soluzione di

ridimensionamento, tra cui *EasyFi* (una piattaforma DeFi, quindi di "finanza decentralizzata"), *Polymarket* (un popolare mercato di previsione) e *Aavegotchi* (un gioco di trading da collezione NFT).

Uno dei primi prodotti disponibili sull'ecosistema Polygon è stato quello della sidechain *Proof of Stake (PoS)*. Una *sidechain* è essenzialmente una catena parallela collegata a un'altra blockchain che può offrire diversi vantaggi, in particolare un aumento del flusso delle transazioni e commissioni ridotte.
Dal momento che Polygon supporta l'*Ethereum Virtual Machine* (EVM), le applicazioni esistenti possono essere trasferite facilmente. Questo può offrire agli utenti un'esperienza paragonabile a quella su Ethereum, con l'aggiunta dell'elevato *throughput* e le basse commissioni menzionate in precedenza. Inoltre, rende la realtà di Polygon una prospettiva molto interessante per gli sviluppatori che già lavorano con *Solidity* (il linguaggio di programmazione nativo di Ethereum).

Quindi, cosa può fare un utente su Polygon? Incredibilmente, si possono effettuare operazione simili a quelle su Ethereum, ma molto più economiche e veloci. Alcune delle dapp DeFi più popolari sono già state trasferite su Polygon, come *Aave, 1inch, Curve* e *Sushi*. Ci sono anche alcune applicazioni native che non esistono altrove, come *QuickSwap* e *Slingshot*. Lo sviluppo di Polygon è guidato dai suoi fondatori: Jaynti Kanani, Sandeep Nailwal, Anurag Arjun e Mihailo Bjelic.

Un altro obbiettivo principale di Polygon è quello di offrire un framework per la creazione di reti blockchain che possono essere interconnesse, invece di essere isolate l'una dall'altra. Polygon ha pianificato una serie di funzionalità innovative, tra cui *ZK roll-up*, che raggruppano un gran numero di trasferimenti *off-chain* in singole transazioni e *Optimistic roll-up*, in esecuzione su Ethereum per fornire transazioni quasi istantanee. Entrambe queste funzionalità offrono vantaggi unici nella corsa per scalare Ethereum e risolvere gli attuali problemi di congestione della rete e le elevate commissioni di transazione.

2 Problemi di scalabilità delle blockchain

La scalabilità di una blockchain è la capacità di gestire flessibilmente qualunque tipo di aumento di transazioni senza peggiorare il servizio. Una buona scalabilità assicura la massima velocità nell'esecuzione delle transazioni anche durante i picchi di traffico a prezzi costanti.

2.1 Problemi di scalabilità delle blockchain, con un focus su Ethereum

Ethereum è la principale blockchain per lo sviluppo di *smart contract* e *Decentralized Applications (DApps)*[1]. Negli anni il traffico sulla rete Ethereum è aumentato esponenzialmente, e per questo è aumentato il costo del gas, ossia il prezzo per eseguire *smart contract*.
In origine, Ethereum adottava un meccanismo di consenso chiamato "*Proof of Work (PoW)*" che consentiva di eseguire solamente 15 transazioni al secondo. La *PoW* si otteneva dai *miners* che dimostravano di avere compiuto un grande lavoro risolvendo un problema matematico complesso. Nel 2022, la blockchain ha adottato il meccanismo della "*Proof of Stake (PoS)*", in quanto la PoW risultava ormai obsoleta per la lentezza e la grande richiesta di energia per la potenza di calcolo. Il cambio di protocollo ha portato quindi dei benefici, tra i quali:

- l'aumento della velocità di inserimento di un blocco, ora costante e uguale a 12 secondi;
- la riduzione del consumo energetico, che si stima essere del 99.95% rispetto a quello del protocollo PoW

Polygon fornisce l'infrastruttura e il codice di base per creare facilmente DApps o blockchain scalabili e compatibili con Ethereum. Nell'ottica di fondare un Internet of Blockchains, Polygon fornisce anche un protocollo di interoperabilità che permette a tutti i suoi network di comunicare tra loro e con Ethereum.
I protocolli principali utilizzati al fine di garantire i servizi suddetti sono:

- **Polygon Proof-of-Stake (PoS)** per l'inserimento di un nuovo blocco nella blockchain;
- **Polygon zkEVM** per il potenziamento della sicurezza quando si creano DApp;
- **Polygon Supernets** per creare blockchain scalabili e specifiche per l'applicazione che si vuole creare.

[1] Le DApp sono applcazioni decentralizzate costruite sulla blockchain di Ethereum, che è una rete *peer-to-peer* distribuita su molti nodi. Le DApp di Ethereum possono offrire una vasta gamma di funzionalità e possono consentire agli utenti di interagire tra loro, eseguire transazioni, scambiare beni e servizi e persino partecipare a governanze o votazioni decentralizzate. Le DApp di Ethereum sono composte da *smart contract*, che sono programmi autonomi eseguiti sulla blockchain.

2.1.1 Polygon Proof-of-Stake (PoS)

Come anticipato, la *Proof of Stake* è il protocollo adottato da Ethereum e anche da Polygon per l'inserimento di un nuovo blocco nella blockchain. Nella *PoS*, è fondamentale il numero di token di valuta digitale detenuti da ciascun utente, in quanto più ne risultano, più è alta la probabilità che non si stia violando il sistema. I partecipanti (*validators*) sono selezionati su base pseudocasuale per coniare i blocchi e aggiungerli così alla blockchain.
I **vantaggi** di utilizzare la PoS, rispetto al vecchio protocollo PoW, sono:

1. La richiesta di meno energia elettrica (la PoS è nata nel 2012 proprio per risolvere questo problema);

2. La sostenibilità a livello ecologico, proprio per il minore consumo di energia elettrica;

3. Il maggiore coinvolgimento dei *validators* all'interno della blockchain rispetto a quanto lo fossero i *miner*.

2.1.2 Polygon zkEVM

Il protocollo zkEVM è una combinazione di due potenti tecnologie:

1. **Zero Knowledge (zk)**: si tratta di un protocollo crittografico che fornisce maggiore sicurezza durante la creazione di prove per convalidare una dichiarazione. L'idea alla base di zk sta nel fatto che è possibile provare un'affermazione senza necessariamente esporre le informazioni utilizzate per raggiungere quella soluzione. Nel campo blockchain, il concetto di *zero knowledge* è utilizzato per aumentare la privacy nelle transazioni, proteggere credenziali e migliorare l'autenticazione.

2. **Ethereum Virtual Machine (EVM)**: si tratta del sistema utilizzato dalla rete Ethereum per consentire l'esecuzione di *smart contract* e *DApp* sulla blockchain, grazie ad un linguaggio di programmazione chiamato *Solidity*. Data la sua funzionalità decentralizzata e la capacità di archiviare *smart contract* eseguibili con EVM, Ethereum diventa un grande computer mondiale decentralizzato, in grado di eseguire istruzioni che portano alla risoluzione di qualsiasi compito specifico.

zkEVM unisce la velocità e il potenziamento della sicurezza della crittografia *Zero Knowledge* con la standardizzazione della codifica e dello sviluppo software di EVM.

Data la difficile scalabilità e i costi di transazione di Ethereum, si possono apportare diverse soluzioni, come nel caso dei *rollup*. Questi fungono da soluzione all'avanguardia per accelerare le transazioni nel campo della blockchain, infatti sono mezzi utilizzati per esternalizzare il calcolo dalla rete a un ambiente *off-chain*. Nello specifico, abbiamo due tipologie di *roll-up* adottate da Polygon:

- **ZK roll-up**: sfrutta la crittografia *Zero Knowledge* per migliorare questo processo *off-chain*. Con *ZK rollup* solo la prova di validità viene inviata ad Ethereum, il che riduce i costi e il tempo di elaborazione delle transazioni.
- **Optimistic roll-up**: si tratta di protocolli che aumentano la produzione di transazioni raggruppando una quantità di esse in lotti (*batch*), che vengono elaborati *off-chain*. Successivamente, i dati delle transazioni vengono registrati sulla catena principale con tecniche di compressione dati che contribuiscono a ridurre i costi e ad aumentare la velocità.

2.1.3 Polygon Supernets

Si tratta di un progetto di rete distribuita che ha il fine di creare blockchain scalabili e specifiche per l'applicazione che si vuole creare. Le *Supernet* sfruttano un "*bridge*[2] nativo" per connettersi con una *rootchain* associata, nello specifico la "*Polygon PoS*", consentendo loro di ereditarne la sicurezza e le capacità. Inoltre, le *Supernet* estendono lo spazio di blocco disponibile sulla *rootchain*, fornendo scalabilità e interoperabilità per le applicazioni decentralizzate.
Con meccanismi di *governance on-chain*, le *Supernet* consentono alle comunità di prendere decisioni e aggiornare la rete in modo trasparente e conforme.

Sottolineiamo il fatto che le *Supernet* possono avere diverse identità con obbiettivi diversi in base alla prospettiva in cui le si guarda. Per esempio, esse possono rappresentare:

- ***Appchain***: reti blockchain per applicazioni progettate per casi d'uso specifici. Queste sono reti blockchain personalizzabili che gli sviluppatori possono adattare per soddisfare casi d'uso specificatamente definiti. Con le *appchain* si possono creare reti blockchain ad alte prestazioni veloci e a basso costo;
- **La fase successiva del ridimensionamento di *Polygon PoS* ed Ethereum**: le *Supernet* consentono a progetti e aziende di creare reti blockchain di livello 3 altamente scalabili che soddisfano i loro requisiti specifici di spazio di blocco ereditando la sicurezza e l'integrità della rete principale Polygon PoS ed Ethereum. Ricordiamo che il livello 3 di una blockchain è il luogo in cui le applicazioni generali sviluppate sul livello 2 (considerato come il livello della scalabilità) possono essere utilizzate per sviluppare soluzioni specifiche;
- **Un framework modulare che semplifica lo sviluppo della blockchain**, fornendo agli sviluppatori gli strumenti necessari per creare reti blockchain personalizzabili che siano scalabili, sicure e interoperabili. Gli sviluppatori possono utilizzare lo *stack Supernet* per creare reti blockchain ad alte prestazioni con funzionalità avanzate senza preoccuparsi di complesse integrazioni o intermediari;

[2] Il meccanismo di *bridging* è un'infrastruttura tecnica che facilita il trasferimento di messaggi tra qualsiasi *rootchain* e una *Supernet*.

- **Reti blockchain personalizzabili per una logica aziendale affidabile**: una macchina virtuale personalizzabile fornisce il supporto completo di EVM pronto all'uso, consentendo agli sviluppatori di adattare la macchina virtuale alle loro esigenze e requisiti specifici;

- **L'infrastruttura blockchain più supportata nello spazio web3**: offrono varie infrastrutture di nodo e distribuzione, indicizzatori, esploratori, oracoli e molti altri strumenti di livello mondiale necessari per la creazione e la distribuzione di *Supernet* e le relative applicazioni associate;

- **Modelli di *governance* ibridi** che consentono la progettazione di reti senza autorizzazione o reti autorizzate con vari gradi di sovranità in base alle esigenze dell'utente e del manutentore, inclusa la possibilità di autorizzare validatori e amministratori di rete. Tutto questo grazie ad un meccaniscmo delle *Supernet* di *governance on-chain* che consente il processo decisionale e la gestione della blockchain guidati dalla comunità;

- ***"Multi-chain"* guidata e interoperabile**: la soluzione di *bridging* nativo adottato dalle *Supernet* consente il trasferimento continuo di risorse da varie blockchain compatibili con EVM all'ecosistema *Polygon*. Questa soluzione di *bridging* consente agli sviluppatori di personalizzare i *plug-in bridge* per soddisfare requisiti specifici, facilitando l'interoperabilità tra blockchain e livelli diversi.

3 Architettura di Polygon

3.1 Spiegazione dell'architettura a *sidechain* di Polygon

L'architettura a *sidechain* di Polygon è una soluzione progettata per risolvere i problemi di scalabilità e congestione della rete Ethereum. In particolare, una *sidechain* è una blockchain indipendente che può essere collegata ad una blockchain principale, come Ethereum, al fine di offrire funzionalità aggiuntive e migliorare la scalabilità del sistema.
La *sidechain* Polygon è gestita da *validators* che garantiscono l'integrità delle transazioni e la sicurezza della rete. Rispetto ad Ethereum, Polygon è una *sidechain* e il token **MATIC** di Polygon è anche un token ERC-20[3] di Ethereum, consentendo una facile interoperabilità tra le due blockchain. Ciò significa che le transazioni e le attività eseguite sulla blockchain Polygon vengono registrate sulla blockchain Ethereum principale, ma senza sovraccaricare la sua capacità di elaborazione.

3.2 Risoluzione dei problemi di scalabilità e congestione della rete

Polygon, come Ethereum, utilizza il protocollo di consenso *Proof of Stake* che, come vedremo, aiuta notevolmente a risolvere i problemi di scalabilità delle blockchain. Polygon Network è quindi una piattaforma di applicazioni blockchain che fornisce *sidechain* ibridi abilitati per *Proof-of-Stake* e Plasma.
Il meccanismo PoS di Polygon consente ai *validators* di bloccare una quantità di criptovaluta come garanzia per la partecipazione alla verifica delle transazioni e alla sicurezza della rete. Inoltre, Polygon utilizza un'architettura chiamata *Heimdall*, popolarizzata da Cosmos, che consente di selezionare casualmente i nodi validatori che saranno i produttori di blocchi.
Per abilitare il meccanismo di *Proof of Stake* sulla piattaforma, un insieme di contratti di gestione dello *staking* viene implementato su Ethereum, insieme a un gruppo di *validators* incentivati che eseguono i nodi Heimdall e Bor.
Questa architettura *dual consensus* consente di decentralizzare la rete e garantire un alto *throughput* delle transazioni, migliorando la scalabilità del sistema. Su una singola *sidechain*, è stato registrato un throughput di 7000 *transazioni al secondo (TPS)*.

Infine, Polygon ha implementato un sistema di incentivi per i *validators*, chiamato *MATIC token*, che viene utilizzato per garantire l'integrità della rete e la sicurezza delle transazioni. In questo modo, è stato creato un ecosistema incentrato sulla sicurezza e sulla scalabilità, che ha permesso di superare i limiti della blockchain Ethereum e offrire una piattaforma più efficiente e scalabile.

[3] ERC-20 è uno standard stabilito da Ethereum per scrivere gli *smart contract* relativi ai token. ERC sta per "Ethereum Request Comment", 20 è un numero arbitrario

3.3 Architettura a livelli di Polygon PoS

Uno sguardo più a fondo nell'architettura che costituisce la **PoS** rivela la presenza di tre livelli già citati:

- *Smart contracts* di *staking* su Ethereum;
- Heimdall (livello *Proof of Stake*);
- Bor (livello produttore di blocchi).

3.3.1 *Smart contracts* di staking su Ethereum

Polygon mantiene un insieme di *smart contracts* su Ethereum, che si occupano di:

- **Gestione dello *staking* per il livello PoS**: lo *staking* è un processo in cui gli utenti detengono e bloccano una determinata quantità di criptovaluta all'interno di un protocollo blockchain, al fine di supportare le operazioni di rete e contribuire alla sicurezza e alla validazione delle transazioni.
- **Gestione della delega**: la gestione della delega, inclusa la condivisione dei validatori, si riferisce al processo di attribuzione delle responsabilità di convalida e di voto ai partecipanti al sistema di *staking*. In un sistema di consenso PoS, i partecipanti che desiderano convalidare transazioni e contribuire alla sicurezza della rete possono delegare le proprie criptovalute ad un nodo o ad un insieme di nodi validatori più esperti o affidabili;
- **Checkpoints/snapshots dello stato delle sidechain**: in un contesto blockchain, i *checkpoint* o gli *snapshot* si riferiscono a un momento specifico in cui viene registrato lo stato attuale di una sidechain. Questi vengono quindi utilizzati per registrare l'intero stato della *sidechain* in un determinato punto nel tempo, inclusi i saldi dei conti, le transazioni eseguite e altre informazioni pertinenti. Questi oggetti sono importanti perchè definiscono la fine delle operazioni e sono inoltre caratterizzati da *Proof of Burn*[4] per definire il prelievo degli asset.

[4] La **PoB** consiste nell'inviare monete a indirizzi verificabili pubblicamente, i quali diventano inaccessibili e inutili. Tipicamente, questi indirizzi (detti anche *eater address*) vengono generati casualmente senza associarvi una chiave privata. Naturalmente, il processo di eliminazione delle monete riduce la disponibilità sul mercato e crea una scarsità economica, causando un potenziale aumento del loro valore. Ma soprattutto, il *coin burning* è un altro modo per investire nella sicurezza del network. E' un modo per dimostrare il proprio impegno nei confronti del network, ottenendo il diritto di "minare" e convalidare transazioni. Dato che il processo di eliminazione delle monete rappresenta *mining power* virtuale, maggiore sarà il numero di monete bruciate da un utente in favore del sistema, maggiore sarà la sua *mining power*.

3.3.2 Heimdall (livello validatori *Proof of Stake*)

Il livello Heimdall amministra sia l'aggregazione dei blocchi prodotti dal **Bor** in un albero di Merkle, che la pubblicazione periodica (*checkpoint*) della radice di Merkle sulla catena principale. Inoltre, si occupa della generazione dei *check*. Per un certo numero di blocchi su Bor, un validatore (sul layer Heimdall):

- convalida tutti i blocchi dall'ultimo checkpoint;
- crea un albero di Merkle degli hash dei blocchi;
- pubblica la radice di Merkle sulla catena principale.

3.3.3 Bor (*Block Producer Layer*)

Bor è il layer generatore di blocchi di Polygon, l'ente responsabile dell'aggregazione delle transazioni in blocchi.
Tramite una selezione del comitato presente in Heimdall, i produttori di blocchi vengono periodicamente rimescolati in intervalli chiamati "span". Dalla produzione dei blocchi nel nodo Bor, si passa alla loro convalida, la quale avviene nei nodi Heidmall. Inoltre un *checkpoint*, contenente l'hash dell'albero di Merkle generato da un insieme di blocchi, viene periodicamente confermato su Ethereum.

4 Sostenibilità ambientale e blockchain

4.1 Problemi ambientali associati alle attività di mining e di elaborazione delle transazioni sulle blockchain

Il mining delle blockchain è un processo altamente costoso dal punto di vista energetico, che minaccia la volontà delle varie nazioni di raggiungere l'indipendenza dalle fonti fossili responsabili dei mutamenti climatici globali e dell'inquinamento. L'incremento delle attività di mining nei vari paesi ha comportato una crescente domanda di energia elettrica con il conseguente aumento delle emissioni di CO_2 e inquinamento dell'aria.
E' stato osservato che molto spesso i miner, a causa del design della *Proof of Work*, sono incentivati a minare velocemente a discapito della fonte di energia utilizzata. In particolare, per operazioni onerose si è evidenziata la tendenza a preferire fonti antieconomiche derivanti da centrali a carbone o piccoli impianti a gas a favore di una disponibilità di energia più rapida.
Inoltre, per un maggiore profitto, molti miners si sono spostati in paesi come Cina o Stati Uniti dove il costo dell'energia è molto più basso, non tenendo in considerazione che circa il 70% di essa è generata da carbone o petrolio.

