APPLICAZIONI DELLA TECNOLOGIA BLOCKCHAIN

VOLUME 2 - 2022

a cura di Danilo Bazzanella e Andrea Gangemi

Autori

Giulia Accossato, Leonardo Barale, Ghassane Ben El Aattar, Riccardo Bertolo, Beatrice Borgogno, Irene Capodicasa, Matteo Cattaneo, Alice Colombatto, Aurora Costantino, Annalisa Deiana, Alessio Dongiovanni, Davide Fioriti , Emanuele Formento, Matteo Galla, Simone Galota, Alessandro Giacchetto, Filippo Grobbo, Seyedhossein Javadizavieh, Davide Leone, Nicola Lombardi, Federica Lorenzo, Davide Manco, Matteo Montrucchio, Niccolò Provvedi, Giulio Quaglia, Fabrizio Santoriello, Lorenzo Tamietti, Paolo Tassoni, Linda Terzi, Giacomo Tomasi Cenesi, Gabriele Vernetti, Michele Vioglio.

DIPARTIMENTO DI SCIENZE MATEMATICHE
POLITECNICO DI TORINO

INDICE

PANORAMICA SU BIP-119: CHECKTEMPLATEVERIFY

Giulia Accossato, Ghassane Ben El Aattar, Niccolò Provvedi, Paolo Tassoni

Capitolo 1

Introduzione

1.1 Contenuti

Questa tesina ha come obiettivo l'analisi della recente proposta BIP-119 da parte di Jeremy Rubin. Verranno prima descritti alcuni concetti generali, utili per la comprensione finale, per poi trattare dettagli tecnici della proposta. Inoltre, verranno esaminati alcuni casi d'uso più pratici e riportate alcune delle discussioni e controversie riguardanti BIP-119 da parte della comunità di Bitcoin.

1.2 Concetti

1.2.1 Cos'è un BIP

I BIP (Bitcoin Improvment Proposal) sono proposte per l'introduzione di funzionalità o informazioni nel protocollo Bitcoin, che possono essere effettuate da chiunque. Come software, Bitcoin è sempre in fase di aggiornamento: i bug devono essere corretti, gli algoritmi possono essere resi più efficienti, il codice può essere semplificato, la compatibilità con altri software deve essere mantenuta e possono essere aggiunte nuove funzionalità.

Nel caso di un normale software appartenente a progetti centralizzati, un manager o uno sviluppatore principale potrebbe semplicemente assegnare compiti e dettare le modifiche che devono essere implementate. Tuttavia, Bitcoin è un sistema open source basato sul consenso. Non c'è un leader. Il processo BIP organizza la comunità Bitcoin in assenza di un leader centrale.

Come nuovo sistema monetario, la reputazione di Bitcoin è ancora in fase di consolidamento e la sicurezza della rete è fondamentale per mantenere la fiducia. Pertanto, il processo di sviluppo di Bitcoin è intenzionalmente lento e deliberato. Il processo da una proposta iniziale, a un BIP formalizzato, a un cambiamento attivato, è lungo. Quando un BIP viene pubblicato, viene discusso sia dalla comunità degli sviluppatori che dalla più ampia comunità di utenti Bitcoin. In background, se il BIP richiede modifiche al codice in Bitcoin Core, gli sviluppatori lavoreranno alla scrittura, al test e all'integrazione di quel codice.

Se vengono sollevate argomentazioni legittime da una parte significativa degli utenti, è probabile che il BIP venga ritirato o rifiutato e il processo di proposta dovrà essere abbandonato o riavviato.

Se la comunità ottiene un consenso e non vengono riscontrati inconvenienti della proposta, la comunità sceglierà un percorso di attivazione e inizierà ad attivare il BIP. Questo è il processo di discussione e approvazione di un BIP (Descritto nel BIP0001):

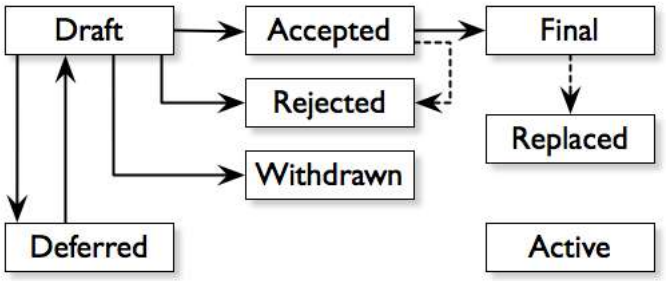


Figura 1.1. BIP Workflow.

1.2.2 Bitcoin covenants

La proposta BIP-119 introduce il concetto di **covenant**. I covenants sono essenzialmente un tipo di restrizione su **come** un determinato insieme di bitcoin può essere speso.
Sono una primitiva di linguaggio per creazione di smart-contract che consentirebbe applicazioni d'uso come per esempio i *vaults*, che potrebbero proteggere i bitcoin di una persona dall'essere facilmente spesi da qualcun'altro che ha ottenuto la sua chiave privata, ma hanno lo svantaggio di essere potenzialmente capaci di abilitare la creazione di bitcoin che possono essere spesi solo per indirizzi specifici.
Anche se al momento non esiste una definizione tecnica formale si riporta quanto detto da Anthony Towns in una discussione nella mailing-list degli sviluppatori Bitcoin:

> "Nell'ecosistema Bitcoin, la definizione più adatta di covenant è quando lo scriptPubKey di un UTXO limita lo scriptPubKey dell'output(s) di una transazione che spende quel UTXO". [12]

Note:

- **ScriptPubKey**: Locking script che impone le condizioni di spesa, fa parte dell'output quando viene creata una transazione
- **UTXO**: Output di Transazione non speso, definisce una quantità di bitcoin spendibile da chi possiede la chiave privata (e soddisfa tutte le condizioni) dell'indirizzo a cui fanno riferimento.
  La spesa di un *UTXO* avviene attraverso la risoluzione del locking script da parte di un unlocking script dato in input.

Capitolo 2

BIP-119

2.1 Proposta BIP-119

Il BIP-119 è stato pubblicato nella lista dei Bitcoin Improvment Proposal il 06/01/2020 da Jeremy Rubin. [8].
Il BIP-119 propone l'introduzione di un nuovo operatore nel linguaggio Script del protocollo Bitcoin, l'operatore **OP_CheckTemplateVerify** (abbreviato con *OP_CTV*).
Questo nuovo operatore introduce la possibilità di eseguire un tipo basilare di covenant, chiamato **template**, che consente un insieme limitato di casi d'uso molto vantaggiosi senza implicare rischi significativi per il protocollo.

2.1.1 Introduzione di un nuovo operatore in Script

Gli operatori nel linguaggio Script di Bitcoin sono chiamati *opcode* e sono in numero limitato, ognuno identificato da un codice univoco e da una stringa testuale che inizia con "*OP_*".
Ad esempio l'operatore che dato un input svolge la funzione di hash sha-256 è identificato dalla stringa *OP_SHA256* e codice 168 (in esadecimale: 0xa8).
L'introduzione di nuovi operatori è possibile grazie all'insieme degli opcodes che vanno dal 176 (0xb0) al 185 (0xb9), chiamati *OP_NOP1 - OP_NOP10*. Questi dieci operatori sono riconosciuti come opcodes "non-operation" poiché, se inseriti in uno script, al momento dell'esecuzione nello stack, non svolgono nessuna operazione e non ritornano o modificano nessun tipo di dato.
La particolarità di questi opcodes è che possono essere modificati per cambiare l'operazione da svolgere, infatti sono riservati appositamente per essere utilizzati per aggiungere nuovi operatori attraverso proposta di soft fork.[13]
Se fosse necessario si potrebbero comunque creare nuovi operatori, aumentandone il numero, per inserire nuove tipologie di operazioni nel linguaggio Script, ma in questo caso si dovrebbe avviare una proposta di hard fork (cosa che si tende a evitare) poiché sarebbe un'adozione di un protocollo non compatibile con quello precedente.

Attualmente *OP_NOP2* e *OP_NOP3* sono utilizzati rispettivamente per *OP_CheckLockTimeVerify* e *OP_CheckSequenceVerify* introdotti nei BIP-065 e BIP-112. Il BIP-119 propone l'attivazione di *OP_CTV* attraverso il cambiamento di semantica dell'opcode *OP_NOP4* (0xb3).

2.1.2 Motivazioni

Attualmente Bitcoin non possiede molta flessibilità per quanto riguarda la programmabilità a livello base delle transazioni e non ha la possibilità di creare smart contracts complessi dato che il suo linguaggio non è Turing completo.
Anche se Taproot, il nuovo aggiornamento introdotto a Novembre 2021, semplifica la costruzione di script complessi e migliora vari aspetti del protocollo, il modo di gestire cosa è possibile fare con le transazioni e di come possono essere programmate rimane piuttosto limitato.
OP_CTV vuole espandere leggermente questo concetto e fornire ulteriori potenzialità.
Nella maggior parte dei casi un utente può controllare come sbloccare una transazione definendo le restrizioni necessarie, ma non può controllare cosa si può fare con quella transazione una volta sbloccata.
Con questa nuova proposta si può abilitare una pre-definizione di quali output sono accettabili, invece di controllarne solo gli input.
Sebbene aggiungere complessità al linguaggio potrebbe comportare rischi per la sicurezza della rete consentendo conseguenze impreviste o non intenzionali la proposta dell'operatore *OP_CTV* risulta piuttosto semplice. [4]

2.2 Operatore CheckTemplateVerify

OP_CTV consente di limitare il modo in cui un *UTXO* possa essere speso, in particolare definisce delle condizioni per l'*UTXO* creato in una transazione, limitandone la possibilità di essere speso solo verso uno specifico insieme di indirizzi.
Specificatamente, *OP_CTV* controlla che la transazione in cui sta operando corrisponda a un certo **template**, un insieme di dati precedentemente definito.

Esempio Alice invia 2 bitcoin a Bob; nel momento dell'invio, e quindi della creazione della transazione con Bob, Alice imposta una condizione definendo un template, in modo tale che l'*UTXO* creato potrà essere speso solo a favore di un determinato indirizzo (Quello di Carl).
Ora Bob ha ricevuto i 2 bitcoin, ma per la condizione imposta da Alice, l'unico modo per spenderli è inviarli all'indirizzo di Carl, altrimenti, tramite il controllo che verrà effettuato da *OP_CTV*, la transazione sarà rifiutata.

2.2.1 Funzionamento

1. Nel momento della creazione di una transazione (come prima tra Alice e Bob), viene creato un hash a partire da un insieme specifico di dati, che vedremo in dettaglio tra poco, che definisce le condizioni di spesa dell'*UTXO*. Questo hash, chiamato **template** e identificato con *<T>*, viene inserito nel locking script dell'output della transazione.

2. Quando si vuole spendere questo *UTXO* si crea una transazione (come prima tra Bob e Carl) dove in input ci sarà l'unlocking script che dovrà risvolvere il locking script creato in precedenza.
A un certo punto la situazione nello stack sarà questa:

```
... <T> OP_CHECKTEMPLATEVERIFY ...
```

3. A Questo punto *OP_CTV* esegue tre controlli in ordine quando viene eseguito:

- Verifica se c'è almeno un elemento nello stack.
- Verifica se l'elemento ha esattamente 32 bytes.
- Verifica se *DefaultCheckTemplateVerifyHash* della transazione all'indice di input corrente è uguale all'elemento nello stack.

Se la verifica fallisce nel primo o nel terzo caso avviene un *fail* e la transazione viene rifiutata, invece nel secondo caso viene eseguito un *OP_NOP* e la transazione prosegue senza fare niente.
Questa implementazione è dovuta a possibili nuove versioni dell'operatore che potrebbero usare più bytes.