Per dare uno sguardo alle principali criptomonete e al loro impatto, possiamo prendere in considerazione delle stime sul consumo degli impianti, nonostante sia effettivamente impossibile misurare efficacemente i reali consumi. Tra le criptomonete più diffuse, è stato stimato da Digiconomist[5] che l'impronta ecologica annua di Bitcoin si attesta a circa $73Mt\ CO_2$ (milioni di tonnelate di CO_2), comparabile con un anno dello stesso periodo di emissioni dell'intero Turkmenistan. Tale risultato ha portato gli esperti a definire la criptovaluta come "carne digitale", in quanto il loro impatto ambientale è comparabile.
Dall'altro canto Ethereum, fino a settembre 2022, era responsabile di "sole" $35.4Mt\ CO_2$ annue, questo prima che abbandonasse la *Proof of Work* per introdurre la *Proof of Stake*, andando a ridurre l'impatto del 99% (cioè attestandosi a $0.01Mt\ CO_2$/anno).
In generale, delle oltre $20,000$ criptomonete esistenti, nessuna (o quasi) tiene traccia del proprio consumo energetico per produrre nuove monete o per la gestione dei servizi. Gli studiosi affermano che il carattere competitivo del processo di mining sia di ostacolo all'obiettivo di ridurre le emissioni e di salvaguardia dell'ambiente, proponendo di adottare sistemi e procedimenti che richiedano meno macchine per svolgerli; un esempio è *The Merge*[6] di Ethereum che semplifica il processo di validazione.

Un altro problema che è andato evidenziandosi con il sorgere dell'era delle criptomonete è la produzione di rifiuti elettronici detti ASIC (circuiti integrati per

[5] Digiconomist è una piattaforma dedicata a esporre le conseguenze indesiderate delle tendenze digitali, in genere da una prospettiva economica.

[6] Con il *merging* di Ethreum si intende il processo mediante il quale la blockchain Ethereum si è spostata verso il protocollo PoS

applicazione specifica) dovuto al fatto che i dispositivi utilizzati diventano facilmente obsoleti come conseguenza della rapida evoluzione del settore informatico ed elettronico. A causa della crescente potenza di calcolo richiesta per il mining, soprattutto nel caso di Bitcoin, i miners tendono ad acquistare apparecchiature sempre più performanti e avanzate dal punto di vista tecnologico, al fine di svolgere calcoli più velocemente e cercare di aggiudicarsi il premio. Molto spesso tali dispositivi hanno come unico fine la risoluzione e la verifica degli hash per cui, una volta sostituiti, non possono essere riutilizzati in alcun modo.
La vita media di quest'ultimi è stimata intorno a 1.29 anni ma in genere vengono cambiati molto prima per ragioni di carattere profittuale che porta ad un incremento di rifiuti elettronici. Questo problema è esacerbato dal fatto che in molti Paesi o corporazioni non ci sia una vera politica di smaltimento di questi rifiuti. Gran parte della responsabilità ricade sulle società che li producono come Bitmain, il principale produttore di ASIC, che paradossalmente è incapace di gestire gli stessi che, tutt'ora, rappresentano l'83% degli scarti elettronici.

4.2 Iniziative sostenibili implementate da alcune blockchain

Per affrontare questi problemi, sono state proposte diverse soluzioni. Una potrebbe essere l'adozione di un sistema di consenso alternativo come il **Proof of Stake** (PoS), che, come detto in precedenza, richiede molta meno energia rispetto al PoW e in particolare non vi è bisogno di uno specifico dispositivo per il processo di validazione. Inoltre, la ricerca di fonti di energia rinnovabile potrebbe rappresentare un'opzione importante per il mining di criptovalute.

Per citare alcune reti blockchain energicamente efficienti, *Chia Network* ha adottato un approccio "eco-friendly" che utilizza la tecnologia di storage invece della computazione intensiva per il mining. Nello specifico è stata implementata la **Proof-of-Space Time** che utilizza *hard drives* e archivi e che prevede un meccanismo di consenso che non richiede un costante bisogno di elettricità per processare e validare le operazioni.
Toucan, assieme ad altre blockchain come *Klima* e Polygon stessa, utilizza *carbon credits* spingendo verso atteggiamenti e progetti sempre più responsabili in materia di emissione e tutela dell'ambiente.

Il **Voluntary Carbon Market** (VCM) lavora diversamente dai mercati regolati dai governi, sono questi ultimi a dettare le regole e gli obiettivi da raggiungere e anche loro stessi si fissano come obiettivo la riduzione delle emissioni. Al **VCM** si contrappone il **Compliance Market** in cui gli enti (come compagnie aeree, industrie, centrali) sono costretti a rispettare e a trovare soluzioni più green.

4.2.1 Il progetto "Moss".

L'iniziativa Moss è due progetti in uno: un token popolare (MCO2) e un progetto NFT (*Non-Fungible Tokens*) basato sul clima. Entrambi i progetti si basano sul concetto di tokenizzazione per incentivare la riduzione delle emissioni. Il token MCO2 è disponibile come token ERC-20 su borse popolari, come Coinbase. L'acquisto del token finanzia progetti di compensazione del carbonio, la maggior parte con sede dentro e intorno alla foresta pluviale amazzonica.
Il progetto **Moss Amazon NFT** funziona in modo leggermente diverso. Moss acquista porzioni dell'Amazzonia a rischio di deforestazione. Quel terreno viene poi diviso in porzioni di 1 ettaro, ciascuna delle dimensioni di un campo da calcio. I diritti su tali porzioni sono digitalizzati e tokenizzati come NFT. Ogni NFT è quindi unico e legato a un pezzo unico di proprietà. Nello specifico, quelli di Moss Amazon sono vere e proprie vendite di terreni di cui il 30% del ricavato va a un fondo di conservazione. Quel fondo paga per il pattugliamento e la protezione fisica delle partecipazioni Amazon NFT.
Polygon è una delle piattaforme usate per la vendita di tali token.

5 Polygon e l'ecosostenibilità

Importante per trattare l'argomento è presentare il **Manifesto Green** che Polygon stesso ha pubblicato.
Citiamo per esteso ciò che viene detto:

A Smart Contract with Planet Earth

"When our children ask us what we were doing during the crucial decade when the future of life on Earth hung in the balance, will it be enough to say we were building a complete suite of Ethereum scaling solutions? Will all of our daring ambition, our hard work and ingenuity, our trials, tribulations and victories seem meaningful from the vantage point of the generation that comes after.
We think the answer can be "yes," but we need to take steps now to make sure that it is. The Polygon team deeply believes that Web3 is a transformative technology that will make the current Internet era seem like the Dark Ages.
But we also recognize that in creating that future we cannot ignore the broader context of what technological progress has meant for the planet.
The geological scale of anthropogenic climate change can be almost incomprehensible to a mere human: waters rushing back to the coastlines as the colossal churn of the Gulf stream weakens its pull, thermal expansion of the oceans, days growing longer as gravity-driven liquid bulge at the equator slows the rotation of the Earth. The scope of the problem can be dispiriting, but we can start by doing what's possible.
That's why Polygon is eliminating all of the network's carbon debt going back to inception and then going carbon negative in 2022. This means that every transaction – an NFT minted by an artist, a DeFi trade that empowers individual economic autonomy, a token bridged to a project building on our network – is accounted for and its environmental impact is offset. When this goal is achieved, Polygon will work on becoming the first blockchain to be climate positive.
Polygon's suite of scaling solutions for Ethereum and investments in cutting-edge zero knowledge technology already put it at the forefront of onboarding the next billion users to Web3. This commitment to sustainability is an acknowledgement of the important role we play in the ecosystem and our responsibility to lead by example.
You can read more about how we plan to accomplish this here. Polygon has also commissioned a third-party assessment of our carbon footprint and the results will be published on our blog.
Let's make meaningful change in the world!"

Nel manifesto appena letto, viene esposta la preoccupazione per il futuro del pianeta e il ruolo che la tecnologia può giocare nella sua salvaguardia. Si fa riferimento a Web3 e come possa essere una potente arma per migliorare le condizioni del pianeta in relazione al forte impatto ambientale che la tecnologia

stessa ha avuto fino ad ora. Il testo sottolinea l'impegno di Polygon nel ridurre al minimo l'impronta ecologica delle transazioni sulla propria piattaforma, eliminando prima le emissioni di carbonio, e diventando poi **carbon negative** dal 2022. Inoltre, viene sottolineato che l'obiettivo di Polygon è diventare la prima blockchain ad essere **climate positive**, riconoscendo il proprio ruolo nel sistema e la responsabilità di guidare gli altri per migliorare la sostenibilità.

5.1 Iniziative di sostenibilità di Polygon, con un focus sull'iniziativa "*Polygon Green*"

La blockchain Polygon si sta impegnando a rendere il proprio network sostenibile. Il Manifesto Green, pubblicato da Polygon nel 2022, introduce il motto **"uno smart contract con il Pianeta Terra"**, sottolineando l'importanza di ridurre l'impatto ambientale delle criptovalute e di accompagnare l'ambizione della blockchain con un progetto concreto per preservare l'ambiente per le generazioni future.

Polygon ha dedicato 20 milioni di dollari per diventare **carbon neutral** nel 2022, registrando e calcolando le emissioni di anidride carbonica prodotte da ogni transazione e compensandole con l'acquisto di crediti di carbonio che finanziano progetti per la tutela ambientale e climatica. Polygon ha pianificato di acquistare crediti di carbonio BCT e MCO_2 certificati dal **Verified Carbon Standard** per garantire l'integrità ambientale del commercio di tale valuta.

In collaborazione con **KlimaDAO**, un collettivo decentralizzato di ambientalisti, sviluppatori e imprenditori, Polygon sta incoraggiando i partner del proprio ecosistema a perorare la causa per la tutela dell'ambiente e a facilitare le donazioni per le ONG che combattono il cambiamento climatico.

5.2 Polygon supporta l'elaborazione di transazioni "carbon neutral" e utilizza energia rinnovabile

Negli ultimi anni, la crescente preoccupazione per l'impatto ambientale delle attività umane ha portato alla necessità di sviluppare tecnologie e processi sostenibili. Anche la tecnologia blockchain, utilizzata per la creazione e lo scambio di criptovalute e asset digitali, ha suscitato preoccupazioni per il suo elevato consumo energetico e le conseguenze ambientali.
In questo contesto, Polygon ha adottato una serie di misure per sostenere l'elaborazione di transazioni **"carbon neutral"** e utilizzare energia rinnovabile.
Andiamo quindi ad esaminarle.

5.2.1 Compensazione delle emissioni di carbonio

Polygon ha collaborato con il fornitore di energia rinnovabile *ClimateTrade* per compensare le emissioni di carbonio prodotte dall'elaborazione delle transazioni sulla sua blockchain.
Questa collaborazione prevede l'acquisto dei sopracitati crediti di carbonio per finanziare progetti che riducono le emissioni di carbonio.

Carbon Credits
I crediti di carbonio, anche noti come certificati di riduzione delle emissioni (CRE), sono strumenti utilizzati per misurare e compensare le emissioni di gas a effetto serra (GHG) nell'atmosfera. Rappresentano una misura delle riduzioni di emissioni di carbonio generate da progetti o azioni che contribuiscono a contrastare i cambiamenti climatici.
L'idea alla base è quella di attribuire un valore monetario alle riduzioni delle emissioni di gas serra. Le imprese o le organizzazioni che riescono in questo intento possono ottenere crediti corrispondenti alla quantità di emissioni che sono riuscite a evitare o compensare.
Questi progetti possono essere di diversi tipi, come la promozione dell'energia rinnovabile, l'efficienza energetica, la protezione delle foreste, riduzione delle emissioni in Paesi in via di sviluppo o l'adozione di pratiche agricole sostenibili.
Le aziende che superano i limiti di emissione possono acquistare i crediti dai soggetti che hanno ecceduto i loro obiettivi di riduzione delle emissioni o che utilizzano tecnologie a basse emissioni di carbonio.
Possono essere acquistati da individui, aziende o organizzazioni oppure possono essere scambiati e utilizzati sul mercato volontario o sul mercato regolamentato, a seconda delle normative e delle iniziative in vigore in diversi Paesi. Sul mercato volontario, i crediti di carbonio sono spesso utilizzati da organizzazioni che desiderano adottare pratiche sostenibili o migliorare la propria immagine aziendale in termini di sostenibilità ambientale. Nel mercato regolamentato, i crediti di carbonio possono essere utilizzati per soddisfare obblighi di conformità o regolamentari legati alle emissioni di GHG.
E' importante sottolineare che l'efficacia dei carbon credit è oggetto di dibattito e critiche, poiché alcuni sostengono che il sistema dei crediti di carbonio potrebbe essere soggetto a manipolazioni o che non affronta direttamente la causa principale del cambiamento climatico, cioè la dipendenza dalle fonti di energia fossile.
I carbon credit sono forniti da varie fonti, tra cui enti governativi, organizzazioni internazionali, istituzioni finanziarie, enti di regolamentazione e progetti di riduzione delle emissioni.
Gli enti governativi possono creare e assegnare crediti di carbonio come parte dei loro programmi di mitigazione del cambiamento climatico. Ad esempio, l'Unione Europea può farlo con il suo sistema di scambio di quote di emissione (EU ETS) oppure come organizzazioni internazionali quali le Nazioni Unite, attraverso il loro meccanismo di sviluppo pulito (Clean Development Mechanism, CDM). Questi progetti devono essere verificati e certificati secondo linee guida

specifiche per poter generare crediti di carbonio validi.
In generale, i carbon credit sono riconosciuti e regolamentati da standard e protocolli a livello internazionale, come il Protocollo di Kyoto e l'Accordo di Parigi. Questi standard stabiliscono criteri rigorosi per la misurazione, la verifica e la validazione delle riduzioni delle emissioni, al fine di garantire l'integrità e l'affidabilità dei carbon credit.

5.2.2 Soluzione di mining "Proof of Stake"

Polygon utilizza una soluzione di mining **"Proof of Stake"** chiamata **"Polygon PoS Chain"**. In questo sistema, il processo di convalida delle transazioni viene effettuato da nodi selezionati in modo casuale sulla base della quantità di criptovalute che possiedono e hanno depositato come garanzia. Ciò significa che non è necessario utilizzare risorse energetiche considerevoli per risolvere complicati puzzle matematici, come accade invece nel tradizionale **"Proof-of-Work"**.

5.2.3 Supporto per tecnologie "Layer 2"

Polygon sta lavorando anche su altre soluzioni ecologiche, come ad esempio il supporto per la tecnologia "Layer 2", che consente di eseguire transazioni sulla blockchain in modo più efficiente, utilizzando meno risorse energetiche.

In sintesi, Polygon sta adottando una serie di misure per una blockchain sostenibile, che includono la collaborazione con un fornitore di energia rinnovabile per compensare le emissioni di carbonio prodotte dalle transazioni, il lavoro su una soluzione di mining *Proof of Stake* che utilizza meno energia, e il supporto per tecnologie come **Layer 2** per rendere l'elaborazione delle transazioni sulla blockchain più efficiente ed ecologica. Queste misure mostrano un impegno verso la sostenibilità ambientale e possono essere utili per sviluppare una blockchain sostenibile per il futuro.

6 Applicazioni di Polygon

6.1 Applicazioni che possono essere sviluppate su Polygon, con un focus sui vantaggi in termini di sostenibilità ambientale

Data la sua affidabilità rispetto alla blockchain di Ethereum, Polygon è una scelta interessante per lo sviluppo di DApp e *smart contract*, consentendo di aumentare l'efficienza della rete e ridurre i costi delle transazioni. Polygon supporta diversi linguaggi di programmazione, tra cui *Solidity* e *Vyper*, semplificando il lavoro degli sviluppatori. Grazie alla sua architettura a *sidechain* e alla compatibilità con Ethereum, gli sviluppatori possono utilizzare gli strumenti e le librerie già presenti senza dover riprogrammare tutto da zero. Questo significa che gli sviluppatori possono trarre vantaggio dalla maggiore scalabilità e dall'efficienza della rete, senza sacrificare sicurezza e decentralizzazione. Inoltre, Polygon offre soluzioni di livello enterprise, come la creazione di reti private e la personalizzazione delle soluzioni di sicurezza. Questo la rende una scelta popolare per le aziende che vogliono utilizzare la tecnologia blockchain per migliorare l'efficienza e la trasparenza delle loro operazioni, ad esempio nella gestione della catena di approvvigionamento o nella condivisione di dati sensibili.
Infine, Polygon fornisce una vasta gamma di servizi di sviluppo, tra cui tool di sviluppo, API e documentazione, semplificando il processo di costruzione di DApp sulla piattaforma. Ciò consente agli sviluppatori di concentrarsi sulla creazione di applicazioni innovative e di successo, invece di dover investire tempo e risorse nella costruzione dell'infrastruttura da zero. Alcune delle possibili applicazioni che possono essere sviluppate con Polygon includono:

- Mercati decentralizzati (DeFi) per il trading di criptovalute e token;
- Tokenizzazione degli asset fisici;
- Tracciabilità della filiera di approvvigionamento (*Supply Chain Traceability*);
- Mercati di energia *peer-to-peer*;
- Votazioni e sistemi di governance decentralizzata

Inoltre, Polygon offre un'alternativa più sostenibile dal punto di vista ambientale rispetto a Ethereum, grazie alla sua architettura di rete più efficiente e scalabile. Poiché la maggior parte delle applicazioni blockchain richiedono una grande quantità di energia per funzionare, la riduzione del consumo energetico è diventata un obiettivo importante per molte reti blockchain. Utilizzando Polygon, gli sviluppatori possono creare applicazioni che consumano meno energia e contribuire così a una maggiore sostenibilità ambientale.

7 Ulteriori commenti e conclusione

Polygon è, quindi, una piattaforma blockchain che affronta i problemi di scalabilità della rete Ethereum. Utilizzando un'architettura di *sidechain*, consente una maggiore velocità e capacità di gestione delle transazioni rispetto a Ethereum. Inoltre, si impegna a essere sostenibile dal punto di vista energetico, utilizzando un algoritmo di consenso a prova di scommessa che consuma meno energia.

L'ecosistema di Polygon è ampiamente adottato dagli sviluppatori grazie alla sua scalabilità e facilità d'uso. Le applicazioni decentralizzate su Polygon spaziano dai giochi agli NFT, dai servizi finanziari decentralizzati alle soluzioni per la gestione dei token. Grazie alla sua interoperabilità, offre la possibilità di integrare applicazioni provenienti da diverse blockchain.

Ricordiamo inoltre che Polygon è una soluzione scalabile e sostenibile per la creazione di applicazioni blockchain. La sua architettura di *sidechain* e le iniziative sostenibili lo rendono un ecosistema attraente per gli sviluppatori che desiderano creare e implementare DApp in modo efficiente e rispettoso dell'ambiente. Dalla sezione 5, in cui riportiamo il *manifesto green* per intero, emerge l'interesse di questa blockchain nel creare un sistema totalmente ecosostenibile e che aiuti il pianeta, con il finanziamento di alcuni progetti che riducono le emissioni di carbonio, come i *carbon credits*.

Per completezza, riteniamo opportuno riportare il valore di Polygon nel mercato. Esso si aggira intorno ai 0.90$ (in data 02/06/2023), un valore leggermente inferiore rispetto alle previsioni tenute nel 2021 per il 2023, che prevedevano un valore minimo di circa 1.09$. Inoltre, le previsioni riportano che entro il 2030 Polygon Matic raggiungerà un valore medio di 7.43$, rialzo dovuto al fatto che, entro il 2028, questa blockchain dovrebbe realizzare delle importanti partnership con altre realtà nel mondo delle criptovalute.

Rimanendo in tema di attualità, nelle ultime due settimane l'ottimizzazione del *gas* ha ridotto drasticamente il costo delle transazioni sul network. Se prima un utente DeFi pagava 8.55$ per aggregarle, la scorsa settimana la stessa operazione costava 1.21$.
Tale miglioramento, assieme all'aumento dell'attività sul network, ha reso Polygon zkEMV il *Layer 2 rollup* più conveniente. All'attività segue liquidità, infatti gli asset annessi sono cresciuti di 7 volte tra il 24 aprile e il 29 maggio raggiungendo quota 18M$ e tale crescita ha portato a minori commissioni. Diversamente da Ethereum, il costo dei *rollup* diventa tanto più basso quanti più utenti partecipano, poichè il costo nel generare *proofs* è ammortizzato su tutte le transazioni all'interno di un gruppo o batch. Un risultato importante che conferma come determinate scelte e i principi su cui si fonda Polygon siano conseguenza di una crescita costante a livello economico e sociale.

8 Bibliografia

Introduzione:

- https://academy.binance.com/it/articles/what-is-polygon-matic

Presentazione di Polygon e del contesto in cui si inserisce:

- https://academy.binance.com/it/articles/what-is-polygon-matic
- https://kriptomat.io/it/criptovalute/polygon/cosa-sono-i-polygon/

Problemi di scalabilità delle blockchain:

- https://academy.youngplatform.com/criptovalute/polygon-matic-scalabilita-ethereum/
- https://www.webeconomia.it/proof-of-stake/
- https://wiki.polygon.technology/docs/home/polygon-basics/zkEVM-basics/
- https://academy.bit2me.com/it/che-cos%27%C3%A8-ethereum-virtual-machine-evm/
- https://wiki.polygon.technology/docs/supernets/get-started/what-are-supernets/

Problemi di scalabilità delle blockchain, con un focus su Ethereum:

- https://wiki.polygon.technology/docs/home/polygon-basics/zkEVM-basics/
- https://wiki.polygon.technology/docs/supernets/get-started/what-are-supernets/

Risoluziome dei problemi di scalabilità e congestione della rete:

- https://it.cointelegraph.com/news/polygon-tables-late-march-launch-date-for-its-zkevm-mainnet-beta
- https://blog.bitnovo.com/en/what-is-polygon-the-eth-scalability-solution/?cn-reloaded=1

Problemi ambientali associati alle attività di mining e di elaborazione delle transazioni sulle blockchain:

- https://www.klimadao.finance/blog/polygon-goes-carbon-neutral-via-klimadao
- https://en.wikipedia.org/wiki/Environmental_effects_of_Bitcoin
- https://earthjustice.org/feature/cryptocurrency-mining-environmental-impacts
- https://www.investopedia.com/tech/whats-environmental-impact-cryptocurrency/

- https://www.theguardian.com/technology/2022/sep/29/bitcoin-climate-impact-gold-mining-environmental-damage-cryptocurrency
- https://youngplatform.com/blog/news/polygon-piano-rendere-matic-criptovaluta-green/
- https://it.cointelegraph.com/news/white-house-science-office-looks-at-crypto-s-effect-on-climate-despite-scarce-data

Iniziative sostenibili implementate da alcune blockchain:

- https://www.esg360.it/digital-for-esg/crediti-di-carbonio-e-blockchain-la-nuova-frontiera-delle-criptovalute-green-per-la-sostenibilita-del-business/
- https://toucan.earth/glossary/voluntary-carbon-market-vcm/

Polygon e l'ecosostenibilità:

- https://polygon.technology/blog/our-green-manifesto

Iniziative di sostenibilità di Polygon, con un focus sull'iniziativa "Polygon Green":

- https://youngplatform.com/blog/news/polygon-piano-rendere-matic-criptovaluta-green/

conclusioni

- https://bitcoinwisdom.com/it/polygon-matic-price-prediction/

I CONSUMI ENERGETICI DI BITCOIN

Simona Di Battista, Davide Prestifilippo, Ilaria Zerbini

Politecnico di Torino
Dipartimento di Scienze Matematiche "Giuseppe Luigi Lagrange"
Corso di Laurea in Ingegneria Matematica

BLOCKCHAIN E CRIPTOECONOMIA

I Consumi Energetici di Bitcoin

ELABORATO SCRITTO

Professori:
Bazzanella Danilo
Gangemi Andrea

Gruppo 15:
Di Battista Simona 302689
Prestifilippo Davide 296221
Zerbini Ilaria 300790

Anno Accademico 2022/2023

Indice

1 Introduzione **1**
1.1 I Bitcoin e la PoW 1
1.2 Il dilemma energetico 3

2 I dati di Bitcoin **5**
2.1 Statistiche generali 5
2.2 Sostenibilità del processo di Proof-of-Work in Bitcoin 10
2.3 Danni ambientali e Proof-of-Work: se ci si affidasse a più fonti rinnovabili? 13
2.4 Un confronto con il sistema bancario 14

3 Possibili Soluzioni **19**
3.1 BBCE: un modello di stima sui futuri consumi di Bitcoin 19
3.2 Alps Blockchain 22
3.3 La Proof-of-Stake 23
3.3.1 Protocollo Ouroboros (Cardano) 28
3.3.2 Protocolli delegati: dBFT (Neo) e DPoS (EOS) 29
3.3.3 Protocollo LPoS (Tezos) 30

4 Alcuni opinionisti **31**
4.1 Michael Saylor 31
4.1.1 Confronto con altre BigTech 32
4.1.2 PoW-PoS 32
4.2 Elon Musk 33
4.3 Saifedean Ammous 34
4.4 Mark Carney 36

Riferimenti **38**

CAPITOLO 1

Introduzione

1.1 I Bitcoin e la PoW

Bitcoin è una rivoluzionaria forma di valuta digitale nata nel 2009. Creato da un individuo o un gruppo di persone sotto lo pseudonimo di Satoshi Nakamoto, Bitcoin rappresenta un sistema di pagamento peer-to-peer anonimo e decentralizzato. La sua tecnologia innovativa ha il potenziale per trasformare il concetto di denaro, offrendo un'alternativa decentralizzata e sicura ai sistemi finanziari tradizionali. Questa sua unicità si manifesta difatti attraverso due caratteristiche fondamentali: la Blockchain e la Proof-of-Work. La prima corrisponde ad un registro pubblico e condiviso che tiene memoria di tutte le transazioni effettuate. La Proof-of-Work (PoW) è invece un algoritmo di consenso utilizzato nel contesto del Bitcoin e di altre criptovalute per verificare e convalidare le transazioni all'interno della blockchain. Il suo scopo principale è di agire come "prova di lavoro", ossia dimostrare che un certo utente si è impegnato a svolgere un servizio per la rete. Infatti, chi partecipa alla PoW, deve trovare un valore casuale a 32 bit, chiamato *nonce*, che, quando inserito in una funzione hash[1] deve produrre un risultato inferiore a un determinato *target*. Una volta trovato un *nonce* valido, il blocco viene considerato "minato" e viene diffuso nella rete per la verifica della sua validità.

Chiunque partecipi al processo di Proof-of-Work (PoW) con l'obiettivo di creare un nuovo blocco è chiamato "miner", che in caso di successo viene ricompensato dalla rete con nuovi Bitcoin. Attualmente, nel giugno 2023, ogni blocco minato produce 6.25 Bitcoin, che corrispondono a circa 160 mila euro. Oltre a ciò, vengono aggiunte le cosiddette "fees", ossia le commissioni richieste per includere una transazione specifica nel blocco. Considerando queste commissioni, il compenso totale per il mining può arrivare approssimativamente a 250-300 mila euro.

Spinti della potenziale ricompensa, i miners si dedicano a risolvere il problema crittografico nel minor tempo possibile per superare la concorrenza. Tuttavia, il processo di mining richiede una considerevole potenza di calcolo, che ha portato a un crescente utilizzo dei cosiddetti "ASIC". Acronimo di Application-Specific Integrated Circuit,

[1] Nel caso del Bitcoin, viene utilizzata la funzione hash SHA-256 eseguita due volte successive.

corrispondono ad unità hardware specializzate nel calcolo intensivo richiesto dal mining di Bitcoin. Al fine di rimanere competitivi, i miners devono costantemente incrementare la loro potenza di calcolo, misurata in *hashrate*, ovvero il numero di operazioni crittografiche (*hash*) calcolate al secondo. Questo ha scatenato una corsa all'acquisizione di ASIC sempre più potenti ed efficienti.
Negli ultimi anni infatti, i progressi nella tecnologia dei semiconduttori hanno alimentato una competizione senza fine, registrando miglioramenti esponenziali nell'efficienza e nelle prestazioni degli ASIC. Rispetto ai modelli del 2014, quelli attuali sono circa 36 volte più efficienti dal punto di vista energetico, e sono in grado di eseguire un miliardo di hash al secondo (gigahash [Gh]).

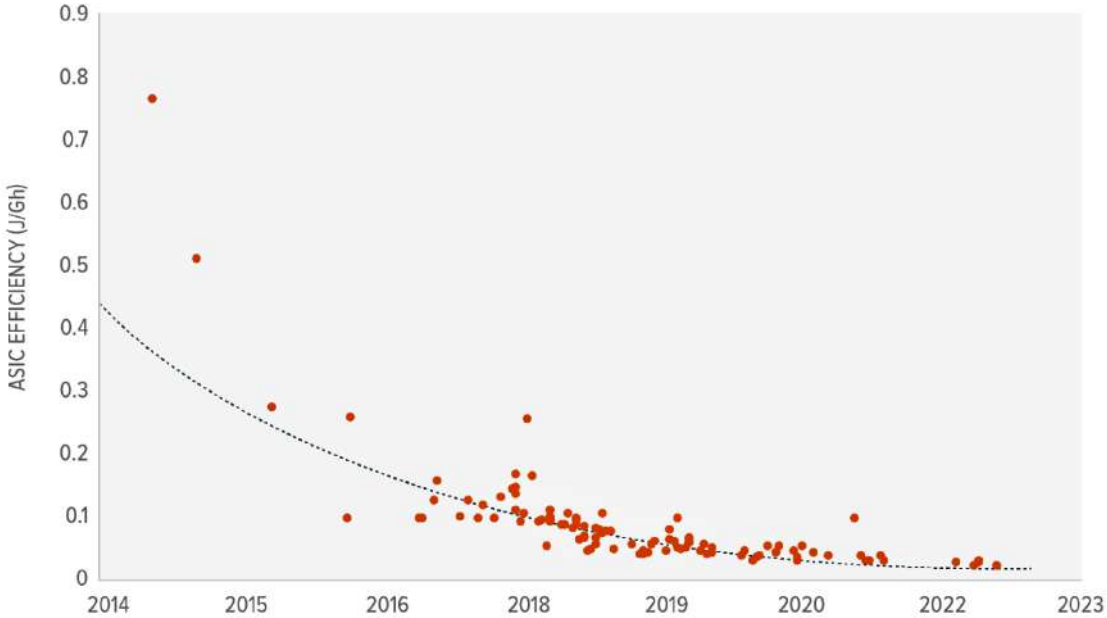


Figura 1.1.1: **Analisi 2014-2022 dell'efficienza degli ASIC (scala esponenziale)**

D'altra parte, per mantenere il tempo di mining costante a circa 10 minuti, il sistema Bitcoin aggiorna il *target* dell'algoritmo crittografico ogni 2016 blocchi, cioè circa ogni 2 settimane. Questo valore tende solitamente a diminuire, in modo tale da rendere la ricerca della soluzione sempre più complicata, in quanto richiede un risultato ancora più piccolo e specifico. Tale fattore di complessità prende il nome di *difficulty*, che rappresenta il rapporto tra il target iniziale di Bitcoin e quello attuale. Il 3 giugno 2023, la cosiddetta *Bitcoin Average difficulty* si attesta approssimativamente a 51 miliardi, registrando un aumento di circa il 71.37% rispetto a giugno dell'anno precedente, nel 2022.

Figura 1.1.2: **Analisi 2018-2023 della Bitcoin Average Difficulty**

Pertanto, la dinamica tra l'evoluzione degli ASIC e l'aggiornamento del target non può proseguire all'infinito, poiché questi dispositivi hardware hanno dei limiti tecnologici intrinseci che non possono essere superati. Questa situazione ha di conseguenza comportato, nel corso degli anni, ricavi sempre più marginali associati all'aumento dell'efficienza della tecnologia ASIC.

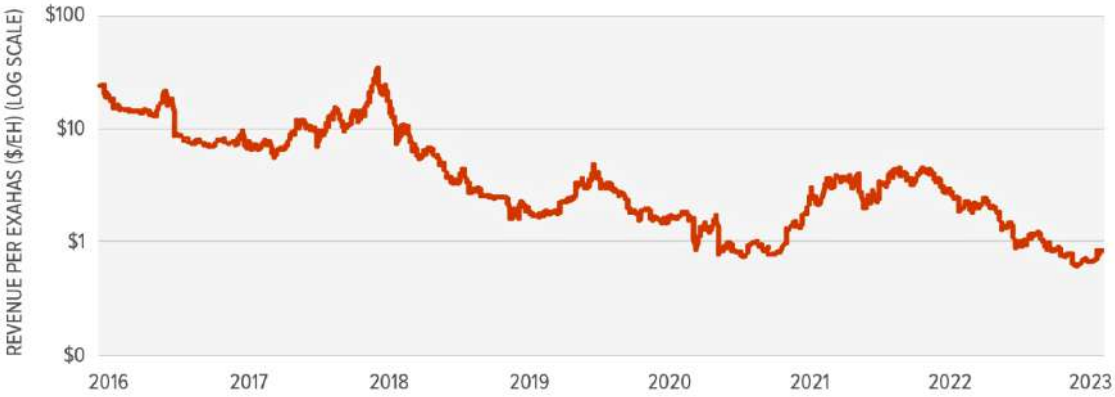


Figura 1.1.3: **Analisi 2016-2023 dei ricavi per exahash degli ASIC (scala logaritmica)**

È importante inoltre considerare che l'aumento della potenza di calcolo degli ASIC richiede anche notevoli investimenti in termini di risorse finanziarie ed energetiche. I minatori devono quindi valutare attentamente il costo dell'hardware e dell'elettricità necessari per il mining, bilanciandoli con i guadagni che possono ottenere. Con la tendenza a guadagni marginali sempre più esigui, nonostante l'investimento in hardware più potenti, i miners stanno iniziando a considerare soluzioni alternative.

1.2 Il dilemma energetico

Ormai Bitcoin risulta essere una realtà affermata, diffusa e sempre più popolare, tuttavia questa sua celebrità ha portato con sé molte critiche principalmente legate alle tematiche ambientali.

Molti descrivono Bitcoin come una delle più grandi rivoluzioni crittografiche atte all'inclusione finanziaria, ma allo stesso tempo come una realtà che si è mossa così

velocemente da aver tralasciato l'entità del suo impatto sull'ambiente.

Proprio a causa del problema "climate change" sempre più pressante, il tema della *sustainability* è al centro delle critiche discusse riguardo la criptovaluta, e le opinioni a questo proposito sono delle più disparate.

Un altro aspetto da considerare è il crescente fenomeno delle "mining pool", ossia gruppi di miner che combinano le proprie risorse di calcolo per aumentare le probabilità di risolvere i problemi crittografici. In questo modo, le ricompense vengono distribuite tra i partecipanti in base al loro contributo computazionale. Da un lato queste offrono diversi vantaggi, come la riduzione della volatilità delle ricompense di mining, un flusso costante di entrate, la condivisione dei costi energetici e l'accesso a strumenti e software specializzati. Le mining pool infatti consentono ai miners con risorse meno potenti di partecipare all'estrazione e di ottenere una parte delle ricompense che sarebbe altrimenti difficile da raggiungere individualmente.
D'altro canto, queste mining pool hanno generato una tendenza contraria alla decentralizzazione, che è ed è stato un principio fondante del Bitcoin fin dalla sua nascita e sviluppo.

Come evidenziato dal grafico sottostante, la maggior parte di queste mining pool si trovano principalmente in Cina, dove è possibile accedere rapidamente alle nuove tecnologie hardware specializzate e beneficiare di costi energetici convenienti.

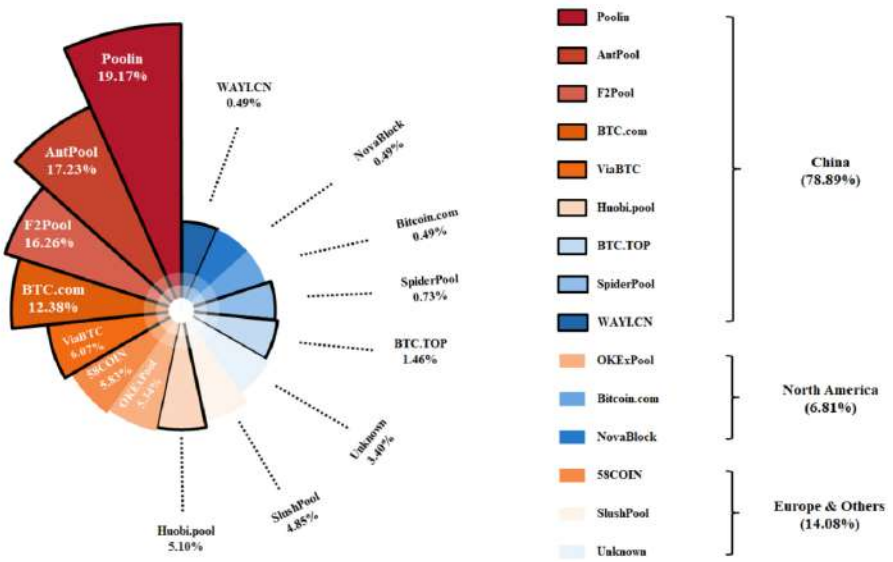


Figura 1.2.1: **Distribuzione delle entità di miners nel mondo e rispettive mining pools**

Ciò che preoccupa maggiormente non è solo la quantità di energia consumata da Bitcoin, ma anche la sua provenienza, dato che la Cina risulta essere in cima alle classifiche delle emissioni di CO_2.

CAPITOLO 2

I dati di Bitcoin

In questa sezione, verranno presentati dati significativi riguardanti Bitcoin, al fine di fornire una panoramica approfondita del suo consumo energetico e valutare i suoi impatti sia energetici che climatici. I dati raccolti consentono di confrontare il consumo energetico di Bitcoin con altre industrie e utilizzi residenziali di elettricità, nonché con l'energia impiegata in prodotti e servizi di uso comune, paesi specifici e settori più tradizionali, come il quello bancario e l'industria dell'oro. Questi confronti contribuiscono a fornire un contesto chiaro e significativo per valutare l'impatto energetico ed ambientale di Bitcoin.

Uno degli aspetti rilevanti che emerge è che la maggior parte dell'elettricità utilizzata per il mining delle criptovalute basate sul protocollo Proof-of-Work, tra cui Bitcoin, proviene da fonti energetiche come il carbone e il gas naturale. Questo scenario ha sollevato legittime preoccupazioni riguardo all'impatto ambientale delle attività di mining e alla sostenibilità di questa tecnologia. È importante comprendere i rischi e le conseguenze di un sistema che richiede un notevole consumo energetico, specialmente quando tale energia proviene da fonti non rinnovabili con un impatto significativo sul clima.

2.1 Statistiche generali

Secondo studi e statistiche continuamente condotti dall'Università di Cambridge, la rete Bitcoin richiede una potenza elettrica annuale stimata a maggio 2023 di 16.98 GW. Questa cifra rappresenta la velocità con cui l'elettricità viene consumata, che, se mantenuta costante al tasso attuale, porta a un consumo totale annuo di elettricità pari a 148.83 TWh. È importante notare che entrambi i valori menzionati rappresentano solo una "istantanea giornaliera" dei dati, che vengono aggiornati ogni 24 ore.