Il terzo passaggio di verifica è esattamente il punto in cui avviene il controllo della condizione di spesa imposta da *<T>* e se questa viene soddisfatta.
In *OP_CTV* la funzione *DefaultCheckTemplateVerifyHash* esegue la funzione di hash sha-256 a questo specifico insieme di dati della **transazione corrente** serializzato in questo ordine:

- Versione
- LockTime
- Hash Scriptsig (se non c'è viene omesso)
- numero di input
- hash sequenza
- numero di output
- hash output
- indice dell'input corrente

4 *DefaultCheckTemplateVerifyHash* viene confrontato con *<T>* e se risultano uguali la condizione viene soddisfatta.
Nota: In *OP_CTV*, essendo un operatore "Verify", se la condizione viene soddisfatta gli elementi nello stack vengono eliminati senza ritornare un valore *true.*

2.2.2 Specifiche

In questa sezione viene riportato e commentato brevemente il codice del funzionamento di *OP_CTV* scritto in C++.
Le funzioni presentate di seguito sono estrapolate dal commit fatto da Jeremy Rubin su GitHub nel fork del repository ufficiale Bitcoin dedicato al BIP-119. [9]

Main Vengono effettuate le tre verifiche principali:

```
1  case OP_CHECKTEMPLATEVERIFY:
2  {
3   if (stack.size() < 1)
4   return set_error(serror, SCRIPT_ERR_INVALID_STACK_OPERATION);
5   // If the argument was not 32 bytes, treat as OP_NOP4:
6   switch (stack.back().size()) {
7    case 32:
8     if (!checker.CheckDefaultCheckTemplateVerifyHash(stack.back())) {
9     return set_error(serror, SCRIPT_ERR_TEMPLATE_MISMATCH);
10    }
11   break;
12   default:
13    // future upgrade can add semantics for this opcode with different
      length args
14    // so discourage use when applicable
15    if (flags & SCRIPT_VERIFY_DISCOURAGE_UPGRADABLE_NOPS) {
16    return set_error(serror, SCRIPT_ERR_DISCOURAGE_UPGRADABLE_NOPS);
17         }
18    }
19 }
20 break;
```

Riga 3: Verifica di almeno un elemento nello stack.
Riga 7: Controllo che l'elemento nello stack abbia dimensione di 32 bytes.
Riga 8: Esecuzione *CheckDefaultCheckTemplateVerifyHash* con argomento l'elemento dello stack (ovvero *<T>*).
Riga 20: Se tutte le verifiche sono soddisfatte la funzione non ritorna niente.

Funzione di confronto Prima viene costruito *DefaultCheckTemplateVerifyHash* e poi viene confrontato con *<T>*.

```
1  class CTransactionSignatureSerializer
2  {
3  private:
4      const T& txTo;              //!< reference to the spending
       transaction (the one being serialized)
5      const CScript& scriptCode; //!< output script being consumed
```

```
6       const unsigned int nIn;     //!< input index of txTo being signed
7   }
8   bool GenericTransactionSignatureChecker<T>::
        CheckDefaultCheckTemplateVerifyHash(const std::vector<unsigned char
        >& hash) const
9   {
10      // Should already be checked before calling...
11      assert(hash.size() == 32);
12      assert(txTo != nullptr);
13      uint256 hash_tmpl = GetDefaultCheckTemplateVerifyHash(*txTo, nIn);
14      return std::equal(hash_tmpl.begin(), hash_tmpl.end(), hash.data());
15  }
```

Riga 13: Costruzione di *DefaultCheckTemplateVerifyHash* chiamando la funzione *GetDefaultCheckTemplateVerifyHash*.
Riga 14: Verifica dell'uguaglianza.
Riga 4,6: I termini usati nella funzione sono puntatori ai dati della transazione corrente.

DefaultCheckTemplateVerifyHash Costruzione di *DefaultCheckTemplateVerifyHash*.

```
1   uint256 GetDefaultCheckTemplateVerifyHash(const TxType& tx, uint32_t
        input_index) {
2       return GetDefaultCheckTemplateVerifyHash(tx, GetOutputsSHA256(tx),
        GetSequencesSHA256(tx), input_index);
3   }
4   uint256 GetDefaultCheckTemplateVerifyHash(const TxType& tx, const
        uint256& outputs_hash, const uint256& sequences_hash,
5                                   const uint32_t input_index) {
6       return NoScriptSigs(tx) ?
        GetDefaultCheckTemplateVerifyHashEmptyScript(tx, outputs_hash,
        sequences_hash, input_index) :
7           GetDefaultCheckTemplateVerifyHashWithScript(tx, outputs_hash,
        sequences_hash, GetScriptSigsSHA256(tx), input_index);
8   }
9   uint256 GetDefaultCheckTemplateVerifyHashEmptyScript(const TxType& tx,
        const uint256& outputs_hash, const uint256& sequences_hash,
10                                  const uint32_t input_index) {
11      auto h = CHashWriter(SER_GETHASH, 0)
12          << tx.nVersion
13          << tx.nLockTime
14          << uint32_t(tx.vin.size())
15          << sequences_hash
16          << uint32_t(tx.vout.size())
17          << outputs_hash
18          << input_index;
19      return h.GetSHA256();
20  }
```

Riga 1,4: Prima vengono eseguite in sequenza queste due funzioni per richiamare i dati necessari.
Riga 9: Vengono serializzati i dati necessari su cui viene eseguita la funzione di hash sha-256 per ottenere *DefaultCheckTemplateVerifyHash*.

2.3 Regole di implementazione

In questa sezione viene approfondito il metodo di implementazione, analizzando singolarmente i campi del covenant *template* e alcune delle scelte progettuali, spiegandone le motivazioni.

2.3.1 Analisi dei campi di template

DefaultCheckTemplateVerifyHash confrontato con l'elemento dello stack

L'insieme di dati per cui è eseguito il commit sono metadati che possono influire sulla composizione dell'id della transazione (*TXID*), oltre agli input.
Questo garantisce che per un dato input noto, i *TXIDs* possano essere conosciuti in anticipo.

Locktime e versione

Se il locktime e la versione non ci fossero, sarebbe possibile ritardare arbitrariamente la spesa di un *UTXO* e modificare ancora di più il *TXID*.
Includendo questi campi, anziché limitarli a valori specifici, viene reso più flessibile l'utilizzo di *OP_CTV*, in quanto consente agli utenti di impostare la versione e il locktime a loro piacimento.

Numero di input e hash delle sequenze

OP_CTV consente agli utenti di impostare l'esatto numero di input. In generale l'utilizzo di più input è difficile e crea piccoli problemi, quindi non è necessario utilizzarne di più se non in applicazioni specifiche.
Se gli hash delle sequenze non fossero inclusi, si potrebbero presentare problemi di malleabilità per il *TXID*, inoltre permettono di imporre un riferimento di tempo relativo senza un *OP_CSV*. Teoricamente l'inclusione degli hash delle sequenze implica il numero degli input, rendendo questo campo ridondante, tuttavia rende più facile e sicuro la costruzione iniziale dello script.

Hash degli output

L'inclusione degli hash degli output garantisce che la spesa dell'*UTXO* sia assicurata per creare gli esatti output richiesti. Viene scelto l'hash, piuttosto che i valori degli output stessi, poiché è già precalcolato per ogni transazione per ottimizzare le firme.

Indice di input corrente

L'inclusione dell'indice di input corrente elimina la vulnerabilità del riutilizzo delle chiavi. Poiché gli script di *OP_CTV* risultano validi per un determinato indice, le istanze riutilizzate di questi script non possono essere spese per lo stesso indice, il che implica che non possono essere spese nella stessa transazione.

2.3.2 Scelte di progettazione

Commit dei valori tramite hash

Usare gli hash dei valori rende più semplice ed efficace la costruzione di *DefaultCheckTemplateVerifyHash* a partire da uno script. I campi che non devono essere impostati possono essere inclusi tramite hash senza incorrere nel problema di ricalcolare tutti gli hash.

Utilizzo di SHA-256

SHA256 è un hash di 32 byte che soddisfa gli standard di sicurezza di Bitcoin ed è già disponibile all'interno di Script per la creazione di template generici.
RIPEMD160, un hash da 20 byte, potrebbe anche essere un hash praticabile in alcuni contesti e presenta alcuni vantaggi, ad esempio per ridurre le commissioni, RIPEMD160 salva 12 byte. Tuttavia, RIPEMD160 non è stato scelto per il BIP-119 perché introduce rischi durante la verifica dei programmi creati da terze parti.

Ordine dei campi serializzati

L'ordine dei campi serializzati per comporre *template* al momento non è significante, tuttavia con un attenta selezione potrebbe essere possibile migliorarne l'efficienza in scripts fututri, in combinazione con opcodes che potrebbero essere aggiunti come *OP_CAT* o *OP_SHA256STREAM* pensati per la manipolazione di stringhe e per creare script dinamicamente.

Capitolo 3

Casi d'uso

Attualmente ogni utente di Bitcoin può spendere i propri UTXO come preferisce. In un mondo post-OP_CTV, come già accennato, si potrebbero mettere in atto delle regole sugli UTXO posseduti per controllare e limitare i possibili modi in cui quest'ultimi possano essere spesi; ancora più importante, l'operatore OP_CTV consente di applicare queste restrizioni alla spesa in modo non interattivo.
Introducendo questo operatore in Bitcoin, potrebbe essere abilitato un insieme più diversificato di casi d'uso e potrebbe emergere un nuovo ecosistema di applicazioni. Alcuni casi d'uso abilitati da OP_CTV potrebbero essere resi possibili oggi, ma il più delle volte l'insieme di utenti che partecipano all'accordo di smart contract dovrebbe essere online e interagire manualmente per coordinare le regole di spesa, il che non è sempre possibile. OP_CTV consente di applicare queste restrizioni in modo programmatico, senza richiedere l'interazione manuale dei partecipanti, aumentando così l'affidabilità del patto.

Alcune delle funzionalità che OP_CTV potrebbe abilitare per Bitcoin includono miglioramenti nella sicurezza, nella privacy e nella scalabilità. La proposta si concentrava inizialmente sulla possibilità di creare transazioni di controllo della congestione, mentre le versioni successive hanno posto maggiore enfasi su altri contratti e patti che potrebbero essere creati utilizzando il nuovo codice operativo come la possibilità di creare soluzioni di custodia più sofisticate (i vaults), transazioni coinjoin in nuovi modi che potrebbero semplificare la costruzione o ridurre le commissioni. Altri autori hanno affermato che il nuovo codice operativo potrebbe essere utilizzato per consentire agli utenti di riunire in modo affidabile i propri fondi in un unico UTXO in un modo che aumenterebbe la privacy.

Analizzeremo nel dettaglio due dei principali casi d'uso che potrebbero essere abilitati in seguito all'attivazione dell'operatore OP_CTV:

- CONGESTION CONTROLLED TRANSACTION [10]

- VAULTS [11]

3.1 Congestion controlled transaction

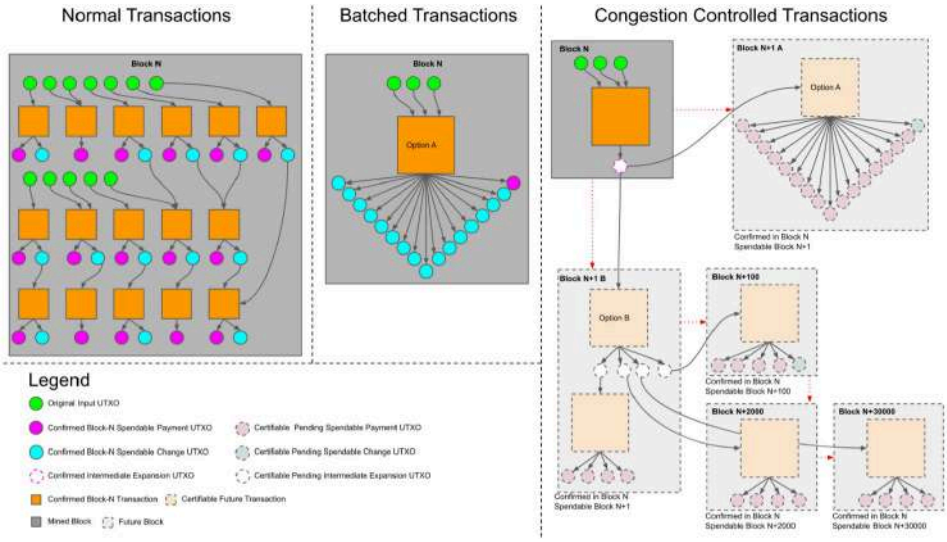


Figura 3.1. Comparazione tra i tipi di transazione.

Definito il *blockspace*, ovvero l'ammontare delle transazioni che possono essere processate in un determinato tempo, se la domanda è molto forte le *fee* aumentano e diventa molto costoso effettuare transazioni. Utilizzando *OP_CTV*, un elaboratore può aggregare tutti i pagamenti in un'unica transazione a scopo di conferma. Quindi, qualche tempo dopo, i pagamenti possono essere espansi da quell'UTXO quando la domanda di *blockspace* diminuisce. Il principale vantaggio del codice operativo proposto è consentire la conferma di una piccola transazione ora (quando le commissioni potrebbero essere elevate) e fare in modo che tale transazione garantisca in modo affidabile che un insieme di persone riceverà i pagamenti effettivi in seguito, quando le commissioni potrebbero essere inferiori. Ciò può essere molto utile per le organizzazioni che già implementano tecniche come il *"payment batching"*, che consiste nell'includere pagamenti multipli nella stessa transazione onchain, per gestire picchi di commissioni improvvise.

Senza *OP_CTV*, questo è attualmente già possibile con Schnorr multisignature. Tuttavia non è possibile farlo in modo non interattivo, il che limita fondamentalmente la fattibilità dell'approccio poiché l'interazione per raccogliere le firme di tutti i destinatari può essere difficile o lenta.