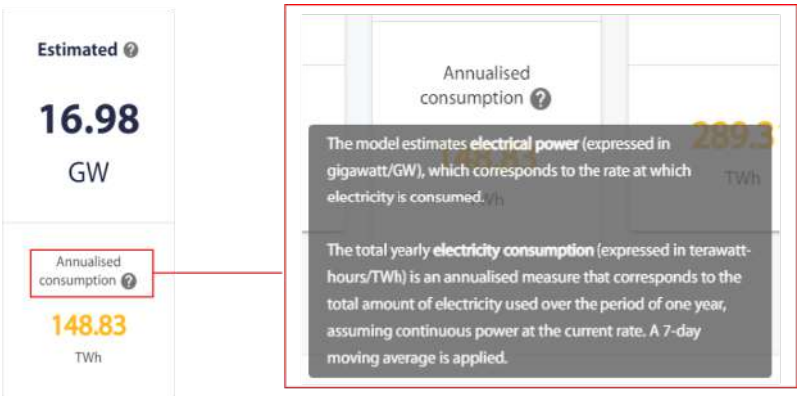


Figura 2.1.1: **Potenza elettrica richiesta dalla rete Bitcoin e il suo consumo di elettricità (annualizzato)**

Grazie a queste stime, è stato possibile creare uno storico dei consumi annui di elettricità e un istogramma relativo al consumo totale di elettricità da parte di Bitcoin nel corso degli anni. Qui i dati di consumo mensili sono ottenuti dalla somma dei contributi giornalieri, calcolati sulla base di un utilizzo costante di energia per 24 ore al giorno, e utilizzando la migliore stima giornaliera della domanda di energia della rete Bitcoin. Il consumo cumulativo (annuale) è la somma dei totali mensili dall'inizio del modello.

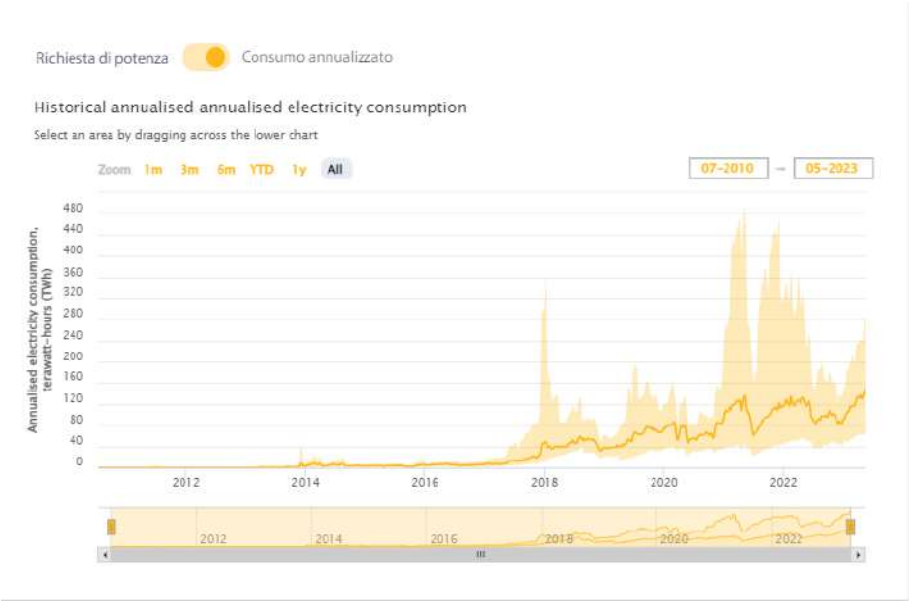


Figura 2.1.2: **Consumo storico (annualizzato) di energia elettrica di Bitcoin**

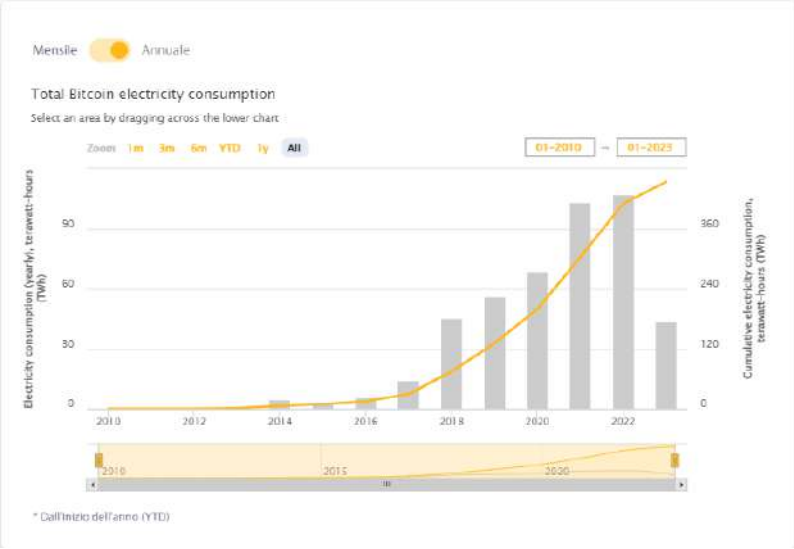


Figura 2.1.3: **Consumo energetico totale di Bitcoin (annuale) da Gennaio 2010 a Gennaio 2023**

Come si può osservare dalle figure sopra riportate, il riferimento temporale parte dal 18 luglio 2010 come data iniziale, poiché non erano disponibili dati di prezzo per il periodo precedente. Tali figure mettono in evidenza un aumento generale del consumo di elettricità dal 2010 fino ad oggi, attribuibile alla progressiva estrazione di nuovi Bitcoin.

Proseguendo lo studio, per rendere il consumo dell'elettricità di Bitcoin più comprensibile, la Figura 2.1.4 confronta tale consumo con altre attività e processi ad alta intensità energetica. Tra questi rientrano il raffreddamento globale dell'aria, la produzione globale di prodotti chimici, nonché la produzione di ferro e acciaio.
Nella Figura 2.1.5, invece, il confronto si sposta sulle emissioni di anidride carbonica equivalente (espressa in $MtCO_2e$), una misura standardizzata che valuta e confronta l'impatto dei diversi gas serra sul cambiamento climatico. L'anidride carbonica equivalente rappresenta la quantità di CO_2 che avrebbe lo stesso effetto di riscaldamento globale del gas considerato. In questo contesto, si può notare che il raffreddamento globale dell'aria ha un impatto significativo, insieme ad altri settori come il turismo o la moda, che rappresentano solo alcuni esempi.

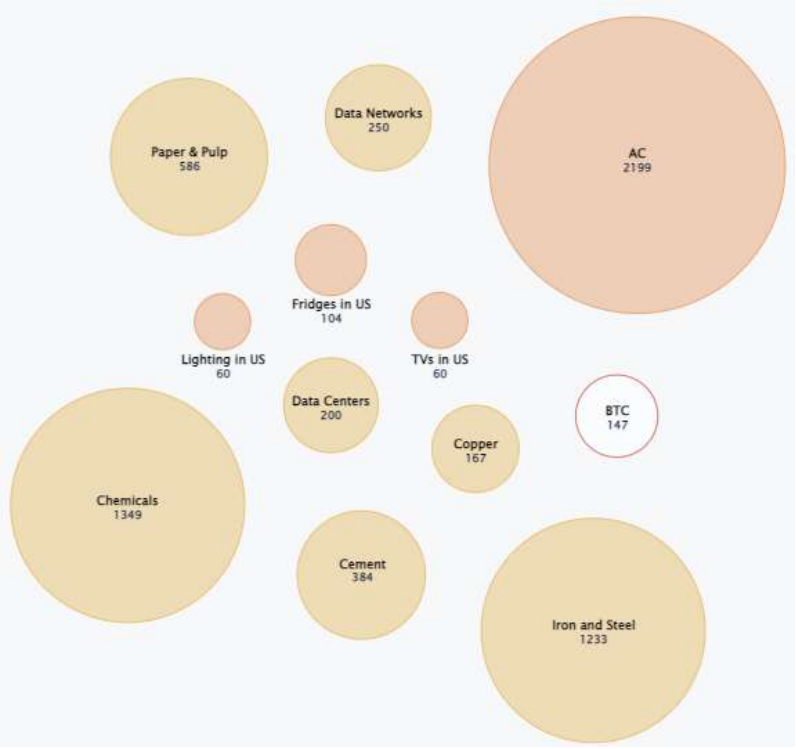


Figura 2.1.4: **Confronto tra il mining di Bitcoin e altri impieghi industriali e residenziali di elettricità**

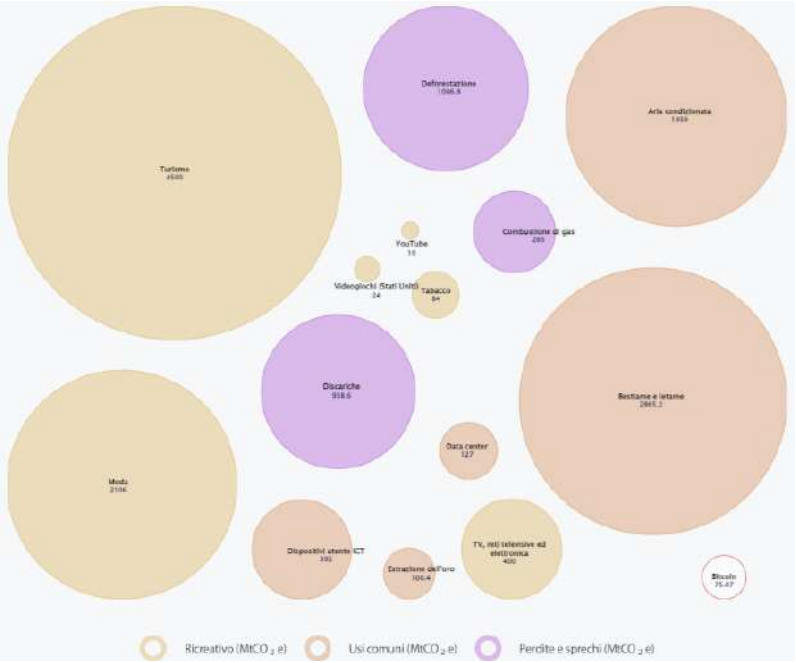


Figura 2.1.5: **Confronto emissioni di Bitcoin e domini di consumo ricreativo, industrie o attività che forniscono prodotti o servizi di uso comune ed emissioni fuggitive e legate ai rifiuti**

La Figura 2.1.6 illustra la proporzione del consumo di Bitcoin rispetto alla produzione e al consumo annuo totale di elettricità a livello mondiale. È importante notare che è inclusa anche una rappresentazione della produzione globale di energia, per considerare il fatto che non tutte le industrie si basano sull'elettricità come fonte energetica.

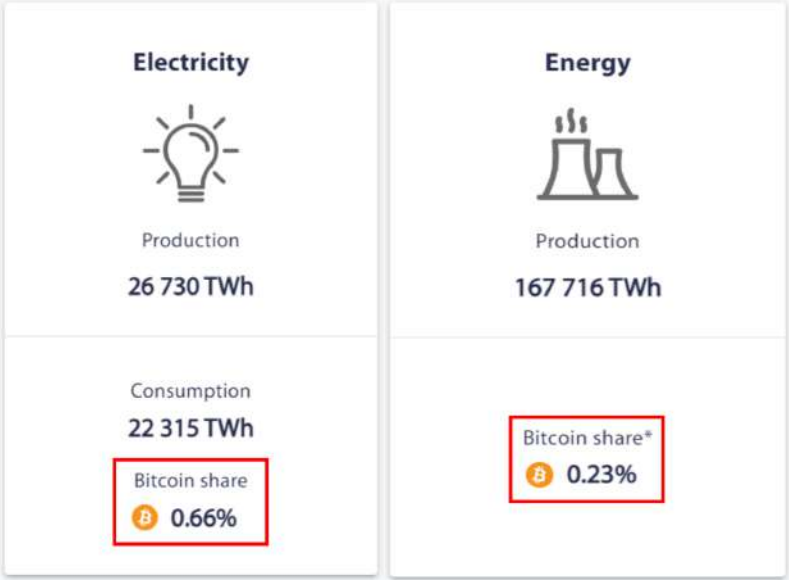


Figura 2.1.6: **Quota di Bitcoin sul totale della produzione e del consumo annuo di energia elettrica a livello mondiale**

Infine, un'altra tipologia di confronto riguarda i consumi di elettricità di Bitcoin tra paesi, spesso utilizzato nel dibattito pubblico per sostenere preoccupazioni sull'entità del consumo. È importante sottolineare che i confronti tra paesi, senza un contesto aggiuntivo, forniscono solo una visione limitata poiché esistono disparità significative tra le diverse nazioni. Il profilo energetico di ogni paese è il risultato di molteplici fattori, tra cui la domanda energetica delle industrie nazionali e dei cittadini, nonché il livello di sviluppo economico e sociale. Pertanto, è necessario considerare questi fattori per comprendere appieno l'impatto del consumo di elettricità di Bitcoin in un determinato contesto nazionale.

Figura 2.1.7: **Confronto consumo di elettricità di Bitcoin con Paesi**

2.2 Sostenibilità del processo di Proof-of-Work in Bitcoin

In questa sottosezione vengono analizzati alcuni segnali empirici relativi ai danni climatici potenzialmente non sostenibili della procedura di Proof-of-Work in ambito Bitcoin. La non sostenibilità del processo è analizzata attraverso tre criteri proposti da Benjamin A. Jones, Andrew L. Goodkind & Robert P. Berrens in "*Economic estimation of Bitcoin mining's climate damages demonstrates closer resemblance to digital crude than digital gold*", datato Settembre 2022.

Un primo criterio consiste nel verificare che l'impatto dei danni climatici stimati per ogni Bitcoin estratto non aumenti a seguito della maturazione dell'industria. Tuttavia, Bitcoin non soddisfa questo requisito: la linea di tendenza non lineare rappresentata di seguito mostra chiaramente un aumento dei danni climatici stimati per unità di moneta. Invece di diminuire con la maturazione dell'industria, tali danni tendono a crescere.

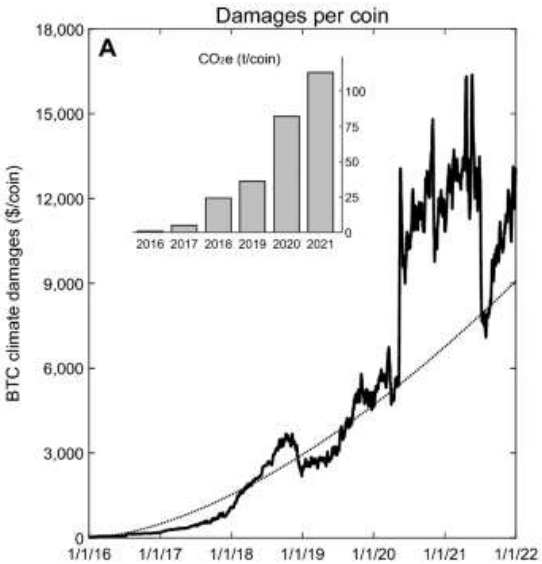


Figura 2.2.1: **Danni climatici generati per moneta da Bitcoin**

Un secondo criterio proposto consiste nel verificare che i danni climatici per unità di Bitcoin estratto non siano mai superiori al valore di mercato della moneta stessa, per qualsiasi periodo di tempo significativo. In questo caso, tra il 2016 e il 2021, i danni climatici del Bitcoin come percentuale del prezzo della moneta hanno superato il 50% del prezzo nella quota giornaliera nel 30.6% dei giorni, e addirittura il 100% nel 6.4% dei giorni. In particolare, nel 2020, il 100% è stato superato per più di un terzo dell'anno, raggiungendo un picco del 156% nel mese di Maggio. Infatti, in quel periodo, si stima che ogni dollaro di valore di mercato del Bitcoin creato abbia comportato 1.56 dollari di danni climatici globali. Pare evidente come Bitcoin fallisca anche il secondo criterio di sostenibilità citato.

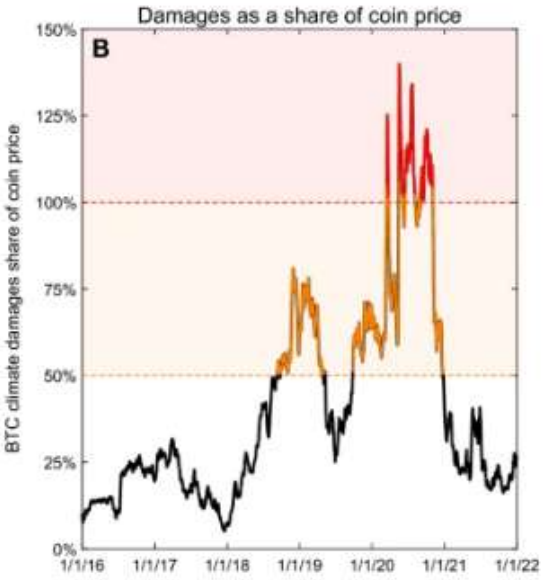


Figura 2.2.2: **Danni ambientali come quota del prezzo della moneta. In rosso le aree in cui il Bitcoin è stato "sommerso"**

Infine, l'ultimo criterio proposto suggerisce di confrontare i danni climatici stimati per ogni moneta estratta con un benchmark percentuale di riferimento dei danni climatici per valore unitario di mercato di altri settori e beni. Il confronto si basa su percentuali di riferimento dei danni per unità di prezzo di mercato (espressi come percentuale del prezzo) causati da Bitcoin nel periodo 2016-2021 rispetto ai danni causati dal ciclo di vita di altre 16 materie prime (per un singolo anno).
Nel caso di Bitcoin, sono stati considerati solo l'utilizzo di energia e le emissioni derivanti dal funzionamento degli impianti di estrazione, ignorando i danni climatici associati al raffreddamento e alla produzione di tali impianti oppure ad altre potenziali fonti di emissioni di anidride carbonica equivalente. Ciò significa che i dati stimati per Bitcoin rappresentano effettivamente un limite inferiore rispetto ai danni causati dall'intero ciclo di vita delle altre 16 commodities prese in considerazione. Per stimare gli impatti climatici relativi a queste ultime, sono state utilizzate le informazioni sul ciclo di vita riportate nella letteratura scientifica e dalle agenzie governative statunitensi, combinate con i dati di prezzo disponibili al pubblico.
Sebbene l'estrazione di Bitcoin non sia dannosa per il clima quanto la generazione di elettricità da carbone, genera danni simili a quelli causati dalla produzione di benzina, la generazione di gas naturale e la produzione di carne bovina, in termini di percentuale rispetto ai prezzi di mercato. Nessuna di queste attività è generalmente considerata sostenibile. Di conseguenza, l'estrazione di Bitcoin attualmente non soddisfa nemmeno questo terzo criterio di sostenibilità.

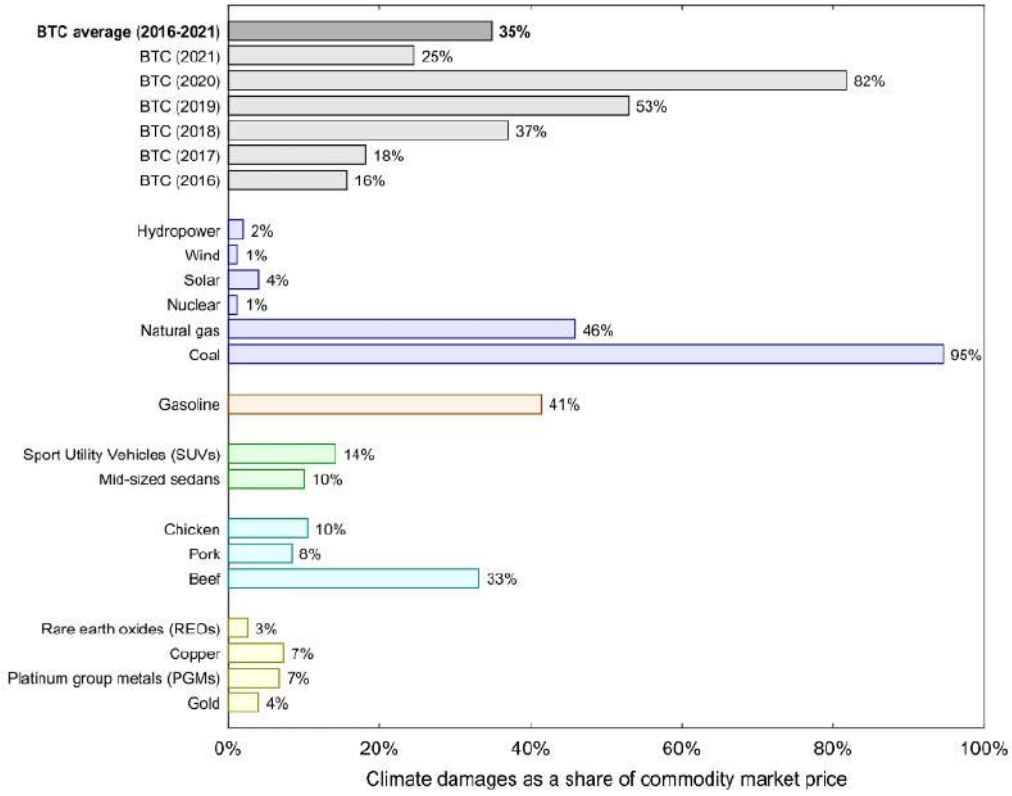


Figura 2.2.3: **Confronto danni climatici per unità del prezzo di mercato (% del prezzo) per Bitcoin con danni climatici dovuti al ciclo di vita di altre 16 altre materie prime**

Durante il periodo temporale analizzato all'interno del paper (2016-2021) è stato stimato un forte aumento delle emissioni di CO_2e (anidride carbonica equivalente) per ogni moneta creata: si ritiene che un Bitcoin estratto nel 2021 emettesse 126 volte più CO_2e di uno estratto nel 2016, passando da 0,9 a 113 tonnellate di CO_2e per moneta. I danni climatici dovuti a tali emissioni, che si sono voluti evidenziare attraverso i criteri proposti, sono stati tutti stimati utilizzando un coefficiente comunemente indicato *costo sociale del carbonio* (SCC), pari a 100 \$/t CO_2e. L'SCC rappresenta il valore attuale stimato dei danni monetari derivanti dall'emissione di una tonnellata aggiuntiva di carbonio oggi, e monetizza le esternalità sociali negative dovute a tali emissioni (la stima dell'SSC utilizzata nello studio è tratta da Pindyck).

I danni climatici per Bitcoin estratto, dunque, sono stati calcolati come moltiplicazione tra emissioni per moneta e SCC:

$$dannipermoneta(\frac{\$}{moneta}) = emissioni(\frac{tCO_2e}{moneta}) \times SSC(\frac{\$}{tCO_2e}).$$

Questi sono stati poi divisi per il prezzo di mercato giornaliero di Bitcoin al fine di ricavare i danni climatici come quota del prezzo della moneta stessa. Tutte le stime dei danni annuali o pluriennali per moneta sono state ponderate per il numero di Bitcoin generati ogni giorno.

2.3 Danni ambientali e Proof-of-Work: se ci si affidasse a più fonti rinnovabili?

Secondo alcune stime dell'Università di Cambridge, la maggior parte dell'elettricità utilizzata per il mining delle criptovalute basate sul Proof-of-Work proviene da fonti di energia non rinnovabile come il carbone e il gas naturale. A livello globale, si stima che il 39% del mining basato sul Proof-of-Work sia alimentato da energia rinnovabile, il che significa che la maggior parte delle fonti di energia utilizzate è non rinnovabile. A causa di questo considerevole utilizzo di energia da fonti fossili, il mining delle criptovalute contribuisce alle emissioni globali di carbonio e ai danni ambientali ad esse correlati.
Studi condotti tra gennaio 2016 e giugno 2018 da Krause e Tolaymat stimano che l'uso di diverse criptovalute, tra cui Bitcoin ed Ethereum, abbia causato emissioni di CO_2 comprese tra 3 e 15 milioni di tonnellate. A titolo di confronto, nel 2018, quantità simili di CO_2 sono state emesse da Paesi come l'Afghanistan, la Slovenia e l'Uruguay.

Inoltre, con l'aumento delle attività di mining nel tempo, si è osservato un notevole aumento delle emissioni di CO_2e per ogni moneta estratta. Nel 2021 è stata effettuata una stima che mostra come un Bitcoin estratto emetta CO_2e in quantità 126 volte superiore rispetto a uno estratto nel 2016. Questa valutazione è stata ottenuta considerando la distribuzione globale dei minatori di Bitcoin, insieme alla composizione del mix energetico locale e i coefficienti di emissione di CO_2e regionali per diverse fonti di generazione. In termini numerici, l'emissione di CO_2e per moneta è aumentata da 0.9 tonnellate nel 2016 a 113 tonnellate nel 2021.

A questo punto, può essere utile riflettere su quale percentuale di utilizzo di fonti di energia elettrica rinnovabile renderebbe la produzione di Bitcoin simile, in termini di impatto sui danni climatici, a quella di materie prime più sostenibili. I risultati suggeriscono che se la quota di elettricità da fonti rinnovabili, nel periodo 2016-2021 analizzato, aumentasse dal 38.5% all'88.4% (con un ulteriore 5.2% dall'energia nucleare) - un aumento del 129% - i danni climatici come percentuale del prezzo di Bitcoin diminuirebbero dal 35% al 4%, avvicinandosi ai danni climatici dell'energia solare o dell'oro.
Al contrario, in assenza di un aumento significativo della quota di elettricità da fonti rinnovabili utilizzata nel mining, i danni climatici causati dal Bitcoin rimarranno un caso eccezionale rispetto alle materie prime più sostenibili.

2.4 Un confronto con il sistema bancario

Dato l'elevato livello di trasparenza di Bitcoin, è possibile valutare facilmente il suo consumo energetico in confronto ad alcuni settori tradizionali, come già affrontato in precedenza nelle figure 2.1.4 e 2.1.5.
Oltre ad essi, Bitcoin viene frequentemente paragonato sia al sistema bancario per quanto riguarda i pagamenti, il risparmio e le transazioni, sia all'oro come riserva di valore non governativa. Tuttavia, è importante sottolineare che Bitcoin rappresenta una tecnologia fondamentalmente innovativa e non può essere considerato un sostituto esatto di nessun sistema precedente.
Il sistema bancario globale si caratterizza per un'ampia infrastruttura che comprende filiali, server centrali, sportelli automatici, reti di comunicazione e molto altro ancora. Richiede inoltre una quantità significativa di carta e risorse fisiche per la produzione di banconote e carte di credito, oltre alla logistica necessaria per la loro distribuzione e gestione.

Di conseguenza, il sistema bancario non fornisce dati precisi sul consumo di elettricità, permettendo solo di effettuare stime che possono essere confrontate con il modello Bitcoin. Secondo un'analisi condotta nel 2021 da *Galaxy Digital Holdings*, le quattro principali aree che contribuiscono al consumo di elettricità nel sistema bancario, con dati sufficienti per effettuare stime accettabili, [1] sono:

1. I centri elaborazione di data bancari (*data center*);
2. Le filiari bancarie (*bank branches*);
3. Gli sportelli bancari (*ATM)*;
4. Pagamenti elettronici attraverso *card networks*.

Data Center La *Bank of America Corporation* è l'unica banca che comunica il numero dei suoi data center, che ammontano a 23. Tuttavia non vengono divulgati i dettagli riguardo alla loro dimensione e alla quantità di energia che richiedono, ma è possibile fare stime basate su dati di settore.

L'area media di un data center corrisponde a circa 6968 metri quadrati e richiede un consumo energetico medio di circa 4306 Watt al metro quadrato. È importante notare che queste stime si riferiscono a data center in generale e potrebbero non riflettere esattamente la situazione dei data center bancari.

In termini temporali, operano ininterrottamente 24 ore al giorno, 7 giorni alla settimana, per 52 settimane all'anno, con un totale finale di 8760 ore.
Pertanto, il consumo energetico annuo della *Bank of America Corporation* può essere stimato come:

[1] Alcuni dati presentati di seguito sono stati convertiti dal sistema di misurazione americano a quello internazionale per favorire una migliore comprensione.

$$E_{BAC}^{D.C.} = 23 \cdot 6968\ m^2 \cdot 4306\ \frac{W}{m^2} \cdot 8760\ h \approx 6.04\ \frac{TWh}{yr} \tag{2.1}$$

Per quanto riguarda invece la domanda energetica dei data center delle prime 100 banche mondiali, alcuni esperti propongono un'ipotesi di correlazione lineare tra il consumo di elettricità stimato in precedenza e i depositi totali. Questi ultimi ammontano a 70972.10 miliardi di dollari, mentre per la *Bank of America Corporation* raggiungono i 1795.48 miliardi di dollari.

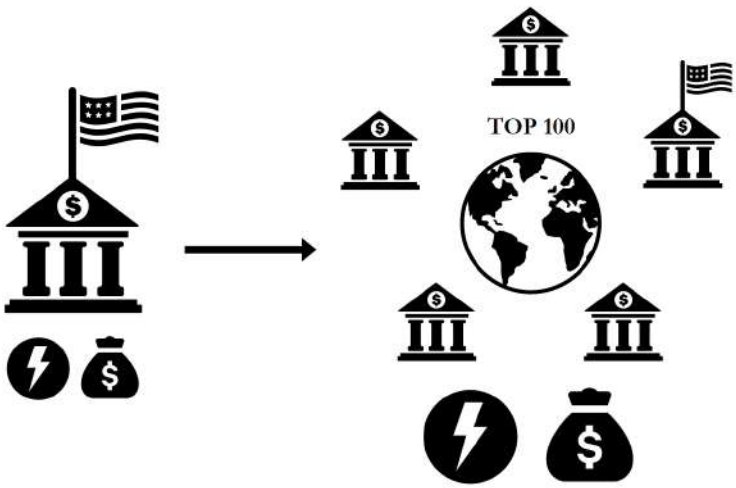


Figura 2.4.1: **Modello lineare depositi-consumi tra la *Bank of America Corporation* e le prime 100 banche mondiali**

È pertanto possibile stimare il contributo energetico dei data center relativo alle prime 100 banche mondiali.

$$\begin{gathered} dep_{BAC}\ :\ dep_{TOT}\ =\ E_{BAC}^{D.C.}\ :\ E_{TOT}^{D.C.} \\ E_{TOT}^{D.C.} = \frac{70972.10\ B\$}{1795.48\ B\$} \cdot 6.04\ \frac{TWh}{yr} \approx 238.75\ \frac{TWh}{yr} \end{gathered} \tag{2.2}$$

Bank Branches Si stima che uno sportello bancario operi per 9 ore al giorno, 5 giorni alla settimana, per 50 settimane all'anno, per un totale di 2250 ore.

Una filiale bancaria è considerata una piccola impresa e per stimare il consumo medio di elettricità a livello globale si possono prendere in considerazione i dati relativi a quattro paesi che rappresentano tra loro differenti realtà: Stati Uniti, Messico, Regno Unito e Cina.

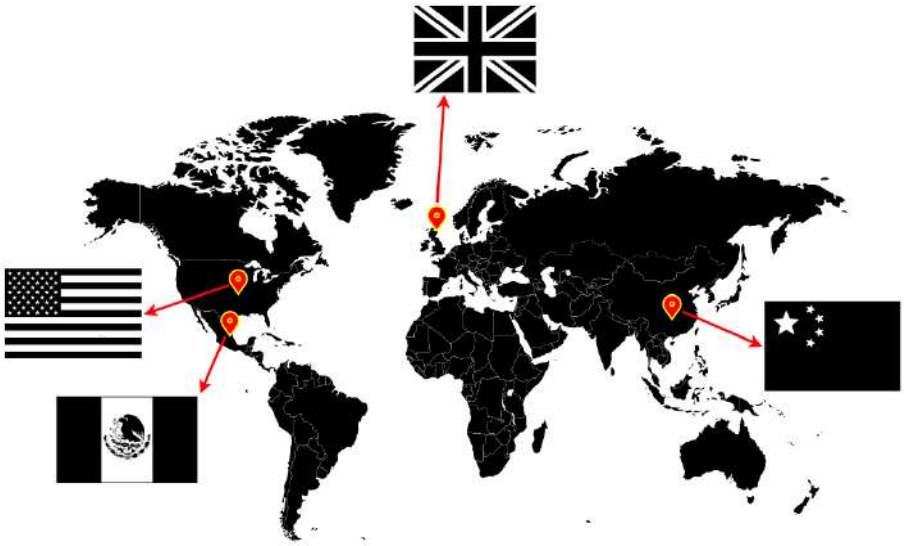


Figura 2.4.2: **Paesi modello per stima media delle filiali bancarie**

In base ai dati disponibili e alle stime relative ai consumi residenziali, insieme ad altre informazioni, si è stimato che il consumo globale annuo di elettricità delle filiali bancarie ammonti a 19.71 TWh/yr.
Tuttavia, è importante notare che questa analisi non tiene conto del consumo di gas nelle filiali bancarie né del consumo di elettricità e gas di tutti gli altri edifici collegati alle loro pratiche finanziarie.

ATM Il sistema bancario non fornisce dati specifici sull'energia elettrica necessaria per il funzionamento degli sportelli automatici. Si può pertanto stimare questa cifra moltiplicando il numero totale di ATM per la domanda energetica tipica e le ore di funzionamento di uno singolo.

Un bancomat funziona in media 24 ore al giorno, 7 giorni alla settimana, per 52 settimane all'anno, per un totale di 8760 ore. Inoltre, la sua richiesta energetica media è di circa 145 Watt.

Secondo alcuni dati del 2021, nel mondo erano presenti 39.69 sportelli automatici per ogni 100 mila adulti. Considerando le diverse leggi e usanze nei paesi, le persone allora riconosciute adulte nel mondo corrispondevano a circa 6.13 miliardi.

Dunque, è possibile stimare che il consumo energetico globale annuo degli sportelli automatici sia:

$$N = \frac{3969\ ATMs}{100000\ adults} \cdot 6.13 \cdot 10^6\ adults \approx 2.43 \cdot 10^6\ ATMs$$
$$E_{TOT}^{ATM} = N \cdot 145\ W \cdot 8760\ h \approx 3.09\ \frac{TWh}{yr} \tag{2.3}$$

Card networks Come precedentemente menzionato, un data center bancario opera per 8760 ore all'anno e richiede un consumo energetico medio di circa 4306 Watt per metro quadrato.

L'unica rete di carte che fornisce alcuni dati pubblicamente disponibili è VISA, che dichiara di gestire cinque data center in tutto il mondo. Sebbene VISA non fornisca informazioni specifiche sulla domanda di elettricità di ciascuno, ne divulga indicativamente la superficie.

VISA central US Denver	6503 m^2
VISA Eastern US Ashburn	13006 m^2
VISA United Kingdom	929 m^2
VISA Singapore	929 m^2

Di conseguenza, si può stimare la sua domanda energetica totale.

$$E_{VISA}^{C.N.} = A_{TOT} \cdot 4306 \, \frac{W}{m^2} \cdot 8760 \, h \approx 0.84 \, \frac{TWh}{yr} \tag{2.4}$$

Nel 2021, VISA ha elaborato 185.5 miliardi di transazioni su un totale di 441 miliardi. Utilizzando queste informazioni e un modello lineare simile ai data center, la valutazione sul consumo energetico globale annuo richiesto per il funzionamento di tutte le reti di carte sia:

$$\begin{gathered} tran_{VISA} \; : \; tran_{TOT} \; = \; E_{VISA}^{C.N.} \; : E_{TOT}^{C.N.} \\ E_{TOT}^{C.N.} = \frac{441 \; \cdot \; 10^9}{185.5 \; \cdot \; 10^9} \cdot 0.84 \, \frac{TWh}{yr} \approx 2.00 \, \frac{TWh}{yr} \end{gathered} \tag{2.5}$$

Utilizzando le informazioni pubblicamente disponibili, è stato possibile stimare in modo approssimativo che il sistema bancario nel 2021 abbia utilizzato circa 263.55 TWh/yr di energia, pari alla somma dei quattro contributi prima calcolati. Questi dati possono essere confrontati con il consumo energetico dell'industria dell'oro e di Bitcoin nello stesso periodo, rispettivamente pari a 240.61 ed a 81.51 TWh/yr.

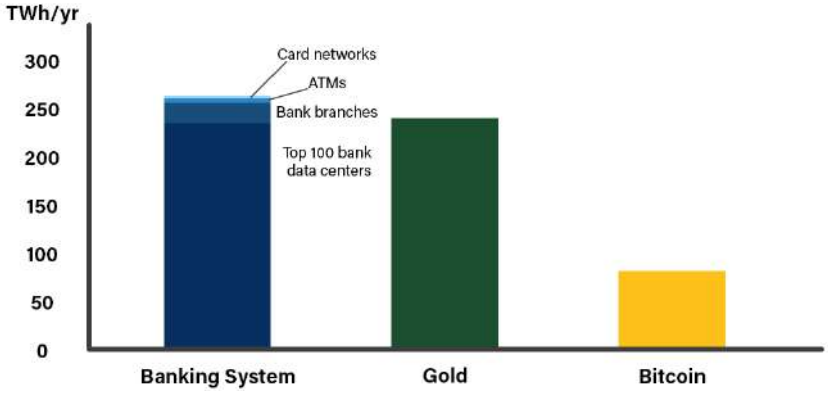


Figura 2.4.3: **Consumo energetico annuo stimato nel 2021 per il sistema bancario, l'industria dell'oro e Bitcoin**

Ottenere una stima precisa del consumo energetico dell'intero settore bancario richiederebbe una dichiarazione da parte delle singole banche, cosa che attualmente non avviene.

Il sistema finanziario tradizionale è una complessa gerarchia di controparti e regolamenti intermedi. Le reti di carte di credito sono efficienti per il trasferimento rapido di pagamenti, ma dipendono dal sistema bancario per il regolamento, il quale a sua volta è legato alle banche centrali per il regolamento finale, e quindi al sistema della valuta nel suo complesso.

Inoltre, valutare l'utilità del sistema bancario esclusivamente in base al suo consumo energetico sarebbe riduttivo, poiché si trascurerebbero i vantaggi derivanti dal trasferimento di grandi quantità di denaro che esso permette.

Sebbene possa sembrare logico confrontare il sistema bancario e Bitcoin, questi due sistemi hanno diverse proprietà di scalabilità. Il primo scala con il conteggio delle transazioni, richiedendo un'infrastruttura aggiuntiva man mano che il volume delle transazioni aumenta. Al contrario, il consumo energetico della criptovaluta non scala in base al numero di transazioni, ma è determinato dall'economia della rete stessa.

Questo ed altri aspetti potrebbero giustificare le differenze energetiche tra questi due settori. Tuttavia, ciò non toglie che, nonostante il consumo energetico di Bitcoin sia inferiore, non sia comunque trascurabile e possa continuare a causare un impatto ambientale disastroso nel lungo termine. Pertanto, è consigliabile ridurre tale impatto orientandosi verso nuove soluzioni.