3.1.1 Esempio

Consideriamo ora la seguente situazione [6]: Alice deve pagare un gruppo di dieci persone, ma le commissioni di transazione sono attualmente elevate. Non desidera inviare dieci transazioni separate o utilizzare *"payment batching"* per inviare una transazione che

includa un output per ciascuno dei destinatari; vuole impegnarsi senza fiducia a pagare ciascun destinatario in futuro quando le commissioni di transazione saranno più basse.

Congestion controlled transaction con *Multisignature*

Alice chiede a ciascuno dei destinatari la chiave pubblica. Crea una *transazione di setup*, non firmata e non trasmessa, diretta a quei destinatari utilizzando un address multisignature 10-di-10 e una *transazione di distribuzione* (transazione multisignature) avente tale address come input e un output per ciascun destinatario. Alice, successivamente, chiede a tutti i destinatari di firmare la transazione di distribuzione, si assicura che ogni persona riceva le firme di tutti gli altri e infine firma e trasmette la transazione di setup. Quando la transazione di setup riceve un numero ragionevole di conferme non c'è modo per Alice di ingannare i 10 ricevitori e finché ciascuno dei ricevitori ha una copia della transazione di distribuzione e di tutte le firme degli altri, non c'è modo per nessun destinatario di ingannare qualsiasi altro destinatario di un pagamento. Quindi, anche se la transazione di distribuzione che paga effettivamente i ricevitori non è stata trasmessa o confermata, i pagamenti sono garantiti dalla transazione di setup confermata. In qualsiasi momento, chiunque dei destinatari che desideri spendere i propri soldi, possedendo tutte le firme, può trasmettere la transazione di distribuzione e attenderne la conferma.

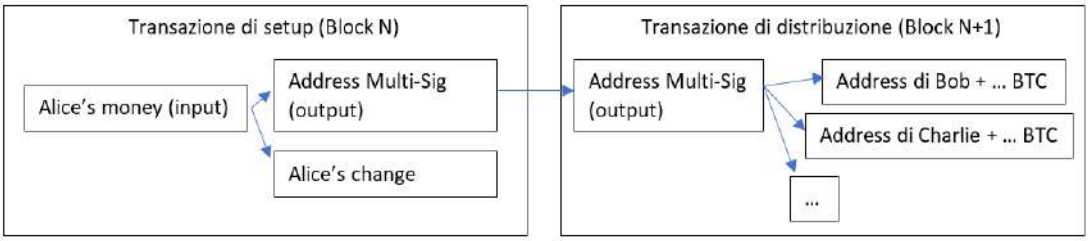


Figura 3.2. Congestion controlled transaction con *Multisignature*.

Congestion controlled transaction con *OP_CTV*

Alice crea una *transazione di setup*, nella quale aggrega tutti i pagamenti, a scopo di conferma utilizzando OP_CTV; quindi, qualche tempo dopo, i pagamenti possono essere espansi da quell'UTXO a tutti i destinatari quando la domanda di spazio di blocco è diminuita. Alice, che è il mittente di una transazione controllata, può scegliere tra molte diverse strutture di transazione. L'opzione più semplice è una singola transazione impegnata che si espande da 1 output a N (Option A). Con l'aumentare del numero di destinatari, un mittente può impegnarsi in un albero di output utilizzando OP_CTV. L'albero consente loro di confermare tutti i pagamenti che desiderano (ad esempio, anche più di quanti possano stare in un blocco). Una tale tecnica inizia ad avere senso quando: $N{*}size\_of(Output) > log(N){*}size\_of(OP\_CHECKTEMPLATEVERIFY(Txn)) + size\_of(Output)$ Assumendo dimensioni di transazione semplici, si tratta di circa 10 destinatari.

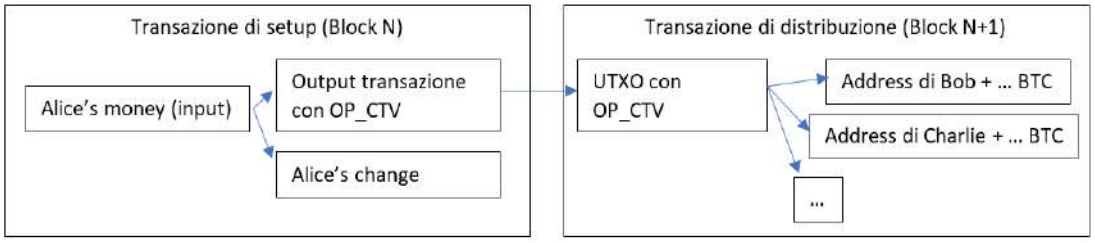


Figura 3.3. Congestion controlled transaction con *OP_CTV*.

3.2 Vaults

Bitcoin offre a utenti e aziende la possibilità di assumersi una nuova e importante responsabilità: la possibilità di controllare unilateralmente il proprio denaro; infatti, bitcoin richiede agli utenti di controllare le proprie chiavi private, che sono gli strumenti esclusivi necessari per autorizzare il trasferimento di fondi. L'auto custodia riduce la dipendenza da terze parti centralizzate come exchanges o custodial wallets.
Dati gli strumenti disponibili ora, il multisig 2-di-3 e la custodia collaborativa sono i migliori veicoli per facilitare l'auto custodia, sacrificando la sicurezza e usabilità il meno possibile. Il principale vantaggio di multisig è che crea una ridondanza aggiuntiva nella gestione delle chiavi: mentre gli indirizzi a firma singola richiedono solo una chiave per spostare bitcoin, gli indirizzi a firma multipla richiedono più chiavi. Gli indirizzi multisig consentono a privati e aziende di impostare schemi personalizzati in base alle proprie esigenze, ad esempio 2-di-3 , 3-di-5 o qualsiasi combinazione di M-di-N. Creando un M-di-N, in cui M è maggiore di uno, un individuo o un'azienda può includere partner fidati senza rinunciare al controllo sovrano e in caso di perdita di una chiave i fondi non sono immediatamente a rischio. In questo modo aumenta la sicurezza, ma aumentano anche la complessità della spesa e della gestione delle informazioni.

Quindi, come è possibile migliorare la custodia multisig con l'introduzione dell'operatore *OP_CTV*?

OP_CTV consente di utilizzare la strategia di deposito senza la necessità di mantenere i dati di transazione preimpostati per tutta la durata, come nel caso di precedenti implementazioni. Il *Vaulting* è una tecnica per porre vincoli su come spendere i bitcoin. I vincoli sono progettati in modo tale da limitare la minaccia di fallimento (dovuta alla perdita della chiave o al tentativo di confisca) durante il processo di custodia. L'idea di base è predeterminare il percorso che le monete nel deposito possono percorrere, il che consente di progettare il flusso di fondi in modo da avere la possibilità di intervenire se accade qualcosa di inaspettato.

"single-hop" vaults usando *OP_CTV*

[5]

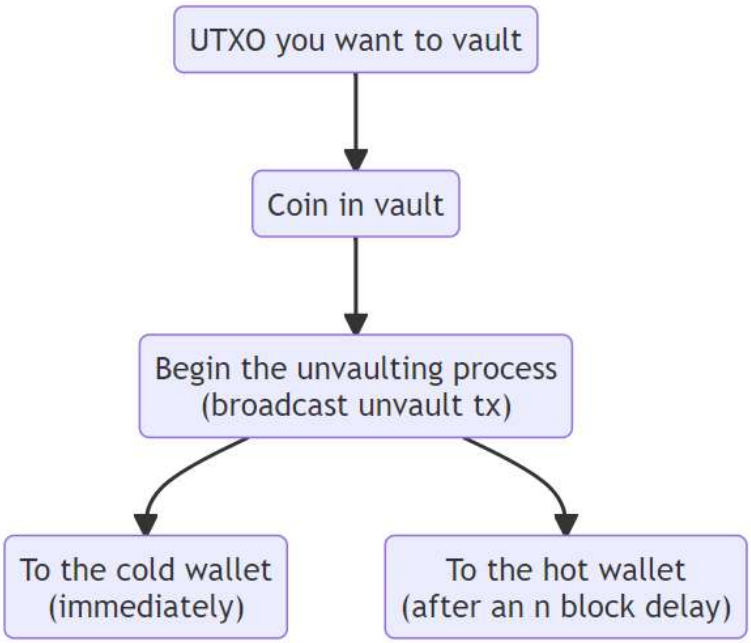


Figura 3.4. "single-hop" vault.

1. L'utente deposita i propri BTC, inviando la moneta a un address con *OP_CTV*, che predetermina e garantisce come questo UTXO può essere speso
2. L'utente conserva una copia della *transazione di unvault* che consente di prelevare immediatamente il saldo un chiave designata come cold wallet oppure iniziare il processo di ripristino e, dopo un ritardo di blocco configurabile dall'utente, spendere le monete in una chiave designata come hot wallet.

Questo metodo consente all'utente di intervenire se vede che un processo di unvault è stato avviato inaspettatamente. Esempio: se un malintenzionato Mallory ottiene il controllo dell'hot wallet dell'utente Alice e vuole rubare le monete del deposito deve trasmettere la transazione di unvault. Se Alice sta guardando la catena vedrà che la transazione di unvault è stata trasmessa inaspettatamente e può immediatamente trasferire il saldo nel suo cold wallet, mentre Mallory deve attendere il ritardo del blocco per riuscire a rubare fondi dal hot wallet.

Capitolo 4

Discussioni e Controversie

Il BIP119 ha suscitato grande scalpore nella comunità Bitcoin, sia per ragioni tecniche, che sfruttano in larga parte i concetti esposti nei capitoli precedenti, sia per ragioni legate alla figura del suo ideatore: *Jeremy Rubin*. Ciascuna delle controversie più importanti e famose che verranno presentate si legano ad uno o più di tali aspetti.

4.1 Introduzione dei Covenant

La maggiore rivoluzione del BIP119 è legata all'introduzione dei *Covenants*. Com'è stato spiegato precedentemente, i *Covenants* possono essere definiti come un meccanismo che permette in linea teorica di imporre condizioni su come le criptomonete verranno spese e gestite in futuro. Un semplice esempio consiste nella possibilità di inviare Bitcoin ad un certo utente, con l'opzione che tali monete vengano inviate solo a determinati tipi di indirizzi.

Una futura applicazione interesserebbe sicuramente le banche, che avrebbero la possibilità di concludere un contratto di finanziamento con una società, con la condizione che il debito debba essere rimborsato nel momento in cui il rapporto tra flusso di cassa e patrimonio netto della società scenda sotto un certo livello. Un altro possibile esempio pratico ha a che fare con le commissioni, poiché con i *Covenants* una transazione potrebbe essere eseguita solo se le commissioni scendono sotto un certo livello [3].
Passiamo quindi ad individuare alcuni tra i principali vantaggi e svantaggi legati a questa nuova proposta. Tra i *vantaggi* possiamo includere i seguenti punti:

1. Essa introduce una serie di nuovi modi per programmare Bitcoin, consentendo la predefinizione piuttosto che il semplice controllo degli input.

2. Il comando *OP_CTV* (**OP_CHECKTEMPLATEVERIFY**) permette l'applicazione programmatica delle restrizioni senza richiedere l'interazione manuale dei partecipanti. Questo aumenta l'affidabilità dell'accordo.

3. Alcune delle funzionalità includono miglioramenti di sicurezza privacy e scalabilità.

4. Il comando *CTV* potrebbe introdurre pool di pagamento, in cui un gruppo di persone condivide un singolo *UTXO* e in cui è possibile redistribuire i fondi in modo affidabile tra i partecipanti.

I *Covenants* ampliano l'insieme di strumenti finanziari esprimibili in Bitcoin e abilitano nuovi potenti casi d'uso, ma allo stesso tempo possono mettere in discussione alcuni tra i concetti chiave che hanno dato importanza tale criptomoneta in questi anni.

Fra gli *svantaggi*, l'aspetto negativo principale su cui vogliamo concentrarci ha a che fare con la fungibilità di Bitcoin, una sua principale caratteristica. La fungibilità è un concetto che si basa sulla considerazione che ogni unità è identica alle altre per funzionalità e qualità.

Queste nuove funzionalità mirano a dare più programmabilità a Bitcoin, consentendo ai programmatori di controllare come le criptomonete da loro inviate potranno essere spese in futuro. Con tali ipotesi si darebbe la possibilità di inserire in whitelist o blacklist determinati indirizzi, limitando come possono essere spesi BTC anche per chi ne possiede la chiave. Sebbene l'autore di BIP119 affermi che con la nuova proposta si possano creare solo regole semplici, essa potrebbe potenzialmente avere conseguenze inaspettate o non intenzionali [2].

Più specificamente il problema risulta evidente quando si generano *Covenant ricorsivi*. Per *Covenant ricorsivo* si intende quando esso non limita solamente la transazione successiva ma anche ogni transazione futura, generando con il tempo delle catene di regole che interagiscono in modo totalmente imprevedibile e potenzialmente dannose alla Blockchain [1].