CAPITOLO 3

Possibili Soluzioni

Molto spesso, l'avvento di una rivoluzione è accompagnato da un grande entusiasmo e fermento, al punto da far dimenticare le eventuali problematiche che questa innovazione potrebbe comportare.

Nel caso di Bitcoin, il successo e l'interesse dei mercati sono da tempo accompagnati da critiche riguardo alle sue politiche, che alcuni ritengono non abbastanza sostenibili dal punto di vista ambientale. Al fine di affrontare questa problematica e renderla più nota al pubblico, nel corso degli anni sono emerse nuove realtà e soluzioni.

3.1 BBCE: un modello di stima sui futuri consumi di Bitcoin

Fra i vari papers e articoli sul tema, *Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China* presenta la costruzione di BBCE, un modello con lo scopo di predire i futuri consumi di Bitcoin in 4 diversi scenari:

1. **BENCHMARK SCENARIO** (BM), in cui si suppone che le politiche energetiche relative alle criptovalute basate sulla blockchain, come Bitcoin, non cambino rispetto a quelle attualmente in uso;

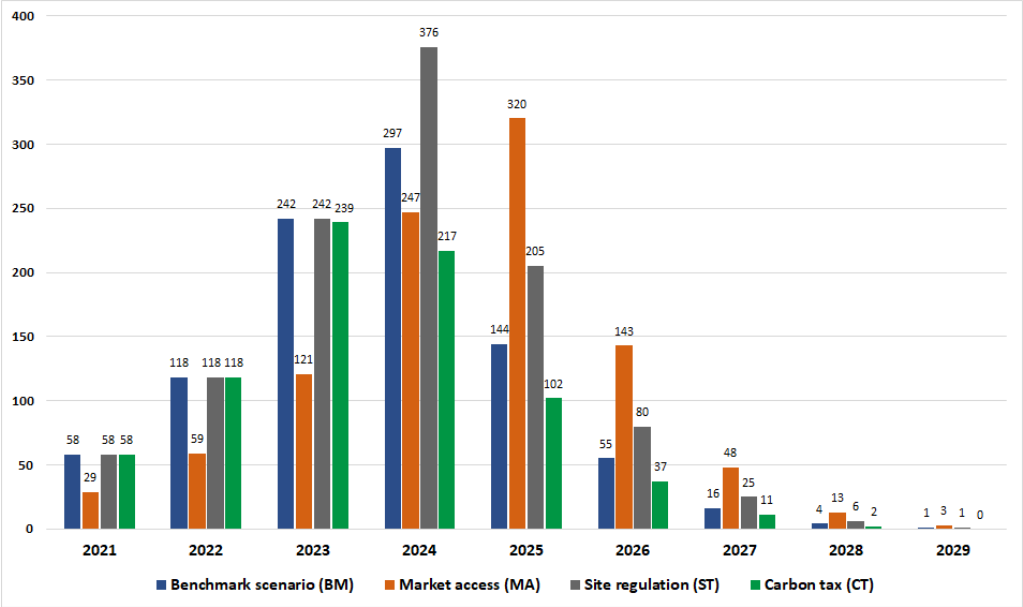
2. **MARKET ACCESS** (MA), nel quale ai miners che mantengono una bassa efficienza energetica è vietato di entrare nel mercato cinese dei Bitcoin;

3. **SITE REGULATION** (ST), dove circa la metà dei miners collocati in aree in cui l'energia è basata sul carbone sono persuasi a spostarsi in aree dove è possibile sfruttare risorse green;

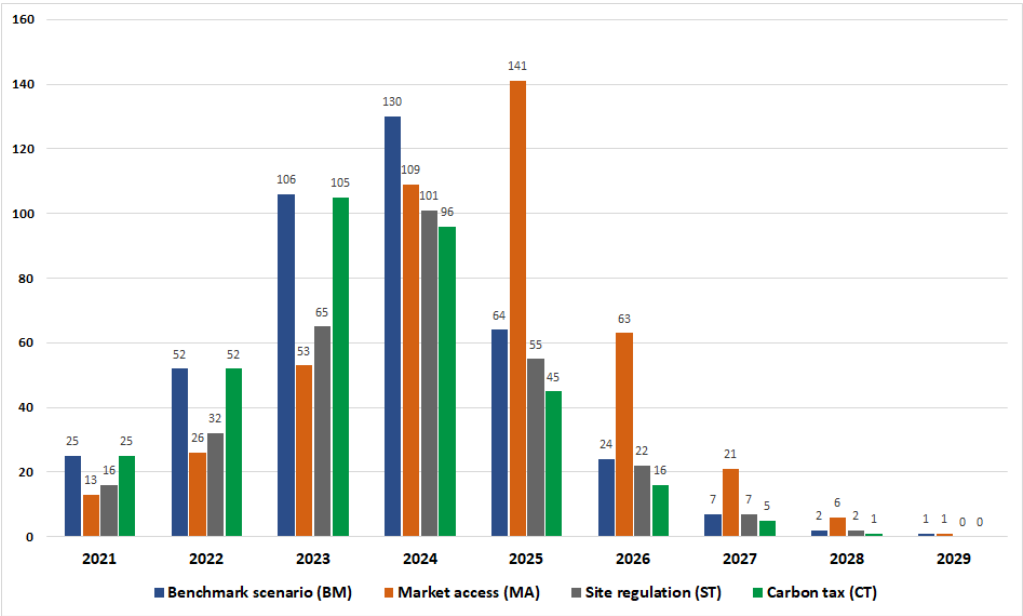
4. **CARBON TAX** (CT), secondo cui la tassa sul carbone è raddoppiata.

Gli autori stessi citano varie fonti a sostegno della loro ipotesi, alcune più focalizzate sul consumo energetico di Bitcoin, equiparato a quello di stati di piccola-media dimensione come Irlanda, Bangladesh e Danimarca, altre più interessate alle emissioni

di CO_2, che stimano raggiungere i 13 milioni di tonnellate metriche. Allo scopo di confermare le stime già fatte e di migliorare quelle future, il modello BBCE è finalizzato a predire e valutare le emissioni di carbonio e i consumi energetici di Bitcoin nei quattro scenari dal 2014 al 2030. Di seguito sono riportati i grafici ottenuti dalle simulazioni:



(a) *Consumi energetici*



(b) *Emissioni di carbonio*

Figura 3.1.1: **Stime dati di Bitcoin tramite simulazione BBCE 2021-2029**

Le stime prodotte dalla simulazione e riportate nei grafici in figura 3.1.1, prevedono che Bitcoin supererà alcuni fra gli stati più sviluppati in entrambe le categorie di

consumo.
In particolare, nello scenario BM, si stima che il consumo energetico di Bitcoin abbia un picco nel 2024, con il valore di 296.59 TWh per anno, superiore a quello registrato per Italia e Arabia Saudita nel 2016, figura 3.1.2, posizionandosi al dodicesimo posto nella classifica mondiale.
Nello scenario CT il consumo si abbassa leggermente, per effetto della politica di tassazione più stringente, mentre nei restanti scenari MA e ST i dati risultano perfino peggiori della stima BM, arrivando a 350.11 TWh sempre nel 2024.
Per quanto riguarda le emissioni di carbonio, troviamo stime consistenti a quelli del consumo energetico, tanto da riportare il picco nello stesso anno per lo scenario BM, che ammonta a 130.50 milioni di tonnellate metriche. Per fare un confronto con i dati di alcuni stati, supererebbe le emissioni della Repubblica Ceca e del Qtar registrare nel 2016, figura 3.1.2, classificandosi al trentaseiesimo posto worldwide. Tuttavia, contrariamente all'andamento del consumo energetico, le emissioni di CO_2 negli scenari CT e SR si ridurrebbero significativamente, probabilmente grazie all'effetto delle politiche suggerite.

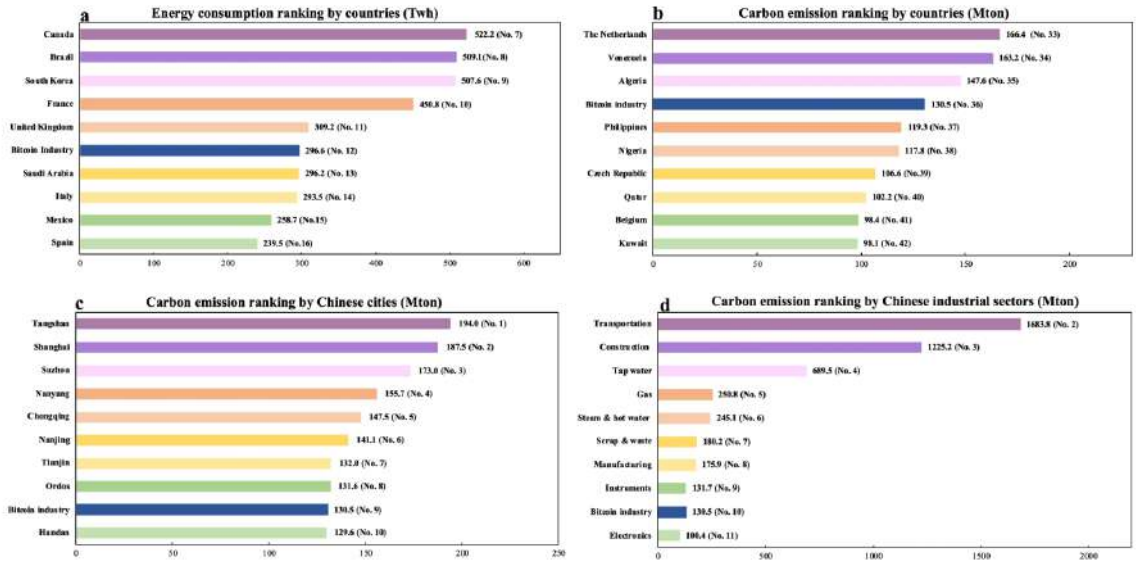


Figura 3.1.2: **Istogrammi di confronto del picco massimo di consumi di Bitcoin con le emissioni di nazioni, città, e settori industriali cinesi. I valori energetici per (a) sono ottenuti da *www.cia.gov*, mentre le emissioni di carbonio in (b) da *www.globalcarbonatlas.org*. I dati relativi alle città cinesi in (c) e i settori industriali (d) provengono da *www.ceads.net*. A causa di alcuni missing values nei dati più recenti, sono riportati i valori del 2016**

Pertanto, il pattern emerso dalle simulazioni fa presagire che Bitcoin possa rappresentare un vero ostacolo al raggiungimento degli obiettivi di riduzione delle emissioni in Cina. Inoltre il trend in salita mostrato dagli istogrammi continuerà a rimanere tale finché, a parere degli autori, il mining rimarrà proficuo nello stato, proprio a causa del meccanismo competitivo della PoW, che ormai richiede risorse sempre più

avanzate ed energy-consuming.
Infine le stime risultano essere consistenti rispetto al trend passato per entrambi i campi di studio, come riportato di seguito in figura 3.1.3.

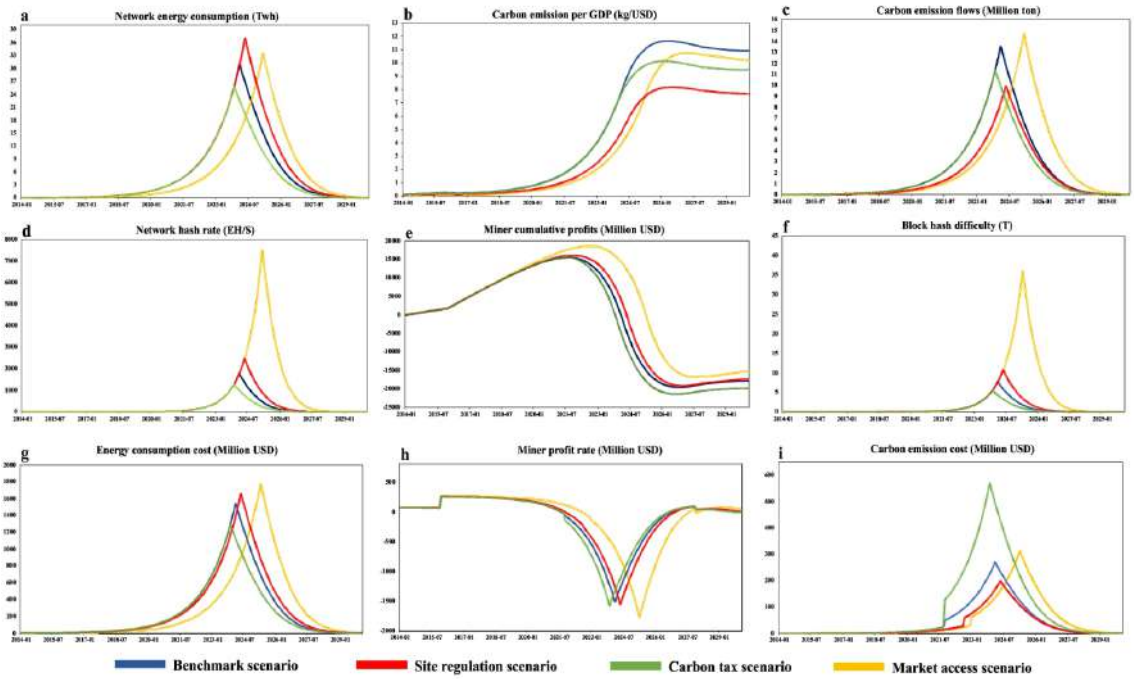


Figura 3.1.3: **Consumi della rete mensili (a), emissioni di carbonio per GDP (b), flussi di emissioni di carbonio (c), hash rate della rete (d), profitto cumulativo dei miners (e), difficoltà di hash (f), costi per del consumo energetico (g), rate di profitto dei miners (h), costo emissioni di carbonio (i) simulati rispetto gli scenari di BBCE**

3.2 Alps Blockchain

Nel marzo 2023 l'asset menager Azimut ha proposto un club deal per investire in *Alps Blockchain*, un'impresa trentina specializzata nello sviluppo in ambito mining. Lo scopo di Alps è produrre potenza di calcolo per la blockchain usando energia verde.
L'azienda è nata nel 2018, una delle prime nel suo campo in Italia, basata sull'intenzione di innovare la gestione e collocazione dei data center adibiti al mining, concentrandosi in zone dove risulterebbe possibile alimentarli con fonti sostenibili, ad esempio vicino a centrali idroelettriche.
Ad oggi Alps ha realizzato ben 20 data center in Italia, i quali ospitano circa 4000 miners e hardware dedicati al mining, e questi si aggiungono quelli dislocati all'estero, in numero sempre crescente.

3.3 La Proof-of-Stake

La Proof-of-Stake (PoS) è un algoritmo di consenso proposto nel 2011, che potrebbe rappresentare una valida alternativa e una possibile soluzione ai problemi associati alla Proof-of-Work. In questo nuovo protocollo, la risoluzione del problema crittografico viene sostituita da un meccanismo in cui un nodo della rete, chiamato *validator*, deposita una quota delle proprie criptovalute come impegno per garantire la validità delle transazioni da inserire nella blockchain.

Il nodo selezionato per convalidare il blocco è scelto seguendo criteri che variano da criptovaluta a criptovaluta, seguendone la struttura e gli ideali. Alcuni fra questi sono: la quantità di valuta posseduta, il tempo di partecipazione alla rete e la velocità di utilizzo della valuta stessa.

Questo protocollo trasforma il processo di mining in un processo di partecipazione che mira a decentralizzare ulteriormente la rete, corrispondendo all'obiettivo principale della tecnologia blockchain che, a seguito del crescente fenomeno delle mining pool, secondo alcuni non è più al centro delle politiche di Bitcoin.

Infatti, al momento del lancio nel 2009, chiunque con un normale computer aveva la possibilità di competere con altri minatori, cercando di risolvere la Proof-of-Work e ottenere la convalida del blocco successivo. Tuttavia, a causa dell'aumento della *difficulty*, i piccoli miners hanno sempre meno possibilità di emergere come vincitori in questa competizione, motivo per cui si sono gradualmente aggregati nelle strutture di mining pool. Come soluzione alle problematiche precedentemente menzionate, è emersa la Proof-of-Stake, con l'obiettivo di ripristinare uno scenario "democratico" di accesso per i partecipanti alle diverse mansioni nella rete.

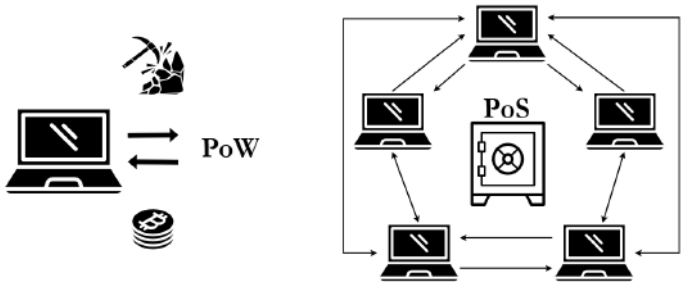


Figura 3.3.1: **Proof-of-Work versus Proof-of-Stake**

Inoltre, scegliendo la PoS, la sicurezza della rete può essere compromessa solo se un nodo *validator* possiede il 51% di tutte le monete. Attualmente, si ipotizza che questo tipo di attacco non sia attuabile, poiché comporterebbe una significativa diminuzione del valore della moneta, causando ingenti perdite economiche per l'attaccante stesso.

Tra il 2017 e il 2018, diverse piattaforme importanti si erano sviluppate utilizzando meccanismi di consenso di tipo Proof-of-Stake, come Cardano (ADA), EOS, Neo

(NEO) e Tezos (XTZ).[1] Nel grafico sottostante viene confrontato il rendimento percentuale di queste piattaforme con i sistemi Proof-of-Work di Bitcoin (BTC) ed Ethereum (ETH) nel periodo 2020-2021. È interessante notare che, nonostante le differenze nei protocolli, le criptovalute PoS hanno registrato un rendimento economico percentuale quasi paragonabile o addirittura superiore a Bitcoin.