Quindi l'introduzione di tali vincoli su BTC modificherebbe le sue proprietà specifiche di unità e comporterebbe la creazione di diverse categorie di Bitcoin, in termini di come possono essere spesi oppure inviati. Limitare il modo in cui possono essere spesi ne limita anche la loro utilità, danneggiando in definitiva il loro valore di scambio.

Concludendo, sebbene quindi la proposta di Rubin prometta di risolvere alcuni degli attuali problemi di sicurezza e ridimensionamento, i *Covenants* potrebbero anche porre limiti dannosi per l'utilità della criptovaluta. Questo andrebbe sicuramente a danneggiare il valore di scambio di Bitcoin a lungo termine.

4.2 Reazione della comunità e la figura di Jeremy Rubin

Un altro ramo delle controversie generate da BIP119, è legato alla figura di Jeremy Rubin: suo ideatore e profondo sostenitore.

Le discussioni suscitate dall'idea partono sicuramente da come la proposta è stata avanzata. Infatti Rubin ha voluto utilizzare uno *Speedy Trial* per l'attivazione del BIP. Come suggerisce il nome, uno *Speedy Trial* accelera il processo di verifica di un aggiornamento per arrivare al consenso. L'aggiornamento *Taproot* di Bitcoin, ad esempio, è stato approvato ed implementato in seguito ad uno *Speedy Trial*.

Importanti bitcoiner si sono chiesti se tale metodo sia appropriato per il consenso di BIP119. Nell'ultimo "Bitcoin Brief": Tone Vays , Adam Back, Jimmy Song e Rodolfo

Novak si sono opposti allo *Speedy Trial* di Rubin, rivelando anche un'opposizione simile da parte di Peter Todd, Matt Corallo, Giacomo Zucco, Luke-Jr, Bitcoin Gandalf, John Carvalho, Francis Pouliot, Andreas Antonopoulos e molti altri esperti hanno vari motivi per opporsi al piano, con alcuni favorevoli a BIP119 ed altri semplicemente contrari allo *Speedy Trial*.

BIP119 richiederebbe l'approvazione del 90% della potenza di mining della rete: su questo punto **Jimmy Song**, programmatore bitcoin, considera molto improbabile un'approvazione del 90% [7].

In un sondaggio non rappresentativo tramite Twitter, il 54% ha dichiarato di essere contrario a *OP_CTV* e Speedy Trial. Il 15% supporta *OP_CTV* ma ha rifiutato lo *Speedy Trial*. Tuttavia il numero insolitamente basso di voti (in genere attira migliaia di voti un tipico sondaggio su Twitter) fa ipotizzare che poche persone capiscano veramente BIP119.

Figura 4.1. Risultato del sondaggio effettuato da Jimmy Song: sostenitore, sviluppatore e autore di Bitcoin che contribuisce a progetti bitcoin open-source dal 2013.

Il problema principale che gli esperti evidenziano è che, a differenza di *Taproot*, l'aggiornamento proposto da Rubin non è riuscito ad ottenere un consenso unanime da parte della comunità Bitcoin e soprattutto non ha ricevuto il grado di scrutinio e di analisi che *Taproot* ha ricevuto. Tutto ciò porterebbe a classificare questo aggiornamento come pericoloso e l'attivazione di uno *Speedy Trial* in questa situazione è considerata da molti del tutto inopportuna. Queste considerazioni lo porterebbero ad essere visto come pericoloso poichè l'attivazione di *softwork* non supportati da un ampio consenso può portare a forzature involontarie o addirittura a spaccature della rete.

I vantaggi principali che si possono elencare, legati all'attivazione del BIP119, fanno tutti riferimento alla possibilità di Bitocoin di generare *SmartContracts*. Per molti però questa nuova funzionalità sarebbe poco sensata rispetto alla natura con cui la rete Bitcoin è stata creata, in particolare esistono altre criptovalute molto più efficienti e ottimizzate per gli *SmartContract* come *Ethereum*.

Figura 4.2. Tra i vari tweet di discussione di sull'argomento riportiamo per esempio quello di Jeremie Davinci: importante investitore in bitcoin, famoso per le sue previsioni sul mercato

Le controversie e dubbi non si fermano però solo alla proposta ma arrivano perfino all'autore stesso. Infatti Jeremy Rubin nel Maggio del 2020 ha fondato *Judica*, una società di ricerca e sviluppo che si concentra su un linguaggio di programmazione *SmartContract* chiamato *Sapio* che sicuramente beneficerebbe finanziariamente dall'adozione di BIP119. A prescindere da queste accuse, molti esperti sostengono che il linguaggio di programmazione *Sapio*, sviluppato appositamente per questo scopo, è ancora in fase di sviluppo e perciò non ancora maturo e adatto agli obiettivi che si pone questo aggiornamento.

Dai risultati ottenuti dal sondaggio si può facilmente intuire come i vantaggi legati all'approvazione del BIP119 non siano perfettamente noti a tutti, a parte quelli più evidenti. Questo nuovo aggiornamento sembra infatti avere per molti più lati negativi che positivi. Allo stesso tempo però non sembra essere veramente compreso da tutti e meriterebbe sicuramente una comunicazione più adeguata, per poterlo portare all'attenzione di più persone possibili nella comunità Bitcoin. Ad oggi il suo creatore rimane la figura più favorevole alla sua approvazione. Non si può sapere con certezza se questa proposta raggiungerà effettivamente il consenso o meno, quello che possiamo affermare con certezza è che BIP119 è un tema che ha generato molteplici discussioni ed ha incentivato il dialogo nella comunità, che riteniamo essere lo scopo primario di proposte di questo tipo ed ha sicuramente influito in un modo o nell'altro negli sviluppi futuri di Bitcoin.

Figura 4.3. Uno dei tanti Tweet di Jeremy Rubin per sollecitare la comunità Bitcoin al cambiamento

Conclusione

La proposta in questione ha suscitato molto clamore e ha dato inizio a discussioni e dibattiti in tutta la community e l'intero ecosistema di Bitcoin, a partire dagli sviluppatori, possessori di nodi fino agli utenti finali. In una sistema così grande e decentralizzato come Bitcoin non può essere che una buona cosa, in modo tale da avere una grande varietà di punti di vista.
Il BIP-119 vuole introdurre in modo definitivo un tipo basilare di covenant con un operatore dedicato, in modo tale da portare il protocollo a fare un primo passo verso un evoluzione tendente a un tipo di programmabilità più complessa.
Da notare, inoltre, che la maggior parte dei casi d'uso proposti con l'operatore CheckTemplateVerify si possono già implementare attraverso altre modalità, anche se in maniera meno efficiente.

Sicuramente la modalità di come è stato proposto il BIP e come l'autore abbia insistito per l'approvazione senza avere prima un consenso generale della community non ha aiutato, inoltre lo stesso autore sostiene una politica di attuazione di soft fork con una frequenza più alta, cosa non ben vista dalla maggior parte della community.
Anche se analizzando a fondo la proposta ci si rende conto che non ci sono effettivamente rischi significativi per il protocollo, la maggior parte degli sviluppatori sostiene che al momento ci siano aggiornamenti più importanti da fare tramite un eventuale soft fork.
Implementazioni di questo genere, che faranno evolvere il protocollo, probabilmente ci saranno in futuro, in ogni caso il BIP-119 potrebbe essere una di queste o la base per proposte più complete e generali che saranno approvate quando sarà il momento adatto.

Riferimenti

[1] Andreas Antonopoulos. *BIP119, EU regulatory attack, El Salvador, and much more in QandA with aantonop (April 2022)*. URL: https://www.youtube.com/watch?v=vAE5fOZ2Luw.

[2] Ruholamin Haqshanas. *Here is How BIP-119 Could 'Kill' Bitcoin According to Andreas Antonopoulosv*. URL: https://cryptonews.com/news/here-is-how-bip-199-could-kill-bitcoin-according-to-andreas-antonopoulos.htm.

[3] Stefanie Herrnberger. *BIP-119 Bitcoin Proposal im Eilverfahren?* URL: https://blockchainwelt.de/news/bip-119.

[4] Namcios. *Explaining Checktemplateverify*. URL: https://bitcoinmagazine.com/technical/what-is-bitcoin-checktemplateverify.

[5] James O'Beirne. *Safer custody with CTV vaults*. URL: https://github.com/jamesob/simple-ctv-vault.

[6] Bitcoin Optech. *Bitcoin Optech Newsletter 48*. URL: https://bitcoinops.org/en/newsletters/2019/05/29/#proposed-transaction-output-commitments.

[7] Protos. *BIP-119: Here's everything you need to know about the Bitcoin proposal*. URL: https://protos.com/bip-119-heres-everything-you-need-to-know-about-the-bitcoin-proposal/.

[8] Jeremy Rubin. *BIP-0119 GitHub*. URL: https://github.com/bitcoin/bips/blob/master/bip-0119.mediawiki/.

[9] Jeremy Rubin. *Codice Fork Bitcoin BIP119*. URL: https://github.com/bitcoin/bitcoin/blob/93f98f65f64f5980e649c58a1ad65829fe972745/src/script/interpreter.cpp/.

[10] Jeremy Rubin. *Scaling*. URL: https://utxos.org/uses/scaling/.

[11] Jeremy Rubin. *Vaults*. URL: https://utxos.org/uses/vaults/.

[12] Anthony Towns. *Definition covenant in [bitcoin-dev]*. URL: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2022-January/019795.html.

[13] Bitcoin Wiki. *Script*. URL: https://en.bitcoin.it/wiki/Script.

ALGORAND

Beatrice Borgogno, Matteo Cattaneo, Matteo Galla, Santoriello Fabrizio

Capitolo 1

Introduzione

1.1 Introduzione ad Algorand

Algorand è una rete decentralizzata costruita con l'obiettivo di risolvere il cosidetto trilemma, cioè poter garantire scalabilità (e dunque velocità nel processare una grande quantità di transazioni), sicurezza e decentralizzazione simultaneamente.
Nel primo white paper di Chen and Micali [2016] che ha portato alla creazione della blockchain Algorand vengono evidenziati i problemi tecnici di Bitcoin, che Algorand si propone di risolvere:

- spreco computazionale: la proof-of-work di Bitcoin richiesta per l'inserimento di un blocco, richiede a tutti i miners di lavorare per trovare il nounce giusto e far sì che l'hash del blocco sia al di sotto del target, ma soltanto un miner inserirà il blocco;
- concentrazione del potere in mano a poche mining pool: l'enorme quantità di sforzo computazionale richiesto per riuscire ad inserire un blocco nella blockchain Bitcoin spinge i miners ad organizzarsi in pools, causando un accentramento del potere;
- ambiguità dovuta alla generazione di forks: la possibilità che due blocchi vengano minati contemporaneamente da due miners diversi è concreta e questo porta alla formazione di biforcazioni, dunque gli ultimi blocchi inseriti contengono transazioni approvate dalla rete ma delle quali non si ha ancora la certezza assoluta.

Per risolvere questi problemi Algorand fa uso di una struttura a due livelli e di un particolare meccanismo di consenso del tipo Pure-Proof-of-Stake (PPoS). Inoltre la ricompensa per l'inserimento di un blocco inizialmente veniva distribuita tra tutti i possessori della criptovaluta e non soltanto a chi inserisce il blocco, come avviene invece in Bitcoin e molte altre blockchain, rendendo il sistema più equo.

1.2 ALGO: la criptovaluta di Algorand

La criptovaluta nativa di Algorand è chiamata Algo (simbolo ⱥ) ed ha un ruolo fondamentale nel funzionamento della rete: i possessori possono partecipare al meccanismo di

consenso presentando e votando i blocchi da inserire, inoltre gli Algo sono anche utilizzati per pagare le fees ed è richiesto il possesso di una minima quantità di Algo per scrivere dati sulla blockchain.
L'unità minima è detta microAlgo ed equivale a 10^{-6} Algo.
Alla genesi della blockchain sono stati coniati 10 miliardi di Algo, una quantità fissa ed immutabile che rappresenta il numero massimo di Algo presenti nella rete. Essi sono allocati come segue:

- 3 miliardi verranno messi in circolazione nei primi dieci anni (fino al 2030)
- 1.75 miliardi distribuiti nel tempo come ricompensa ai Participation Nodes
- 2.5 miliardi distribuiti nel tempo ai Relay Nodes
- 2.5 miliardi riservati per la Algorand Foundation e Algorand Inc.
- 0.25 miliardi distribuiti per sovvenzione agli utenti finali

Da qui si deduce che la rete non è propriamente decentralizzata, data la quantità di Algo in possesso della Algorand Foundation, ma la decentralizzazione aumenta con il tempo grazie al meccanismo democratico di distribuzione delle ricompense.