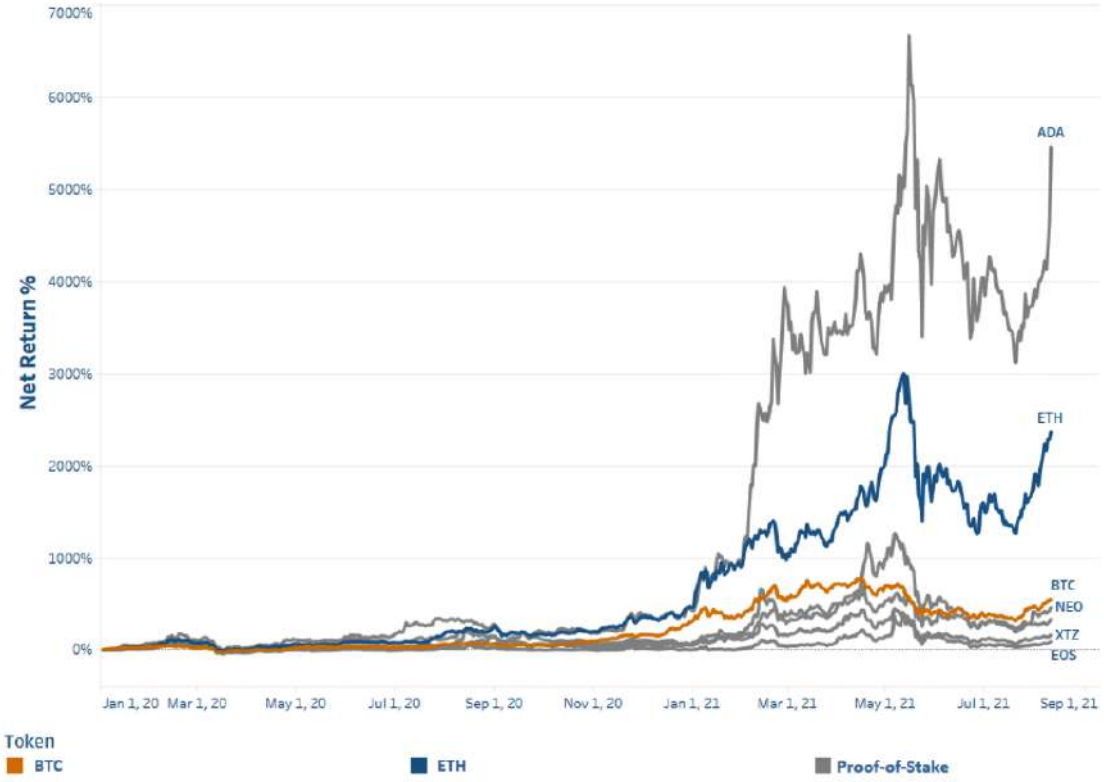


Figura 3.3.2: **Rendimenti negli anni 2020-2021 di alcuni sistemi PoW (BTC, ETH) e PoS (ADA, NEO, XTZ, EOS).**

Tuttavia, è lecito considerare che questi dati potrebbero non confrontare direttamente i due diversi protocolli, ma piuttosto lo sviluppo di criptovalute più recenti. Bitcoin ha avuto origine nel 2008, quindi nel periodo di analisi di 20 mesi era una realtà più consolidata rispetto alle altre criptovalute, che sono state introdotte molti anni dopo. Ad esempio, all'inizio del 2020, Cardano era la tredicesima criptovaluta per capitalizzazione di mercato, con poco più di 900 milioni di dollari, corrispondenti allo 0.67% di quella di Bitcoin. Verso la fine del 2021, grazie al suo sviluppo, ha registrato una crescita economica di quasi l'8000%, diventando la terza criptovaluta per capitalizzazione di mercato, rispetto al 505% di Bitcoin, che era una criptovaluta più stabile. Tuttavia, la capitalizzazione di mercato di Cardano rappresentava ancora solo una piccola parte di quella di Bitcoin, pari all'8.70%. Lo stesso discorso potrebbe applicarsi alle altre criptovalute menzionate, sia in ambito di capitalizzazione di mercato che di prezzo di valuta.

[1]Cardano: 2017. EOS: 2017. Neo: 2017, già nota nel 2014 come Antshares. Tezos: 2014, ma con il lancio principale nel 2018.

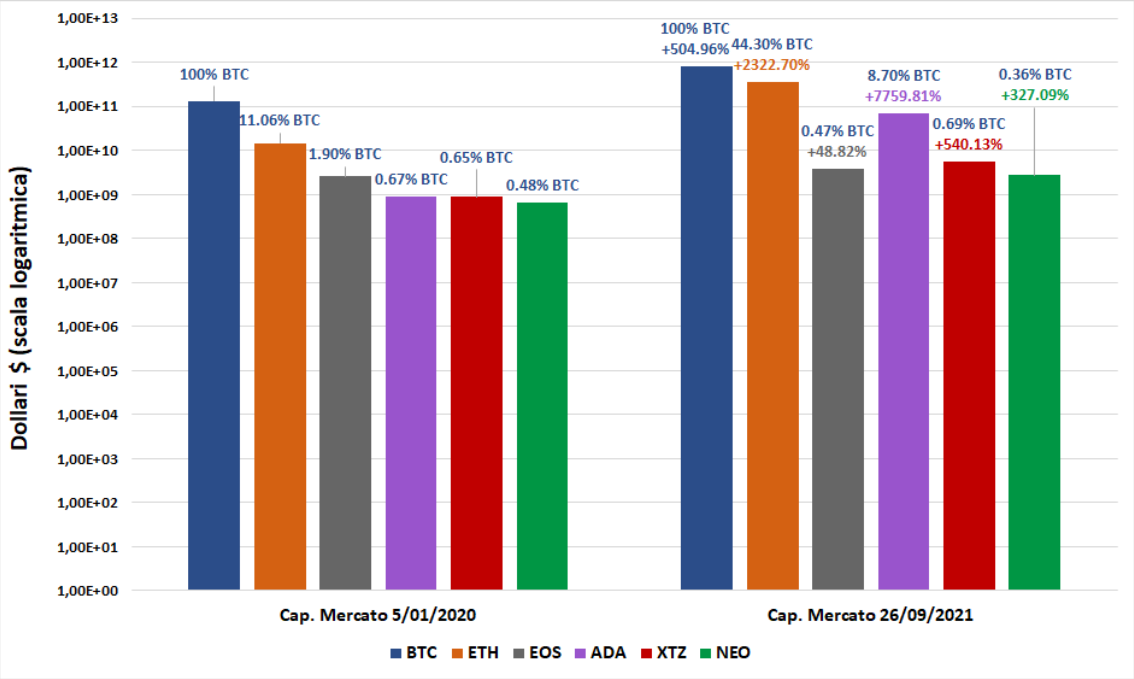


Figura 3.3.3: **Capitalizzazione di mercato negli anni 2020-2021 di alcuni sistemi PoW (BTC, ETH) e PoS (ADA, NEO, XTZ, EOS)**

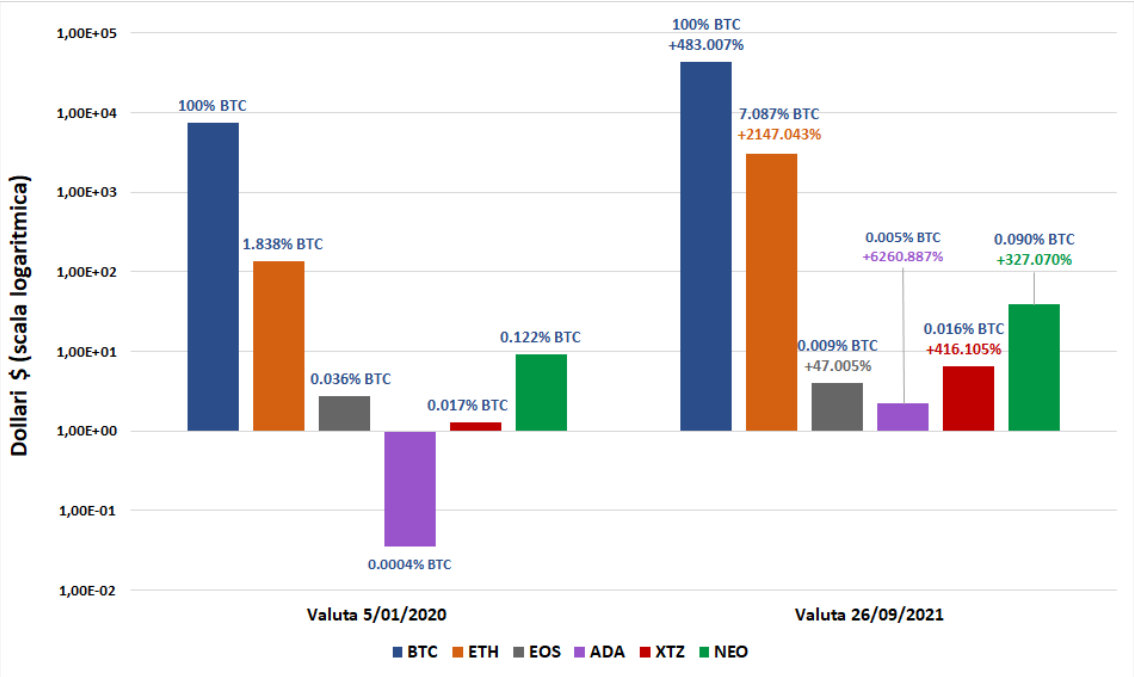
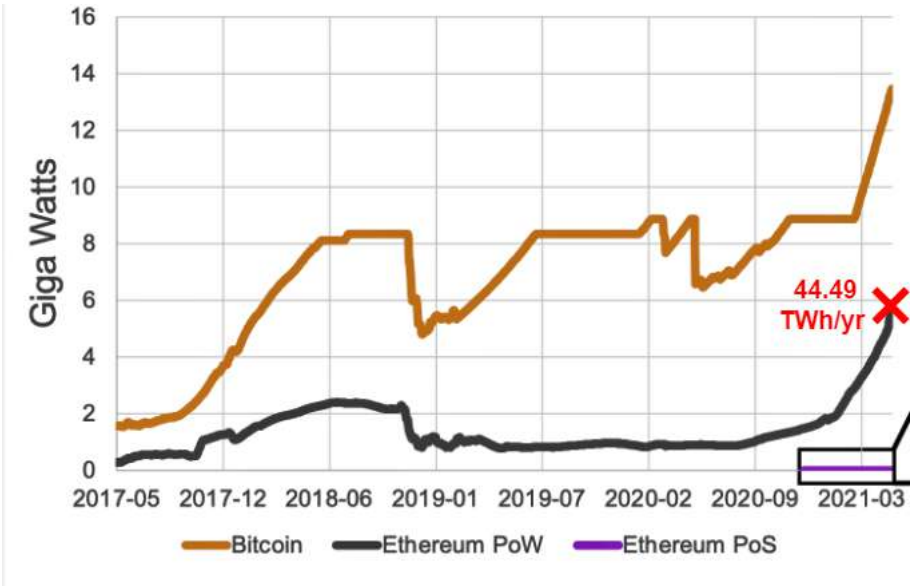


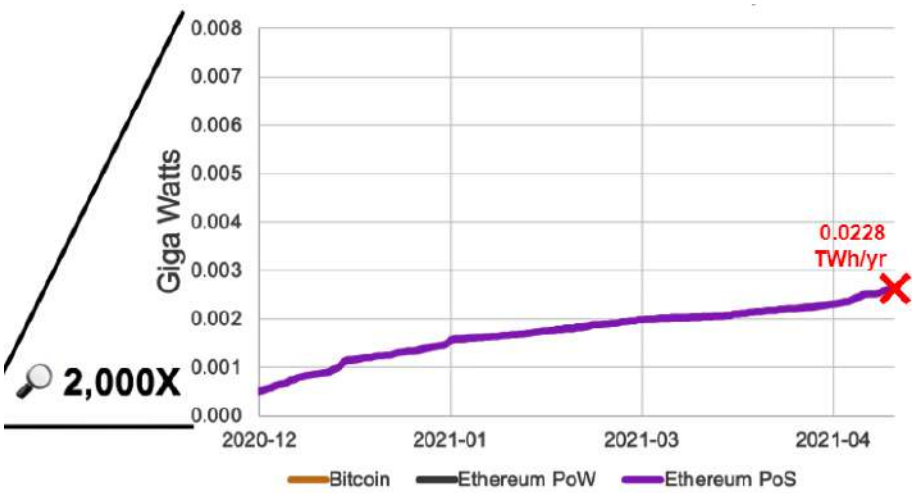
Figura 3.3.4: **Prezzo di valuta negli anni 2020-2021 di alcuni sistemi PoW (BTC, ETH) e PoS (ADA, NEO, XTZ, EOS)**

Ethereum, nata nel 2013, è stata (e continua ad essere) la seconda criptovaluta per capitalizzazione di mercato durante l'intero periodo di analisi, da gennaio 2020 a settembre 2021. Pertanto, potrebbe essere un miglior punto di riferimento rispetto

a Bitcoin, poiché è una realtà più stabile rispetto al precedente esempio di Cardano. Inoltre, Ethereum è stata originariamente basata su Proof-of-Work, ma ha iniziato una transizione al protocollo di consenso Proof-of-Stake a partire da dicembre 2020, all'inizio del periodo di analisi. Questa transizione, conosciuta come *Ethereum 2.0* o *The Merge*, è stata ufficialmente completata il 15 settembre 2022 e grazie ad essa Ethereum è riuscita a risolvere problemi legati alla scalabilità, alla sicurezza e soprattutto alla sostenibilità. Durante la transizione, si è registrata una significativa riduzione del consumo in potenza rispetto a Ethereum Proof-of-Work, con un valore massimo di soli 0.0026 GW nel marzo 2021, ovvero una riduzione del 99.95% rispetto al corrispettivo 5.15 GW della versione precedente. I due consumi di potenza sono stimati in modo continuo, ossia interruzioni temporali in un anno (circa 8760 ore).



(a) scala 1x



(b) scala 2000x

Figura 3.3.5: **Potenza elettrica di Bitcoin (BTC) e di Ethereum PoW e PoS (ETH)**

Potenza elettrica	Energia elettrica
0.0026 GW	0.0026 GW · 8760 h ≈ 0.0228 TWh/yr
5.1300 GW	5.1300 GW · 8760 h ≈ 44.4900 TWh/yr

Tabella 3.1: **Conversione dei consumi**

Ricerche più recenti datate a maggio 2023 hanno migliorato le previsioni per l'uso di energia di Ethereum Proof-of-Stake a 0.0026 TWh/yr, rappresentando un miglioramento superiore al 99.99% rispetto ai corrispettivi 78 TWh/yr. Questa transizione ha consentito ad Ethereum di diventare una blockchain più efficiente dal punto di vista energetico, in particolare rispetto alla Proof-of-Work della sua versione precedente e a Bitcoin, ma anche rispetto ad altri settori spesso paragonati alle criptovalute, come il settore bancario e l'industria dell'oro. Questi dati promettenti su Ethereum PoS hanno contribuito a ridurre il suo impatto ambientale legato al mining e alle transazioni, rappresentando un importante passo avanti verso un consumo più sostenibile nel settore delle criptovalute.

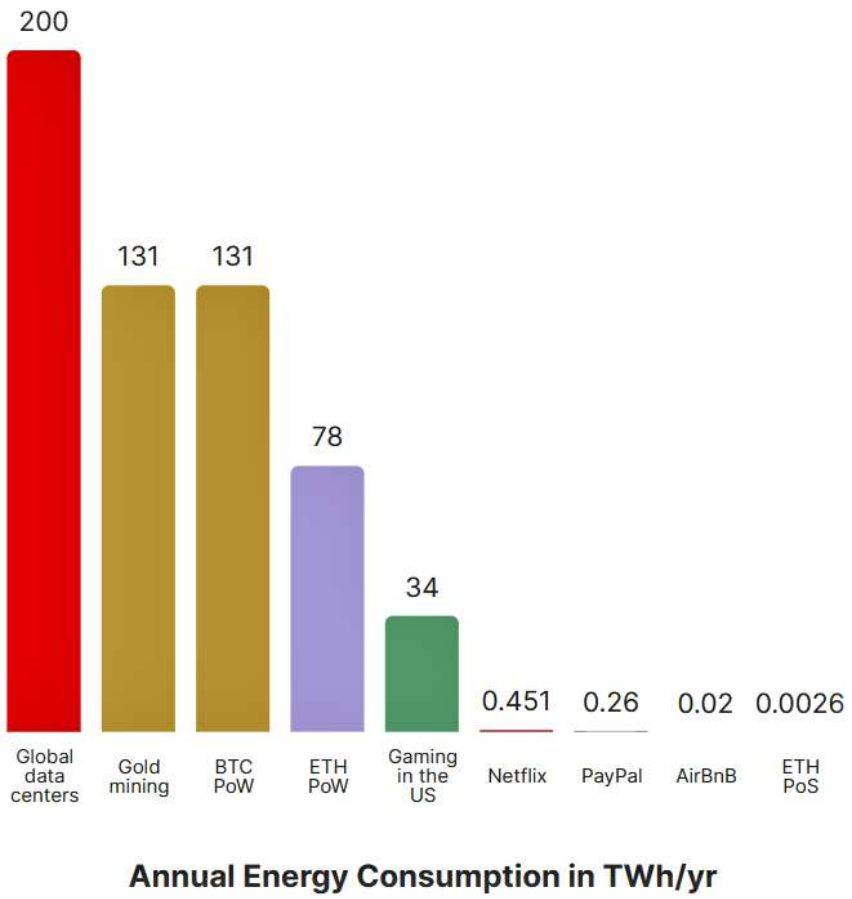


Figura 3.3.6: **Energia elettrica di ETH PoS rispetto ad alcune industrie (Maggio 2023)**

Al momento, Bitcoin non sembra interessato a modificare il proprio protocollo. Sebbene la PoS miri ad eliminare svantaggi come i requisiti hardware e l'alto consumo energetico, perde i vantaggi di sicurezza della PoW.

Infatti, Bitcoin sostiene che i sistemi Proof-of-Stake possano presentare problemi di sicurezza, in quanto influenzati dai nodi *validator* che possiedono la maggior quantità di criptovaluta. Questi possono mettere in gioco più risorse come pegno, aumentando così le probabilità di essere selezionati per la validazione di un blocco e accumulando sempre più liquidità. Tale circolo vizioso, quindi, porterebbe alla concentrazione delle risorse nelle mani di pochi utenti, potenzialmente mettendo a rischio la decentralizzazione della rete e aprendo la possibilità ad attacchi.

Per una migliore comprensione del concetto, si può considerare l'esempio di una società di servizi finanziari focalizzata su Bitcoin chiamata *River Financial*. Immaginando una rete blockchain con un valore di 100 miliardi di dollari, se utilizzasse un protocollo Proof-of-Stake in cui il 10% dei token disponibili è bloccato nello staking, essa sarebbe vulnerabile ad essere conquistata da un attaccante con un capitale di 10 miliardi di dollari. Questo è possibile poiché il controllo finanziario gli permetterebbe di accumulare una considerevole quantità di token, ottenendo così una significativa influenza sulle decisioni della rete e mettendo a rischio la sua decentralizzazione e sicurezza. Al contrario, attaccare una rete simile, ma con un protocollo PoW, richiederebbe l'acquisto di ASIC e l'acquisizione di contratti di spazio ed energia necessari per eseguire il mining su una scala molto più ampia rispetto all'intera rete. Inoltre, richiederebbe l'assunzione e l'organizzazione di un numero significativo di personale per eseguire l'attacco. Se un evento di tale dimensioni fosse in corso, probabilmente l'intera rete verrebbe avvisata in anticipo a causa dell'enorme domanda di ASIC ed di elettricità che sarebbe necessaria.

Queste considerazioni evidenziano alcune delle sfide e delle potenziali criticità associate all'adozione del Proof-of-Stake come protocollo di consenso. Tuttavia, è importante notare che le criptovalute che utilizzano PoS, come le sopracitate Cardano, EOS, Neo e Tezos, stanno già operando con successo su questo modello e stanno cercando soluzioni per mitigare tali potenziali vulnerabilità e garantire un ecosistema sicuro e decentralizzato.

3.3.1 Protocollo Ouroboros (Cardano)

Cardano (ADA) è una criptovaluta basata sulla tecnologia blockchain, fondata nel 2015 da Charles Hoskinson, che è stato anche uno dei co-fondatori di Ethereum. A differenza di altre criptovalute che utilizzano la Proof-of-Work, Cardano si basa sul protocollo di consenso chiamato Ouroboros, che adotta un approccio Proof-of-Stake ma presenta delle differenze significative rispetto ad altri protocolli.

Ouroboros introduce due nuovi concetti temporali: gli "slot" e le "epoche". Gli slot sono brevi unità di tempo, mentre le epoche hanno una durata di 432 mila slot,

corrispondenti a circa 5 giorni, per garantire una maggiore sincronizzazione della rete nel suo complesso.

Durante ogni slot, un partecipante viene designato come "leader" secondo una modalità casuale, ma comunque ponderata in base alla quantità di criptovaluta messa in stake. Egli ha la responsabilità di creare un blocco contenente le transazioni, che poi viene convalidato dagli altri partecipanti della rete per garantirne l'integrità e la correttezza. Questo processo di convalida delle transazioni avviene rapidamente, entro una finestra temporale di 20 secondi, fornendo una solida protezione contro potenziali attacchi malevoli. Nel caso in cui il blocco non venga convalidato o propagato tempestivamente, il protocollo Ouroboros può prevedere la presenza di leader alternativi per garantire la continuità del processo. Viceversa, se il blocco viene convalidato, si passa al successivo slot con la nomina di un nuovo leader, e così via.

Alla fine di ogni epoca, le ricompense vengono distribuite ai leader dei blocchi e ai partecipanti che hanno contribuito alla convalida, incentivando la partecipazione al processo di consenso all'interno della rete di Cardano.

In questo protocollo, così come negli altri simili alla PoS, l'opportunità di produrre un nuovo blocco e di ricevere ricompense non dipende dal potere computazionale, ma dalla quantità di valuta messa come garanzia per la partecipazione attiva. Poiché non c'è una corsa per estrarre blocchi, non vi è uno spreco di energia o risorse computazionali.

3.3.2 Protocolli delegati: dBFT (Neo) e DPoS (EOS)

I protocolli delegati combinano il concetto di PoS e di consenso delegato con una struttura che affronta il problema dei generali bizantini. In un'ipotetica situazione in cui un gruppo di generali dell'esercito bizantino deve coordinare un attacco contro un nemico comune, la sfida principale consiste nel raggiungere un accordo unanime sulla decisione di attaccare o ritirarsi. La risoluzione di questo problema implica trovare un modo per consentire ai generali di prendere una decisione condivisa nonostante la presenza di traditori o problemi di comunicazione tra di loro.

A differenza del protocollo Proof-of-Stake (PoS), che coinvolge l'intera rete, nei protocolli delegati il compito di produrre i blocchi è affidato a un numero limitato di "delegati" eletti dall'intera rete in modo da consentire una maggiore partecipazione e un equo potere decisionale, anche da parte di nodi stakeholder più piccoli. I protocolli delegati generalmente si compongono di due fasi principali: la proposta e la validazione. Durante la fase di proposta, uno dei nodi delegati propone un nuovo blocco contenente un insieme di transazioni. Successivamente, gli altri nodi delegati verificano la correttezza e la validità del blocco proposto. Se il blocco viene confermato da almeno il 66% dei nodi, viene considerato valido e aggiunto alla blockchain. Questo meccanismo garantisce la prevenzione di comportamenti arbitrari o maliziosi, in modo simile ai traditori tra i generali bizantini, poiché la produzione di un blocco non valido comporterà l'esclusione del produttore del blocco dalla futura

votazione e la conseguente perdita delle ricompense.

I protocolli delegati offrono diversi vantaggi rispetto alla PoS. Come accennato in precedenza, la creazione e la validazione dei blocchi sono affidate a una porzione ristretta della rete, il che garantisce un consenso rapido e definitivo e richiede meno energia, soprattutto per la fase di validazione.

Tra i protocolli delegati, due esempi significativi sono il dBFT, introdotto da Neo nel 2016, e il più comune DPoS, acronimo di Delegated Proof-of-Stake, utilizzato da diverse criptovalute come EOS. Nonostante entrambi siano protocolli delegati, presentano differenze sostanziali nella loro implementazione. Tra le più importanti e riconoscibili, il dBFT non basa la selezione dei nodi delegati solo sul possesso della valuta, come nel DPoS, ma tiene conto anche di altri criteri come la reputazione del nodo e il suo impegno nel favorire l'economia della valuta all'interno della sua rete. Inoltre, in caso di comportamenti potenzialmente malevoli, nel DPoS i nodi delegati possono essere soggetti a sanzioni come la perdita delle proprie valute, mentre nel dBFT non sono previsti meccanismi di sanzione specifici. Ciò implica che, nel dBFT, i nodi delegati non sono incentivati a comportarsi malevolmente, ma non subiscono sanzioni specifiche nel caso lo facciano.

3.3.3 Protocollo LPoS (Tezos)

Nel 2018 Tezos (XTZ) è stato uno dei primi progetti a implementare su larga scala un sistema di consenso chiamato "Liquid Proof-of-Stake" (LPoS). Questo sistema innovativo introduce nuove caratteristiche rispetto ai tradizionali Proof-of-Stake e Delegated Proof-of-Stake.

Rispetto a quest'ultimo, la delega in Tezos è opzionale, il che significa che non esiste un numero fisso di produttori di blocchi. I diritti di produzione vengono assegnati in base alla quantità di partecipazione e della valuta posseduta. Questo approccio offre più flessibilità e scalabilità nel processo di produzione dei blocchi.

Inoltre, la Liquid Proof-of-Stake consente diritto di voto diretto ai possessori della valuta, che permette loro di votare direttamente sulle modifiche del protocollo. Questo offre un'opportunità di partecipazione attiva nella governance del sistema, che va oltre la semplice selezione dei produttori di blocchi come avviene nelle DPoS.

Nonostante presenti alcune differenze nell'organizzazione rispetto ai protocolli delegati, il LPoS offre vantaggi simili in termini di consumo energetico. La rete è gestita da un numero limitato ma comunque affidabile di partecipanti, che utilizzano un processo di convalida meno intensivo rispetto al mining tradizionale. Questo approccio riduce il consumo energetico complessivo necessario per mantenere la rete e convalidare i blocchi.

CAPITOLO 4

Alcuni opinionisti

In questa sezione sono riportate le opinioni di alcune delle personalità più note del settore, che in particolare apprezzano Twitter come mezzo di divulgazione e di dialogo. Questa piattaforma ospita spesso discussioni intense sul tema, consentendo non solo di condividere il proprio pensiero, ma anche di ricevere feedback attraverso i commenti degli altri utenti.

4.1 Michael Saylor

Michael Saylor è un imprenditore americano e un dirigente aziendale, nonché co-fondatore di *MicroStrategy*, un'azienda specializzata nell'intelligence aziendale. Il suo grande interesse per Bitcoin si è concretizzato nel 2020 quando ha acquistato circa 21 Bitcoin per 250 milioni di dollari, al fine di dare una nuova forma alle liquidità dell'azienda.

Nel settembre 2022, in risposta al passaggio ufficiale di Ethereum alla Proof-of-Stake, Saylor ha espresso le sue opinioni al fine di chiarire ciò che lui definisce "disinformazione e propaganda" riguardo all'impatto ambientale di Bitcoin e della sua Proof-of-Work. In particolare, il tweet di Saylor risponde ad alcuni di questi principali punti critici.

Energy Inefficiency della PoW

L'imprenditore adotta una posizione decisa a riguardo, sostenendo addirittura che la Proof-of-Work rappresenti "l'uso più pulito di energia nell'ambito industriale" e che "la sua efficienza energetica stia migliorando al ritmo più veloce fra le grandi industrie". A sostegno della sua argomentazione, cita dati provenienti dal *Bitcoin Mining Council*, un gruppo composto da 45 compagnie che affermano di rappresentare il 50.5% dell'intera rete Bitcoin. I dati mostrano che circa il 60% dell'energia utilizzata per il mining proviene da fonti sostenibili, e che l'efficienza energetica è migliorata del 46% su base annua.

Figura 4.1.1: **Tweet di Michael Saylor**

Questo è un argomento particolarmente delicato, considerando che alcuni stati americani hanno addirittura intrapreso azioni per vietare il mining di criptovalute.

4.1.1 Confronto con altre BigTech

Un altro punto di cui si fa forte Saylors nel suo tweet è il confronto con altre grandi compagnie tech come *Google*, *Facebook* e *Netflix*, rispetto alle quali Bitcoin conserverebbe un rapporto "energy consumption - valore economico" di gran lunga migliore.

4.1.2 PoW-PoS

Viene infine prestata particolare attenzione all'ipotesi che le critiche ambientaliste rivolte a Bitcoin possano essere semplicemente una campagna a favore della Proof-of-Stake, e che autorità e investitori stiano trascurando i problemi che potrebbero sorgere con il nuovo protocollo. In particolare, si evidenzia il fatto che gli asset legati alla PoS siano generalmente considerati titoli non registrati e siano scambiati su piattaforme senza una regolamentazione adeguata. Si fa riferimento, ad esempio, al caso di Ripple vs SEC.

4.2 Elon Musk

Elon Musk è un imprenditore e innovatore americano, noto per essere il fondatore e CEO di aziende come *Tesla Inc.*, *SpaceX* e *Neuralink*. È un personaggio visionario coinvolto in numerosi altri progetti di rilievo. Musk è infatti famoso per la sua visione audace e la sua costante ricerca di soluzioni innovative per affrontare le sfide globali, in particolare nel settore dell'energia sostenibile e dell'esplorazione spaziale.

La preoccupazione per il consumo energetico associato a Bitcoin è stata da lui sollevata su Twitter nel 2021. In un annuncio, Musk ha dichiarato che la sua azienda non avrebbe più accettato Bitcoin come metodo di pagamento a causa delle crescenti preoccupazioni riguardo all'uso di combustibili fossili nel mining e nelle transazioni di Bitcoin. Questa decisione è arrivata meno di due mesi dopo l'annuncio iniziale che consentiva ai clienti di acquistare veicoli Tesla utilizzando Bitcoin. Tale evento ha ricevuto un'ampia copertura mediatica.

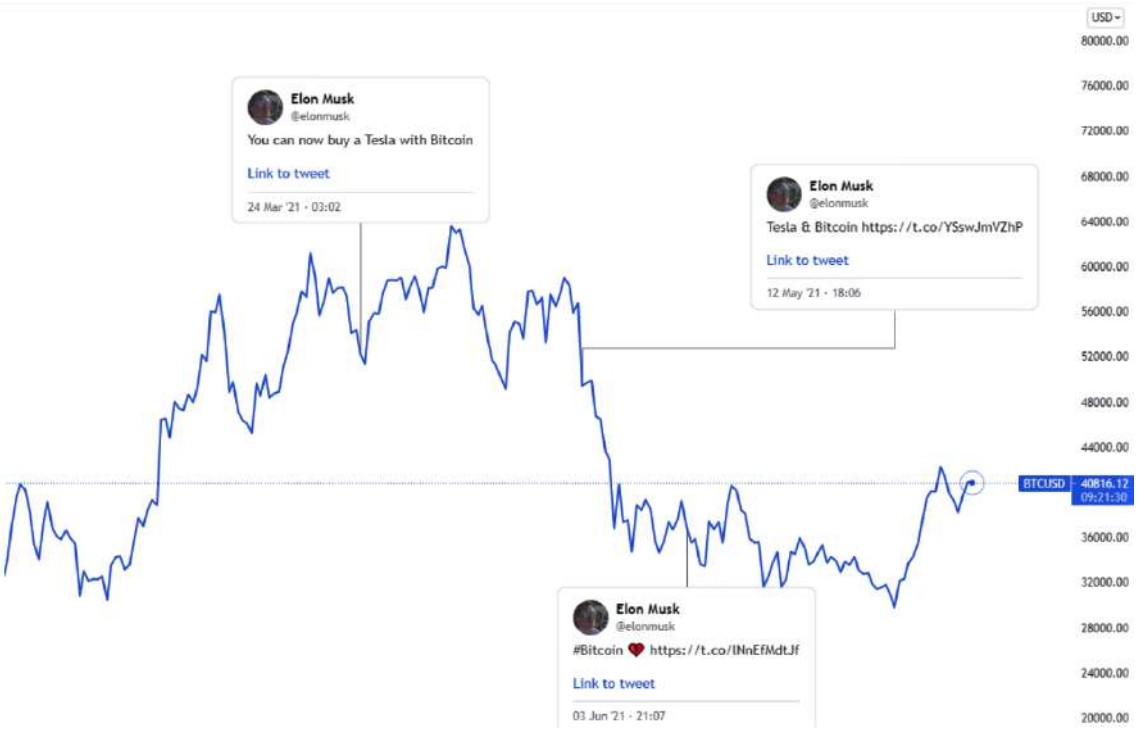


Figura 4.2.1: **I tweet di Elon Musk nel 2021 legati al rapporto Tesla-Bitcoin**

4.3 Saifedean Ammous

Saifedean Ammous, professore di economia presso la Adnan Kassar School of Business, è un esperto e sostenitore delle criptovalute. È l'autore del libro *Bitcoin Standard: The Decentralized Alternative to Central Banking*, considerato un punto di riferimento nel campo della blockchain.

La posizione di Ammous è fortemente favorevole a Bitcoin e si basa sulla valorizzazione dei servizi che essa offre, soprattutto l'indipendenza da entità centralizzate. A differenza di Saylor, Ammous utilizza un approccio diverso e non cerca di dimostrare che i dati sul consumo energetico di Bitcoin siano gonfiati o oggetto di attacchi da parte di altre grandi aziende tecnologiche. Al contrario, ritiene che il consumo energetico di Bitcoin sia una realtà intrinseca alla struttura stessa della criptovaluta. In effetti, secondo Ammous, questo aspetto potrebbe essere sfruttato come un deterrente alla necessità di un governo "leader" responsabile della regolamentazione e della garanzia degli scambi internazionali.

Figura 4.3.1: **Tweet di Saidedean Ammous a sostegno delle politiche ambientali e di consumo di Bitcoin**

Figura 4.3.2: **Insight sull'opinione di Ammous**

4.4 Mark Carney

Mark Carney è un economista e banchiere canadese, noto soprattutto per il suo ruolo di governatore della Banca del Canada dal 2008 al 2013. Dopo la fine del suo mandato, è diventato governatore della Banca d'Inghilterra dal 2013 al 2020, guidando il paese attraverso un periodo di significativa incertezza economica, inclusa la complessa situazione della Brexit. Oltre alla sue cariche menzionate, Carney è stato consulente speciale delle Nazioni Unite per l'azione climatica e finanziaria.

Sebbene egli non abbia espresso esplicitamente il suo parere su Bitcoin sulla piattaforma Twitter, lo ha fatto durante la Conferenza economica scozzese inaugurale, tenutasi a marzo del 2018 presso la Central Hall di Edimburgo. A metà del suo discorso di quasi un'ora, Mark Carney ha fornito un'opinione critica nei confronti di Bitcoin, evidenziandone le limitazioni come mezzo di scambio e di conservazione del valore, nonché i costi energetici e di transazione associati.

L'autore evidenzia il fatto che al momento pochi rivenditori accettano Bitcoin come metodo di pagamento, sia nel Regno Unito che negli Stati Uniti, e che la velocità e i costi delle transazioni con Bitcoin sono generalmente più lenti e costosi rispetto ai pagamenti in valuta tradizionale come la sterlina. Inoltre, le criptovalute più utilizzate affrontano gravi limiti di capacità rispetto ad altri sistemi di pagamento, come dimostrato dal confronto tra VISA, che può elaborare fino a 65 mila transazioni al secondo a livello globale, e Bitcoin, che può gestirne solo 7 al secondo.

Viene sottolineato che i tempi di attesa per le transazioni Bitcoin possono essere di ore, a differenza dei pagamenti con carta di debito o di credito nel Regno Unito, che vengono completati in pochi secondi e senza rischi di cambio. Gli utenti di Bitcoin devono offrire commissioni di transazione abbastanza elevate per convincere i miners di Bitcoin a elaborare le transazioni in modo tempestivo, il che può rendere costoso l'utilizzo di Bitcoin rispetto a contanti, carte o pagamenti online.

Inoltre, si sottolinea che i costi dell'estrazione di Bitcoin sono enormi, con un consumo annuale di energia che è stimato essere fino a 52 TWh, pari al doppio del consumo di energia della Scozia. A confronto, il consumo energetico della rete di carte di credito VISA è inferiore allo 0.5% di quello di Bitcoin, nonostante elabori molte più transazioni, circa paria ad un fattore 9000.

Riferimenti

[1] Erik Anderson and Rohan Reddy. *Bitcoin Mining Is Set to Turn Greener*. https://www.globalxetfs.com/bitcoin-mining-is-set-to-turn-greener/#:~:text=The%20Bitcoin%20Mining%20Council%20(BMC,36.8%25%20estimated%20in%20Q1%202021, (Marzo, 2023).

[2] Redazione ANSA. *ansa.it*. https://www.ansa.it/canale_ambiente/notizie/energia/2023/03/28/azimut-investe-40-milioni-nella-blockchain-sostenibile-alps_65adad94-0f64-4a86-870a-9801d028bf8d.html, (Marzo, 2023).

[3] Stakin Articles, Guides, and Newsletters. *The Proof-of-Stake Guidebook: PoS, DPoS, LPoS, BPoS, Kézako?* https://blog.stakin.com/proof-of-stake-guide-dpos-vs-lpos-vs-bpos-vs-hybrid/, (Ottobre, 2021).

[4] Mark Carney. *The Future of Money*. https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/the-future-of-money-speech-by-mark-carney, (Maggio, 2018).

[5] Wayne Duggan and Michael Adams. *What Is Ethereum 2.0? Understanding The Ethereum Merge*. https://www.forbes.com/advisor/investing/cryptocurrency/what-is-ethereum-2-merge/, (Settembre, 2022).

[6] River Financial Inc. *Proof-of-Work (PoW) vs Proof-of-Stake (PoS)*. https://river.com/learn/proof-of-work-pow-vs-pos-proof-of-stake#:~:text=Proof-of-Work%20(PoW)%20is%20a%20mechanism%20Bitcoin,to%20owners%20of%20the%20token., (Maggio, 2021).

[7] Shangrong Jiang, Yuze Li, Quanying Lu, Yongmiao Hong, Dabo Guan, Yu Xiong, and Shouyang Wang. *Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China*. *Nature communications*, 12(1):1–10, (Aprile, 2021).

[8] Benjamin A Jones, Andrew L Goodkind, and Robert P Berrens. *Economic estimation of Bitcoin mining's climate damages demonstrates closer resemblance to digital crude than digital gold*. *Scientific Reports*, 12(1):14512, (Settembre, 2022).

[9] Galaxy Digital Holdings LP. *On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question.* https://www.galaxy.com/research/whitepapers/on-bitcoins-energy-consumption/, (Maggio, 2021).

[10] José Maldonado. *What is Cardano (ADA)?* https://academy.bit2me.com/en/what-is-cardano-ada/, (Marzo, 2023).

[11] Baxtel: Data Center news, events, and information. *VisaNet Data Centers and Colocation.* https://baxtel.com/data-centers/visanet, (Aprile, 2023).

[12] University of Cambridge. Cambridge bitcoin electricity consumption index. https://ccaf.io/cbnsi/cbeci, (Maggio, 2023).

[13] Ethereum Org. *Ethereum's energy expenditure.* https://ethereum.org/en/energy-consumption/, (Maggio, 2023).

[14] Coin Rivet. *Delegated Byzantine Fault Tolerance (dBFT) explained.* https://coinrivet.com/delegated-byzantine-fault-tolerance-dbft-explained/, (Marzo, 2019).

[15] Alessandro Rubino. *Proof of work: cos'è e le differenze con il proof of stake.* https://www.blockchain4innovation.it/criptovalute/blockchain-cosa-sono-i-protocolli-pow-e-pos-e-a-cosa-servono/, (Marzo, 2020).

[16] FTSE Russell. *Proof-of-Stake: A crypto path to lower energy consumption and yield.* https://content.ftserussell.com/sites/default/files/education_proof_of_stake_paper_v6_0.pdf, (Gennaio, 2022).

[17] YCharts. *Bitcoin Average Difficulty (I:BAD).* https://ycharts.com/indicators/bitcoin_average_difficulty#:~:text=Bitcoin%20Average%20Difficulty%20is%20at,53.61%25%20from%20one%20year%20ago., (Maggio, 2023).