1.3 Algorand Foundation

Algorand Foundation è una organizzazione no-profit che sovrintende al finanziamento di Algorand Inc (società legale) ed allo sviluppo del protocollo Algorand stesso. La fondazione si occupa di promuovere il progetto e supportare la formazione degli sviluppatori in tutto il mondo, attraverso corsi di formazione universitaria, eventi, hackathon e certificazioni.
Come riportato sul sito della fondazione[1], l'impegno è quello di mantenere la promessa di una blockchain che garantisca un'economia solida, una governance decentralizzata ed un ecosistema open-source sano e prosperoso.

1.4 Punti di forza

Algorand, come ogni blockchain, ha i propri punti di forza.

- Velocità: Algo può essere inviato a qualunque wallet in meno di 4,5 secondi e non bisogna aspettare un certo lasso di tempo per essere sicuri che il pagamento sia stato confermato, la conferma è istantanea. Attualmente il protocollo può gestire 1000 transazioni al secondo e si calcola che entro la fine dell'anno possa raggiungere la velocità di 10000 transazioni al secondo

[1] Algorand Foundation: https://algorand.foundation/

- Scalabilità: la blockchain di Algorand è stata costruita per essere utilizzata da miliardi di utenti quindi a prescindere dal numero di utilizzatori il pagamento avverrà sempre in meno di 4,5 secondi[2]
- Affidabilità: la blockchain è stata progettata in modo da evitare in modo quasi assoluto le biforcazioni (la probabilità è di 10^{-18})
- Trasparenza: tutta la supply di Algo è pari a 10 miliardi di Algo creati al lancio della blockchain il 19 giugno 2019 e chiunque può visualizzarla perché pubblica
- Sicurezza: la rete è progettata in modo da essere resiliente contro gli attacchi che ne causano il partizionamento, l'attaccante non riuscirà a convincere due utenti onesti ad accettare due blocchi diversi
- Commissioni: le commissioni sono calcolate in base alla dimensione della transazione. Sono estremamente basse se paragonate a quelle imposte dai circuiti come Visa e Mastercard[3] oppure a quelle delle criptovalute più famose come Bitcoin ed Ethereum. Ad oggi le commissioni per ogni transazione sono fissate a 0.001 Ⱥ, pari a circa 0.0004$ al cambio attuale (02/06/2022)[2].

[2]Sito di Algorand dove ci sono i dati aggiornati https://www.algorand.com/

[3]Le commissioni sono molto variabili in base al tipo di pagamento(fisico o online), al tipo di POS scelto o alla banca di appoggio. In ogni caso partono dal 1% fino anche al 5% sull'importo della transazione. Per esempio al seguente link si possono consultare le commissioni della piattaforma myPOS https://www.mypos.com/it/pricing-and-fees

Capitolo 2

Il protocollo

2.1 Struttura del protocollo

La blockchain Algorand ha una particolare struttura a 2 livelli (layers) con lo scopo di processare separatamente gli smart contract e le dApp più pesanti e le transazioni semplici, in modo da garantire una velocità di esecuzione maggiore a queste ultime e non appesantire la chain principale con gli smart contract più grandi e complessi, che vengono eseguiti *off-chain*.

Layer-1

In particolare gli smart contract di primo livello (cioè quelli eseguiti *on-chain*) permettono di eseguire transazioni comuni, più o meno articolate, direttamente sulla blockchain stessa. Un esempio sono le transazioni *atomic swap*: grazie al supporto nativo è possibile vincolare l'esecuzione di due o più transazioni in modo che vengano eseguite tutte oppure nessuna. Un'altra tipologia di smart contract supportata nel primo livello è lo scambio di *Algorand Standard Asset* (ASA): gli utenti possono creare il proprio asset (o token) e scambiarlo sulla blockchain esattamente come avviene per la criptovaluta nativa, garantendo ai nuovi token la stessa sicurezza e rapidità di esecuzione che si ha per gli ALGOs.
Infine gli smart contract di primo livello permettono di gestire transazioni di vendita di beni, prestiti con garanzia, raccolte fondi, transazioni da utenti verificati e wallet multi-sig.

Layer-2

Negli smart contract di secondo livello rientrano tutte quelle applicazioni che richiedono in termini di spazio, di costo computazionale o di complessità del codice uno sforzo maggiore rispetto alle applicazioni più standard del Layer-1. Smart contract che necessitano di memorizzare una grande quantità di dati (di clienti, merci...), oppure che utilizzano algoritmi crittografici complessi per offrire un elevato livello di privacy rischierebbero di rallentare la velocità d'inserimento dei blocchi nella chain poiché tutti i nodi dovrebbero eseguirli.
Per questo motivo il protocollo Algorand prevede di far eseguire gli smart contract di

secondo livello ad un comitato di utenti diverso da quello che si occupa della votazione e validazione dei blocchi. Ogni utente del comitato (chiamato *contract execution committee*) esegue il contratto richiesto e genera una sequenza di transazioni come risultato dell'esecuzione, il comitato intero poi produce un certificato firmato che approva il risultato. Infine il certificato e le transazioni vengono presentati al comitato di consenso (*consensus committee*, che si occupa di validare i blocchi). In questo modo il comitato di esecuzione dei contratti svolge il lavoro più oneroso senza togliere risorse alle transazioni di primo livello, mentre il comitato di consenso dovrà solamente approvare il certificato e le transazioni prodotte off-chain.

2.1.1 Struttura della rete

La rete Algorand prevede due tipologie di nodi al fine di ottimizzare la gestione del flusso di transazioni e di massimizzare la decentralizzazione: i *Relay Nodes* e i *Participation Nodes*.

Relay Nodes

Traducibile in italiano con "nodi di inoltro", servono a garantire la connettività della rete. Per questo motivo non ci sono requisiti prestazionali per i relay nodes, ma si richiede che siano collegati alla rete attraverso una connessione affidabile e veloce in modo da poter gestire contemporaneamente un numero elevato di comunicazioni da e verso altri nodi. Il compito di questi nodi è abbastanza semplice: ricevono i messaggi del protocollo dai participation nodes (o dai relay nodes, che a loro volta li hanno ricevuti dai participation), effettuano rapide verifiche di validità e integrità e inoltrano il messaggio verso nodo il destinatario.

Il protocollo non prevede ricompense per chi configura un nuovo nodo della rete, ma di tanto in tanto la fondazione annuncia dei programmi di inserimento di nuovi relay nodes in cui vengono selezionate università, aziende ed utenti della community che potranno aggiungere un nodo alla rete in cambio di una ricompensa economica. Dunque non è possibile inserire liberamente un nodo nella rete ma è necessaria l'autorizzazione della fondazione. Ad oggi ci sono circa 120 relay nodes attivi che garantiscono il funzionamento della rete decentralizzata.

Sebbene questo sistema non sia completamente democratico e decentralizzato poiché la fondazione decide chi può configurare un nodo della rete, ciò garantisce che la backbone della rete sia robusta ed affidabile oltre a garantire un controllo sulla scalabilità: qualora fossero necessari più relay nodes per aumentare la velocità di inoltro dei messaggi nella rete, la fondazione potrebbe intervenire rapidamente. Infine la fondazione e la community stanno cercando soluzioni per rendere più decentralizzata questa fase di decisione sui relay nodes.

Participation Nodes

Sono i nodi che permettono agli utenti la partecipazione al protocollo di consenso, infatti essi hanno in memoria le chiavi di partecipazione degli utenti e attraverso esse possono

proporre e votare i nuovi blocchi per conto degli utenti. Questa tipologia di nodi è quella più comune, qualsiasi utente può configurare il proprio computer come nodo di partecipazione ed è incoraggiato a farlo poiché facendolo aumenta la sicurezza del protocollo e la decentralizzazione della rete: se la maggioranza dei participation nodes esegue correttamente il protocollo di consenso è garantito che non avverranno fork nella blockchain e dunque si prevengono gli attacchi che sfruttano le fork.

Fonti

Algorand's Smart Contract Architecture, Silvio Micali, Algorand Blog
Algorand Network Architecture, Algorand Foundation

2.2 La curva ellittica Curve25519

2.2.1 Le curve in forma di Montgomery

La curva ellittica usata da Algorand è la curva Curve25519, la cui rappresentazione è:

$$y^2 = x^3 + 486662x^2 + x$$

La curva è espressa in forma di Montgomery, cioè è del tipo:

$$M_{A,B} : By^2 = x^3 + Ax^2 + x$$

con $A, B \in K$, cioè il campo finito scelto. Inoltre A e B vengono scelti in modo tale che $B(A^2 - 4) \neq 0$, ovvero $B \neq 0$ e $A \neq \pm 2$. .

- divisione del LHS e del RHS per B^3:

$$\frac{y^2}{B^2} = \frac{x^3}{B^3} + \frac{Ax^2}{B^3} + \frac{x}{B^3}$$

- sostituzione di variabili $u = \frac{x}{B}$ e $v = \frac{y}{B}$:

$$v^2 = u^3 + \frac{A}{B}u^2 + \frac{1}{B^2}u$$

- sostituzione di u con $t - \frac{A}{3B}$:

$$v^2 = t^3 + (\frac{3 - A^2}{3B^2})t + (\frac{2A^3 - 9A}{27B^3})$$

Non è necessariamente possibile il contrario, cioè passare dalla forma di Weierstrass a quella di Montgomery, infatti ciò è possibile se e solo se:

- $x^3 + ax + b = 0$ ha almeno una radice $\alpha \in F$

- $3\alpha^2 + a$ è un residuo quadratico in F

date queste condizioni si può definire il mapping inverso dalla forma di Weierstrass a quella di Montgomery:

$$E_{a,b} : v^2 = t^3 + at + b$$

$$(t, v) \mapsto (x, y) = \left(\frac{t - \alpha}{\sqrt{3\alpha^2 - a}}, \frac{v}{\sqrt{3\alpha^2 - a}} \right)$$

$$A = \frac{3\alpha}{\sqrt{3\alpha^2 - a}} \; B = \frac{1}{\sqrt{3\alpha^2 - a}}$$

2.2.2 Aritmetica delle curve di Montgomery

Sulle curve ellittiche in forma di Montgomery, dati due punti $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$, è possibile definire $P_3 = P_1 + P_2$, che geometricamente consiste nel punto ottenuto intersecando la retta congiungente P_1, P_2 e la curva ellittica, e invertendo il segno della coordinata y.

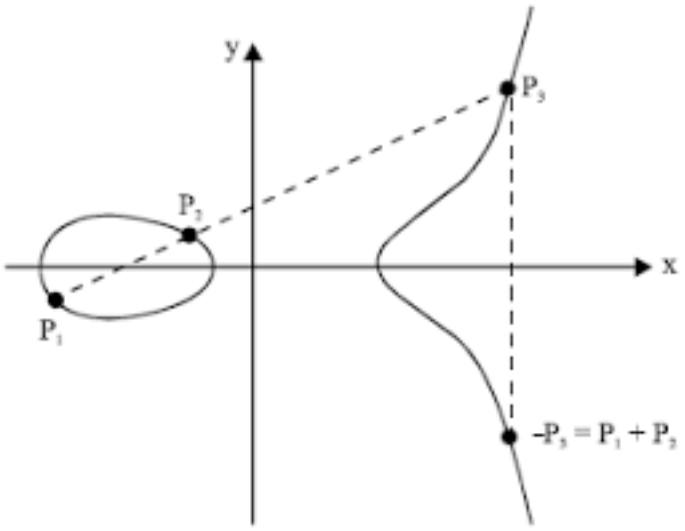


Figura 2.1. Somma su curve ellittiche

Il punto P_3 può essere ricavato da P_1, P_2 nel seguente modo (tutti i calcoli sono svolti su Z_p):

- il coefficiente angolare della retta $y = \lambda x + q$ che unisce P_1e P_2 è facilmente ottenibile:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ e dunque } q = y_1 - \lambda x_1$$

- intersecando la retta ottenuta e la curva ellittica (cioè sostituendo y con $\lambda x + q$ si ottiene il punto P_3:

$$x^3 + (A - B\lambda^2)x^2 + (1 - 2B\lambda q)x - Bq^2 = 0.$$

avendo tre radici può essere espressa come:

$$(x - x_{P_1})(x - x_{P_2})(x - x_{P_3}) = 0$$

dunque sviluppando la seconda espressione e la prima si ottiene che:

$$-x_1 - x_2 - x_3 = A - B\lambda^2$$

che implica:

$$x_3 = B\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - A - x_1 - x_2$$

- infine inserendo x_3 in $y = \lambda x + q$ e cambiando di segno all'espressione ottenuta:

$$y_3 = \frac{(2x_1 + x_2 + A)(y_2 - y_1)}{x_2 - x_1} - \frac{B(y_2 - y_1)^3}{(x_2 - x_1)^3} - y_1$$

in modo analogo è possibile definire il doubling di un punto $2P = P + P$ (e in modo simile dunque kP.
In questo caso la retta congiungente P_1 e P_2 è sostituita dalla retta tangente alla curva ellittica in P, dunque $\lambda = -\frac{\partial f}{\partial x} \Big/ \frac{\partial f}{\partial y}$.
L'espressione di $2P$ é:

$$\begin{aligned} x_3 &= \frac{B(3x_1^2 + 2Ax_1 + 1)^2}{(2By_1)^2} - A - x_1 - x_1 \\ y_3 &= \frac{(2x_1 + x_1 + A)(3{x_1}^2 + 2Ax_1 + 1)}{2By_1} - \frac{B(3{x_1}^2 + 2Ax_1 + 1)^3}{(2By_1)^3} - y_1. \end{aligned}$$

2.2.3 La curva Curve25519

Come già detto, la curva Curve25519, è un esempio di curva in forma di Montgomery, in particolare è una delle curve più veloci fra quelle non coperte da alcun brevetto. È introdotta nel 2005 da Daniel J. Bernstein, ed offre delle chiavi di lunghezza 256 bit. Scendendo nel dettaglio, Bernstein nel suo lavoro descrive e motiva la scelta dei parametri (Bernstein [2006]):

- $p = 2^{255} - 19$ dev'essere un primo abbastanza grande da evitare attacchi, e vicino ad una potenza di 2 per motivi computazionali.

- $B = 1$ e $A = 486662$, infatti $\frac{A-2}{4}$ dev'essere un intero piccolo per facilitare la moltiplicazione per $\frac{A-2}{4}$, usata nell'algoritmo per il doubling dei punti. Inoltre la curva deve avere un'ordine $4n$ o $8n$, con $n > 2^{252}$ primo, per generare delle chiavi evitando il caso in cui la chiave generata sia pari all'ordine.
- Base point: $(9, y)$ affinché l'ordine sia un primo grande, ed evitare "small subgroup attacks".

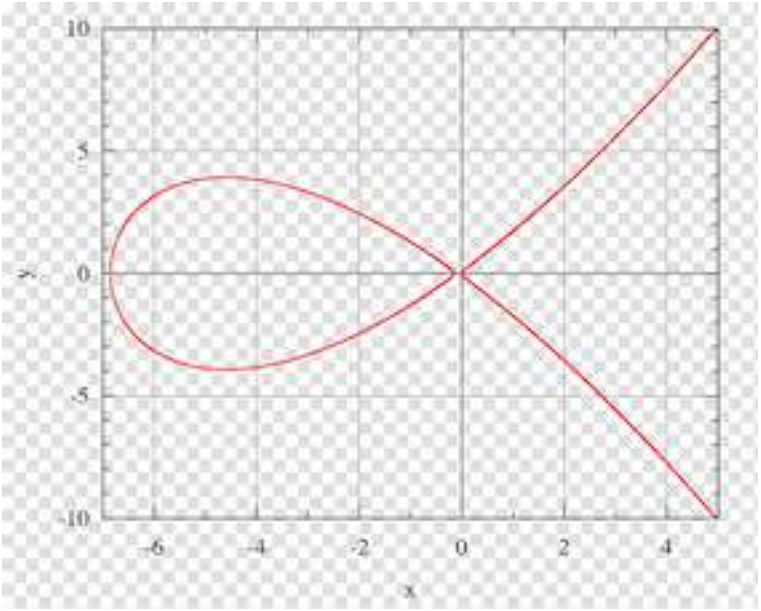


Figura 2.2. Rappresentazione della Curve25519

2.3 Governance e Algorand Governors

Il programma di governance di Algorand è legato al processo decisionale dell'utilizzo dell'Algorand Ecosystem Resources Pool (AERP). L'AERP è composto da cinque fondi separati, dedicati a sostenere lo sviluppo della rete e dell'ecosistema Algorand, con l'obiettivo di costruire una rete blockchain pubblica robusta, decentralizzata, ampiamente adottata e utilizzata. Questi fondi sono programmati per essere messi in circolazione fino al 2030. Inizialmente queste decisioni venivano prese solamente dalla Fondazione mentre gli altri utenti potevano partecipare solamente al consenso. La versione di consenso si può vedere come la lingua che ogni nodo parla con gli altri. È essenziale quindi che ogni nodo abbia la stessa versione in modo che la rete possa funzionare correttamente.

Il 10 giugno 2021[1] la Fondazione annuncia un referendum su tutto il network riguardo il programma di governance. Il referendum propone il passaggio a una governance decentralizzata dove saranno gli utenti a poter votare e prendere decisioni. Tutti gli account Algorand online che partecipano al consenso possono votare. Il 30 giugno 2021 il referendum è stato avviato ed esistono solo due opzioni di voto: SI e NO. Per votare sì un nodo deve installare l'aggiornamento proposto mentre per il no non bisogna fare nulla. Il referendum passa se almeno il 90% dei nodi sarà d'accordo e avrà aggiornato il software entro il 14 luglio 2021.

A partire dal 1° ottobre 2021[2], in seguito a un referendum, la governance di Algorand è passata a un modello completamente decentralizzato nel quale sono i titolari di Algo a prendere le decisioni tramite una votazione. Chi partecipa alla governance è detto governatore ed avrà un ruolo sempre più responsabile nelle decisioni economiche e politiche. Per essere governatore bisogna possedere un wallet e detenere Algo che andranno tenuti in staking per un certo periodo. Per ogni anno ci sono quattro periodi di voto trimestrali. Alla fine di ognuno i governatori che avranno rispettato i requisiti riceveranno una ricompensa in base al numero di Algo tenuti in staking in tale trimestre. Per ogni periodo di governance ci sarà almeno una sessione di voto e i governatori potranno votare sì, no oppure votare in accordo con la Fondazione. È importante far notare che la Fondazione non parteciperà alle votazioni ma le organizzerà solamente, assumendo il ruolo di supervisore e impegnandosi a renderle semplici e intuitive.

Il programma di governance segna il passaggio dai primi giorni della rete Algorand a una fase più matura in cui la comunità prenderà in mano il proprio destino e le ricompense saranno distribuite in cambio di un impegno verificabile.

2.3.1 Sessioni di voto

Di seguito vengono elencate per ogni trimestre le proposte di voto.

[1] News referendum: https://algorand.foundation/it/news/algorand-governance-referendum

[2] Governance: https://algorand.foundation/it/governance-it

1° periodo di voto (quarto trimestre 2021)

Nel primo periodo di voto è stato chiesto ai governatori se aumentare le ricompense di governance stanziate per il 2022, passando da 282 milioni a 362 milioni e cambiare il meccanismo di voto nel seguente modo: i governatori che non votano o che non mantengono in staking gli algo per il periodo stabilito incorrono in una decurtazione del 8% dell'importo messo in staking. La somma degli importi decurtati andrà poi a finire nel AERP e quindi tornerebbe nel sistema.
I governors hanno scelto di non adottare questo cambiamento.

2° periodo di voto (primo semestre 2022)

In questo periodo di votazioni è stato chiesto se adottare un nuovo sistema di governance. Il nuovo sistema consiste nella creazione di un nuovo livello di governatori ovvero gli Expert Governors (xGovs), i quali attraverso un meccanismo decentralizzato come il DAO (Decentralized Autonomous Organization) abbiano il potere di proporre delle decisioni da sottoporre ai governatori durante i trimestri di voto. Regole più approfondite riguardo gli xGov verranno discusse in futuro nel caso la proposta venga approvata.
L'esito della votazione questa volta è stato positivo.

3° periodo di voto (secondo trimestre 2022)

In questo terzo periodo di voto sono state proposte due votazioni differenti.
La **prima proposta** riguarda la possibilità di far partecipare alla governance anche i progetti DeFi qualificati dando un peso doppio al loro voto ma mantenendo le ricompense uguali agli altri.
La **seconda proposta** è una continuazione riguardo le regole da adottare con il nuovo sistema di governance introdotto nella scorsa sessione di votazione. Si vuole creare un meccanismo dove la community può fare delle proposte che verranno considerate dagli xGovs ed eventualmente messe a voto.
I risultati non sono ancora disponibili perchè la sessione non è ancora conclusa (agg. 02/06/2022).

Fonti

Decentrare la governance di Algorand, Algorand Foundation
Algorand Governance Proposals, Algorand Foundation

2.4 Meccanismo di consenso: Pure-Proof-of-Stake

Il protocollo di consenso usato dalla Algorand Blockchain, è noto come Pure Proof of Stake (PPoS): un meccanismo di consenso senza autorizzazione e specifico per questa blockchain. Garantisce piena partecipazione, protezione blockchain e buone velocità di trasferimento, in una rete veramente decentralizzata ed è per questi motivi che con la creazione di questo protocollo Micali e il suo gruppo di ricerca mirano a risolvere il problema del trilemma

(presentato in (1.1)).

Assunzioni Prima di analizzare il protocollo PPoS, è importante evidenziare alcune assunzioni che vengono previste sulla rete.
La prima ipotesi è nota con il nome di *Honesty Majority*: questo implica che il numero di utenti onesti deve essere $> \frac{2}{3}$ rispetto al numero di utenti totali. Questa assunzione è analoga a considerare il 51% della potenza di calcolo in una rete di tipo Bitcoin.
L'ipotesi *Honesty Majority of Money* è necessaria per considerare che gli utenti onesti posseggano più della metà di tutta la valuta del sistema al round $r - k$ precedente. Il round rappresenta l'unità logica di organizzazione di Algorand.
Inoltre la *Computational Power* viene distribuita su tutti gli utenti.
Infine si considera che un *messaggio* inviato al tempo $t - \lambda_{\rho,\mu}$ in un tempo t raggiungerà almeno un frazione pari a ρ utenti onesti, con $\rho > 95\%$, μ che indica il numero di byte del messaggio.

Selezione dei validatori Per prima cosa è necessario scegliere i validatori. Nella Proof of Stake la scelta dipende dalla quantità di moneta posseduta; nel caso della Pure Proof of Stake si aggiunge anche una probabilità randomica. Questo rende un attaccante non in grado di corrompere i validatori prima che questi abbiano inserito il blocco nella blockchain. La procedura di selezione casuale si basa sulla *Verifiable Random Function* (funzione casuale verificabile, VRF): una quantità di moneta viene messa a garanzia e più questo "stake" è grande, più alta è la probabilità che quel nodo venga scelto per l'inserimento di un nuovo blocco.

Ogni investitore che possiede ₳ può prendere parte al protocollo di consenso semplicemente generando una chiave di partecipazione con la quale è possibile partecipare alla proposta e alla votazione dei blocchi. Ogni blocco in Algorand include un "selection seed", che è casuale e imprevedibile, quest'ultimo determina e decide quali utenti dovrebbero partecipare come validatori al prossimo round del protocollo di consenso. Quando il nuovo blocco viene aggiunto alla blockchain, tutti gli utenti vedranno questo selection seed. Ogni utente che si è proposto come validatore può controllare segretamente se è stato selezionato per partecipare valutando una VRF, con l'ausilio della chiave di partecipazione che possiede e in base a quel selection seed. Il calcolo VRF produce quindi un output pseudocasuale, con una prova crittografica che chiunque può utilizzare per verificare il risultato. Conservando o inviando tale prova, un utente può dimostrare in qualsiasi momento di essere stato effettivamente selezionato per partecipare al meccanismo di consenso.
Ogni utente calcola

$$VRF_{sk}(seed||role)$$

con sk chiave segreta dell'utente, per scoprire se è stato scelto per essere il validatore. Quando il blocco è stato inserito, ogni utente della rete può verificare il ruolo dei validatori tramite la funzione

$$VerifySort_{pk}$$

con pk chiave pubblica del validatore.
La scelta del seed viene effettuata anche questa in modo casuale per evitare eventuali attacchi.
Definita W la quantità totale di ALGO presente nel sistema e τ la soglia per selezionare un certo numero di utenti per un determinato ruolo, la probabilità per ogni unità di valuta per ogni nodo di essere scelto è

$$p = \frac{\tau}{W}$$

Questo metodo, quindi, permette di selezionare gli utenti in base alla quantità di valuta che posseggono, ma scelti in modo casuale. Inoltre un avversario non sa in anticipo se un utente verrà selezionato perché non ha accesso alla sua chiave privata sk. Quando gli utenti selezionati iniziano a diffondere la prova insieme al proprio parere sul blocco da aggiungere, un attaccante può provare ad attaccarli. A questo punto, però, (come afferma anche Micali) è troppo tardi e non è più possibile richiamare il messaggio.

Votazione e aggiunta del blocco Il meccanismo di consenso Pure Proof of Stake si sviluppa in 3 passaggi per poter inserire un nuovo blocco nella blockchain. E' importante sottolineare che in questo protocollo sono presenti due gruppi di utenti: un gruppo di utenti con il preciso scopo di "validatori", mentre vi è un secondo gruppo con il compito di proporre i blocchi. La probabilità, per ogni utente, di essere scelto in uno dei gruppi è proporzionale alla quantità di Ⱥ che sono stati messi in stake dall'utente stesso.

1. Proposta: Ogni nodo tramite la funzione VRF determina quali account sono online e disposti a partecipare, inviando le informazioni al resto dei nodi della rete. Quindi, ogni nodo riceve proposte di blocco dal resto dei nodi sulla rete, insieme all'output della VRF, che dimostra che tali proposte sono valide. È qui, quindi, che vengono selezionati i candidati validatori.

2. Soft Vote: Ogni nodo della rete esegue il calcolo della VRF per analizzare se l'account è stato scelto per partecipare al *Soft Vote*. In caso affermativo, quell'account otterrà un numero di voti proporzionale alla quantità di ALGO che possiede. Tra tutte le proposte viene selezionata quella con priorità maggiore. La priorità è calcolata facendo una hash dell'output della funzione VRF. Raggiunto il quorum per il *Soft Vote*, il processo passa alla fase di certificazione del voto.

3. Certificazione del voto e inserimento del blocco nella blockchain: In questa fase viene selezionato un nuovo gruppo di nodi per verificare la proposta di blocco risultante dal *Soft Vote*. Se non vengono individuati overspending e double-spending (o altre deviazioni), il blocco è considerato valido e la commissione lo certifica quindi come tale.
   Se il blocco non viene approvato, allora si ha l'inserimento di un blocco vuoto nella blockchain.

In conclusione, quindi, il meccanismo di consenso Pure Proof of Stake è una variante della Proof of Stake, in cui i validatori di un nuovo blocco non vengono selezionati solo in

base al numero di token che hanno messo in "stake" ma anche casualmente attraverso la Verifiable Random Function (VRF). Tutti gli utenti online hanno la possibilità di essere scelti per proporre un blocco e votare.
Questo protocollo sceglie casualmente i blocchi leader, mantenendo segreto lo stato dei validatori fino a quando le transazioni non sono state confermate come corrette.

2.4.1 Confronto PPoS con le altre prove di lavoro

PPoS vs PoW La Proof of Work (PoW) è un approccio in cui gli utenti gareggiano per risolvere un problema crittografico molto complesso (si veda la PoW per la blockchain Bitcoin). Il primo miner che trova la soluzione ha il diritto di attaccare il blocco e riceve il compenso per il lavoro svolto.
La PoW richiede l'utilizzo di hardware specializzati per essere competitivi e inoltre registra un enorme consumo di elettricità. Solo i miner professionisti hanno, quindi, la possibilità di partecipare alla generazione di nuovi blocchi e quindi solo questi riceveranno il compenso.
Al contrario, la PPoS non richiede di risolvere un enigma crittografico, ma tutti gli utenti che sono online e che posseggono criptovaluta hanno la possibilità di essere scelti per partecipare al voto. La generazione dei blocchi non richiede un calcolo computazionale costoso, la potenza di calcolo per verificare la VRF necessaria è minima, quindi è possibile utilizzare anche un dispositivo con risorse limitate.
Inoltre con la PoW si verifica una concentrazione della potenza di calcolo in 2/3 mining pool e questo porta ad una centralizzazione della rete. In Algorand, invece, questo non accade. Un utente può aumentare la probabilità di essere scelto solo aumentando il suo stake.
In sistemi di PoW (i.e. Bitcoin) viene inserito un nuovo blocco in media ogni 10 minuti. Questo porta a diminuire la scalabilità della rete che, se usata in campo economico, non riuscirebbe a gestire un numero elevato di transazioni da eseguire in breve tempo. Nella blockchain di Algorand questo rischio non si corre: infatti i blocchi vengono inseriti in qualche secondo perché non richiedono di risolvere un difficile problema. Il protocollo è quindi in grado di gestire milioni di utenti e di reggere un alto rate di transazioni.
Per quanto riguarda la formazione di forks invece, queste non si realizzano in Algorand perché un solo blocco supera la fase di votazione e quindi un solo blocco può essere certificato in ogni round.

PPoS vs DPoS La Delegated Proof of Stake (DPoS) è un approccio in cui viene selezionato un numero fisso di delegati che possono creare un nuovo blocco. I delegati vengono votati dagli utenti della rete e ricevono un numero di voti proporzionale ai token che possiedono. Il numero di generatori di nuovi blocchi è, quindi, limitato. La DPoS è in grado di gestire un flusso di transazioni con ordini di grandezza superiore rispetto a quelli della PoW, ma risulta essere intrinsecamente centralizzata. Non vi è alcuna garanzia che tutti i delegati rimarranno onesti e anche se la loro onestà fosse una certezza, possono essere facilmente attaccati perché sono noti. Un avversario potrebbe far cadere tutti i delegati

con un attacco Fast Denial of Service.
Al contrario, PPoS non considera un piccolo gruppo di utenti responsabile della generazione dei blocchi e gli utenti non hanno bisogno di delegare il proprio potere di voto a pochi eletti. Ogni utente può proporre e votare blocchi con una probabilità direttamente proporzionale al proprio stake e non esiste un gruppo speciale di utenti noto che un attaccante possa prendere di mira.

PPoS vs BPoS La Bonded Proof of Stake (BPoS) segue un approccio in cui ogni utente mette da parte uno stake (i.e. una obbligazione) per influenzare la generazione dei blocchi. Gli utenti depositano una parte del loro stake per un certo periodo di tempo e ricevono in cambio una possibilità, proporzionale allo stake, di inserire il prossimo blocco nella blokchain. Il protocollo prevede che il voto di ogni utente abbia un peso proporzionale con lo stake che è stato depositato. Una volta depositato, lo stake non può essere toccato per un periodo di tempo specifico. Questo riduce la capacità dell'utente di spendere il suo stake partecipando al protocollo di consenso.
Al contrario la PPoS di Algorand non prevede alcun deposito di valuta, gli utenti sono liberi di spendere il loro stake in ogni istante di tempo. Tutto l'ammontare della valuta in gioco è sempre dove dovrebbe essere: nei portafogli degli utenti pronti per essere spesi o nei vari strumenti finanziari alla base della blockchain di Algorand.

2.4.2 Ricompensa per i miners

La blockchain di Algorand è una delle poche blockchain che permetteva (fino al 14/05/2022) di ottenere dei premi semplicemente detenendo dei token ALGO sul proprio wallet. Lo staking avveniva in maniera automatica, con la necessità solo di avere un wallet dedicato. Questi premi provenivano da delle pool predisposte che, ad ogni blocco generato, rilasciavano un importo di ALGO da distribuire alla rete. Dato che un nuovo blocco viene creato in media ogni 4 secondi, anche il premio veniva corrisposto in modo rapido. Per ricevere il premio era sufficiente effettuare una transazione per vedere aggiunto all'importo ricevuto il premio spettante.
Tuttavia i fondi stanziati per i *participation rewards* sono terminati e dal 14/05/2022 non è più possibile ricevere questi premi, la nuova modalità per ricevere ricompense di partecipazione al sistema distribuito è attraverso la governance ovvero la partecipazione al sistema di decisioni sulle modifiche al protocollo.

Fonti

Algorand's Pure Proof of Stake Approach, Algorand.com
Cos'è la Pure Proof of Stake, Cryptorobin.it
Algorand: Come funzionano i premi della blockchain, Cryptonomist.ch
Why Algo?, Algorand Developer Portal

2.5 Wallet

Per effettuare una prova pratica di transazione su Algorand abbiamo sfruttato la TestNet: una chain indipendente da quella principale che può essere utilizzata dagli sviluppatori per testare le dApp in fase di sviluppo prima di inviarle alla blockchain ufficiale. Sulla TestNet le criptomonete non hanno alcun valore reale e non possono essere trasferite ad un indirizzo della MainNet, perciò gli utenti possono effettuare transazioni di qualsiasi entità senza preoccuparsi di perdere denaro.

Per creare un indirizzo abbiamo utilizzato il wallet MyAlgo[3], che permette di operare sia sulla MainNet che sulla TestNet. La procedura è molto semplice: è sufficiente inserire una password di sicurezza e successivamente richiedere la generazione della frase mnemonica (menmonic phrase) costituita da 25 parole ordinate, questa frase rappresenta il seme (seed) utilizzato per generare la chiave privata del wallet. Una volta che la frase è stata trascritta in modo sicuro e si è superata una breve verifica possiamo utilizzare il nostro wallet.

Mnemonic phrase La frase mnemonica è una rappresentazione human-readable della chiave privata del wallet attraverso 25 parole in lingua inglese, generata nel seguente modo:

- attraverso operazioni logiche che prendono in input la chiave privata vengono generate 24 stringhe da 11 bit ciascuna
- ciascuna stringa è interpretata come numero intero (nell'intervallo 0-2047 poiché ci sono $2^{11} = 2048$ combinazioni possibili)
- ogni numero intero è mappato in una parola dello standard BIP-39.

Si ottengono così 24 parole, l'ultima rappresenta il checksum ed è calcolata utilizzando i primi 2 byte della hash SHA512/256 della chiave privata, trasformati in un intero di 11 bit che viene mappato in una parola dello standard BIP-39 come prima. La frase mnemonica può essere utilizzata per recuperare l'accesso al wallet poiché rappresenta la chiave privata in modo univoco, per questo motivo essa deve essere trascritta in modo sicuro, meglio se su un supporto cartaceo e non attaccabile per via informatica.

Password La chiave privata viene memorizzata sul dispositivo dell'utente in forma cifrata attraverso una password: l'utente dovrà inserire la password per decifrare la chiave e poter accedere al wallet. In questo modo l'unica informazione che l'utente dovrà ricordare è la password da lui scelta.

Fonti

Understanding Mnemonic Keys And How Are They Generated, Blaise Bayuo, Algorand Community Blog

[3]Wallet MyAlgo: `https://wallet.myalgo.com/`

2.6 Transazioni

La struttura di una transazione sulla blockchain Algorand rappresentata in formato JSON è la seguente:


```
{
  "txn": {
    "amt": 5000000,
    "fee": 1000,
    "fv": 6000000,
    "gen": "mainnet-v1.0",
    "gh": "wGHE2Pwdvd7S12BL5FaOP20EGYesN73ktiC1qzkkit8=",
    "lv": 6001000,
    "note": "SGVsbG8gV29ybGQ=",
    "rcv": "GD64YIY3TWGDMCNPP553DZPPR6LDUSFQOIJVFDPPXWEG3FVOJCCDBBHU5A",
    "snd": "EW64GC6F24M7NDSC5R3ES4YUVE3ZXXNMARJHDCCCLIHZU6TBEOC7XRSBG4",
    "type": "pay"
  }
}
```


- `"amt"` riporta la quantità da trasferire dal mittente (`"snd"`) al destinatario (`"rcv"`), misurata in microALGOs
- `"fee"` riporta le commissioni pagate per la transazione
- `"fw"` e `"lw"` rappresentano l'intervallo di validità della transazione, in questo caso la transazione è valida se inserita tra il blocco `6000000` e il blocco `6001000`
- `"gen"` è l'ID del blocco genesi che rappresenta la chain, tuttavia non c'è garanzia che questo ID sia univoco, per questo motivo si riporta il Genesis Hash `"gh"`
- `"type"` rappresenta la tipologia della transazione, in questo caso è un trasferimento di criptovaluta (`"pay"`)
- `"note"` è un campo opzionale che riporta la codifica Base64 di un'annotazione inserita dall'utente, che può occupare fino a 1000 bytes.

La transazione mostrata è di tipo *payment*, ha cioè l'obiettivo di trasferire moneta da un indirizzo ad un altro. Il protocollo Algorand, a differenza di quello Bitcoin, non obbliga il mittente a spendere tutte le criptomonete in suo possesso. Ciò significa che non è necessario indicare un secondo indirizzo destinatario a cui dare il resto del pagamento. Tuttavia è possibile decidere di "chiudere" l'account mittente al termine della transazione, in questo caso si dovrà indicare l'indirizzo a cui trasferire l'ammontare di criptovaluta rimanente dopo il pagamento, attraverso la proprietà `"close"`.

Questa tipologia di transazione viene utilizzata anche per registrare sulla blockchain i voti degli utenti che partecipano alla governance: ad ogni voto di un utente corrisponde una transazione di 0 Ⱥ verso un indirizzo predisposto dalla fondazione. Il voto espresso viene inserito nel campo `"note"` della transazione.

2.6.1 Altre Tipologie di Transazioni

Come visto il protocollo Algorand prevede l'indicazione del tipo di transazione attraverso la proprietà `"type"`, oltre alle transazioni di tipo *payment* esistono altre cinque tipologie di transazione:

Key Registration

Questa tipologia di transazione viene utilizzata per registrare un account e permettere la partecipazione al meccanismo di consenso.

Ci sono alcune proprietà che differiscono da una transazione *payment*:

- `"selkey"` è la chiave pubblica utilizzata all'interno della Verifiable Random Function che permetterà di verificare se l'account è stato selezionato per il meccanismo di voting;
- `"votekey"` è una chiave pubblica di partecipazione associata all'indirizzo `"snd"`;
- `"votefst"` e `"votelst"` rappresentano rispettivamente il primo e l'ultimo blocco in cui la chiave di partecipazione è valida;
- `"votekd"` rappresenta il numero di round per la generazione di nuove chiavi.

Application Call

Questa tipologia di transazioni è utilizzata per eseguire una dApp presente sulla blockchain, i parametri principali di questo tipo di transazione sono due: l'id univoco dell'applicazione (`"apid"`) da eseguire ed un intero che rappresenta eventuali azioni da eseguire al termine dell'esecuzione (`"apan"`).
Ci sono poi molti altri parametri che è possibile configurare in base a ciò che si vuole fare con la dApp: è possibile indicare con quali altre dApp può interagire, a quali account può accedere, il limite massimo di variabili che può utilizzare nello storage locale e/o globale...

Asset Configuration

Sono le transazioni utilizzare per la creazione di un asset, prevedono la possibilità di specificare parametri quali il nome (`"an"`), l'unità di misura (`"un"`), la quantità totale dell'asset (`"t"`) e gli indirizzi degli account preposti ad operare sull'asset:

- `"m"` (`manager`) è l'indirizzo dell'account manager, cioè colui che può modificare la configurazione dell'asset e distruggerlo;
- `"r"` (`reserve`) è l'indirizzo che detiene la riserva, cioè la quantità di asset che non è ancora stata coniata;
- `"f"` (`freeze`) è l'indirizzo che può congelare tutti i possedimenti dell'asset, se non viene specificato non è possibile effettuare il congelamento (freezing);

- `"c"` (`clawback`) è l'indirizzo che può recuperare (reclamare) tutti i possedimenti dell'asset.

Nel caso in cui si indichi anche l'id univoco dell'asset (proprietà `"caid"`), la transazione diventa una transazione di riconfigurazione e permette di cambiare i parametri impostati alla creazione.

Asset Transfer

Questa tipologia di transazioni si indica con `"type": "axfer"` e vengono utilizzate per trasferire una certa quantità di un asset tra due indirizzi. Sono simili alle transazioni di pagamento, ma anziché trasferire criptovaluta si trasferisce un determinato asset creato in precedenza. Si indica il destinatario dell'asset (`"arcv"`), il mittente (`"snd"`), l'id dell'asset (`"xaid"`) e la quantità da trasferire (`"aamt"`).
Con questa tipologia di transazioni è possibile anche revocare un asset: semplicemente indicando lo stesso indirizzo nei due campi mittente (`"snd"`) e destinatario dell'asset (`"arcv"`) ed indicando come mittente dell'asset (`"asnd"`) l'indirizzo a cui si vuole revocare l'asset. Perché la transazione venga approvata è necessario che l'indirizzo che sta attuando la revoca e che riceverà l'asset sia stato indicato precedentemente come indirizzo di clawback.

Asset Freeze

Quest'ultima tipologia di transazioni permette di congelare (e quindi bloccare l'invio/-ricezione) o decongelare (e quindi permettere nuovamente l'invio/ricezione) un determinato asset in possesso dell'indirizzo freeze (`"fadd"`). Per congelare l'asset si indica `"afrz": true`, per scongelarlo si indica `"afrz": false`.

Fonti

Transaction Structure, Algorand Developer Portal

Capitolo 3

Sostenibilità, Applicazioni e Casi d'Uso

3.1 Ecosostenibilità

La fondazione definisce Algorand "The Green Blockchain", soprattutto grazie alla minima quantità di energia richiesta dal protocollo di consenso basato sulla PPoS (vedi la sezione 2.4.2 per il confronto con le altre tipologie di prove di lavoro). La minima quantità di capacità di calcolo richiesta per la validazione dei blocchi permette di utilizzare come Participation Nodes computer che consumano pochissima energia come il Raspberry Pi 4, un mini-computer confrontabile con uno smartphone in termini di dimensioni e consumi.

Supponendo di avere circa 4000 nodi validatori nella rete che utilizzano computer di questo tipo, viene stimato che ogni transazione finalizzata richieda un consumo di energia di circa $0{,}008Wh$. Il vantaggio rispetto alle blockchain di prima generazione è che non ci sono sprechi: le transazioni vengono processate una sola volta e subito inserite in un blocco, non ci sono blocchi *stale* che sono stati inseriti e successivamente scartati e non ci sono più utenti che lavorano in competizione sullo stesso problema.
Per le blockchain Bitcoin ed Ethereum la stima del consumo di energia per transazione è rispettivamente di $930kWh$ e $70kWh$, si parla di circa 7 ed 8 ordini di grandezza di differenza rispettivamente (notare che è stata utilizzata un'unità di misura diversa nel riportare le due quantità, proprio per la diversa scala di grandezza). In termini di emissioni per ogni transazione validata ed inserita nella blockchain si stimano circa $0{,}0000004kg$ di CO_2, 2 milioni di volte meno rispetto alle transazioni Bitcoin.
Anche se queste stime sono molto approssimative ed ottimistiche, rendono l'idea della differenza nella quantità di energia consumata e nell'impatto ambientale per la finalizzazione di una transazione su blockchain diverse.

Infine, con l'obiettivo di diventare una rete *carbon-negative*, Algorand ha avviato una collaborazione con ClimateTrade, dal quale dovrebbe nascere un *oracolo della sostenibilità*. Il ruolo dell'oracolo sarebbe quello di autenticare l'impatto in termini di emissioni di

carbonio della blockchain per ogni epoca. Sfruttando poi degli asset che rappresentano il *carbon credit* ovvero del credito in termini di emissioni generato grazie ad azioni in difesa dell'ambiente, già scambiati sulla blockchain grazie a ClimateTrade, si potranno compensare le emissioni necessarie a far funzionare la blockchain. Sfruttando gli smart contract della rete Algorand è possibili automatizzare tutto ciò, prevedendo una tesoreria green che raccolga e blocchi autonomamente la quantità di asset necessaria a compensare le emissioni o addirittura a rendere il sistema ad emissioni negative.

Fonti

Sustainable Blockchain: Estimating the Carbon Footprint of Algorand's Pure Proof-of-Stake, Algorand Blog
Algorand Pledges to be the Greenest Blockchain with a Carbon-Negative Network Now and in the Future

3.2 Casi d'Uso

Come tutte le blockchain esistono infinite possibilità di utilizzo del sistema Algorand. Qui riportiamo alcune delle applicazioni più interessanti in cui Algorand è stato utilizzato fino ad oggi.

Per rendere l'idea della trasversalità di Algorand, di seguito è riportato un elenco degli ambiti in cui la fondazione trova applicazione:

- **Infrastrutture**
- **Supply chain**
- **Assicurazioni**
- **Settore pubblico**
- **Gaming**
- **DeFi**
- **Eco-Friendly**

Algorand sta costruendo la tecnologia per dare vita al "Futuro della Finanza" (FutureFi), la convergenza di modelli tradizionali e decentralizzati in un sistema unificato che è inclusivo, senza frizioni e sicuro. Algorand ha sviluppato un'infrastruttura blockchain che offre l'interoperabilità e la capacità di gestire il volume di transazioni necessarie alla Defi, alle istituzioni finanziarie e ai governi per una transizione semplice verso il FutureFi. È una tecnologia scelta da più di 500 organizzazioni a livello globale, Algorand consente la semplice creazione di prodotti finanziari, protocolli e scambio di valore di nuova generazione.

3.2.1 Caso della SIAE

Il 24 marzo 2021 è stato annunciato che la SIAE, Società Italiana degli Autori ed Editori fondata nel 1882, rappresenterà i diritti degli autori con asset digitali. L'accordo è stato siglato nel 2019 tramite una partnership tra Algorand e la SIAE. È la prima volta che i diritti d'autore vengono rappresentati come asset digitali.
Sono stati creati più di 4.000.000 di NFTs (Non Fungible Token) che rappresenteranno digitalmente i diritti di oltre 95.000 autori. I token non fungibili (NFT) sono un tipo di asset digitale registrato su blockchain.
Il progetto partito dall'Italia ha tutte le caratteristiche per divenire internazionale. La gestione del diritto d'autore è infatti un tema globale e le soluzioni basate su tecnologia blockchain sono scalabili per definizione.
Con la blockchain un autore che vuole provare che un'opera è sua, non memorizza l'opera nella catena di blocchi ma registra una hash che identifica in modo univoco l'opera. Inoltre la hash consente la verifica dell'autore e fornisce la prova che l'opera esisteva in un certo istante, ma senza rivelarne il contenuto. Quindi la tecnologia blockchain può aiutare nella creazione di un registro di diritti d'autore e diritti connessi, in quanto può facilmente fornire prove del momento della creazione, informazioni sulla gestione dei diritti.
Algorand sarà quindi, un registro decentralizzato, che permette agli autori la gestione personale dei loro diritti e la riscossione dei pagamenti. Questo è possibile grazie agli NFT saranno legati alla moneta digitale. Inoltre è utile a coloro che dovendo usare opere altrui devono capire a chi rivolgersi per le licenze.

Figura 3.1. SIAE e Algorand

3.2.2 Caso Planetwatch

Planetwatch è un'azienda francese con l'obiettivo di costruire una rete globale di sensori per misurare la qualità dell'aria. I dati provenienti dai sensori sono registrati sulla blockchain Algorand, creando il primo ledger globale, decentralizzato e permanente sulla qualità dell'aria. Il framework di gestione e cattura dell'enorme quantità di dati sfrutta il CERN Control and Monitoring Platform (C2MON) che è un framework eterogeneo per l'acquisizione dei dati, offre varie funzionalità ed è utilizzato da più di 10 anni dal CERN. E'

stata scelta la blockchain di Algorand per la sue sicurezza, scalabilità e la qualità "green" che la contraddistingue. Chiunque può partecipare alla rete di sensori, basta comprarne uno e una licenza dal loro sito, seguire le istruzioni e il gioco è fatto. In base al numero di misurazioni che si invieranno si verrà ricompensati con un token basato sulla blockchain Algorand.

Fonti

Siae rappresenta i diritti degli autori con asset digitali, Siae.it
SIAE [...] represents authors' rights as digital assets managed on the Algorand blockchain, SIAE on Algorand.com
How Planetwatch is using Algorand, Algorand.com

Bibliografia

Algorand.com. How planetwatch is using algorand. https://www.algorand.com/ecosystem/use-cases/planetwatch, a.

Algorand.com. Algorand's pure proof of stake approach. https://www.algorand.com/technology/pure-proof-of-stake, b.

Blaise Bayuo. Understanding mnemonic keys and how are they generated. Algorand Community Blog https://community.algorand.org/blog/understanding-mnemonic-keys-and-how-they-are-generated-on-the-algorand-blockchain/.

Daniel J. Bernstein. Curve25519: New diffie-hellman speed records. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *Public Key Cryptography - PKC 2006*, pages 207–228, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. ISBN 978-3-540-33852-9.

Jing Chen and Silvio Micali. Algorand, 2016. URL https://arxiv.org/abs/1607.01341.

Cryptonomist.ch. Algorand: Come funzionano i premi della blockchain. https://cryptonomist.ch/2020/04/26/algorand-premi-blockchain/.

Cryptorobin.it. Cos'è la pure proof of stake. https://cryptorobin.it/cose-la-pure-proof-of-stake.

Algorand Foundation. Decentrare la governance di algorand. https://prismic-io.s3.amazonaws.com/algorandfoundationv2/0eedc44a-54eb-4c9d-82ef-1f7c5b286215_Decentralizing_Algorand_Governance+Proposal_IT.pdf, a.

Algorand Foundation. Algorand governance proposals. https://governance.algorand.foundation/governance-period-3, b.

Algorand Foundation. Algorand network architecture. https://algorand.foundation/algorand-protocol/network/, c.

Algorand News. Algorand pledges to be the greenest blockchain with a carbon-negative network now and in the future. https://www.algorand.com/resources/algorand-announcements/carbon_negative_announcement.

Cosimo Bassi on Algorand Blog. Sustainable blockchain: Estimating the carbon footprint of algorand's pure proof-of-stake. https://www.algorand.com/resources/blog/sustainable-blockchain-calculating-the-carbon-footprint/, a.

Silvio Micali on Algorand Blog. Algorand's smart contract architecture. https://www.algorand.com/resources/blog/algorand-smart-contract-architecture, b.

SIAE on Algorand.com. Siae [...] represents authors' rights as digital assets managed on the algorand blockchain. https://www.algorand.com/resources/ecosystem-announcements/siae-launches-4-million-nfts-on-algorand-for-creators.

Algorand Developer Portal. Transactions structure. https://developer.algorand.org/docs/get-details/transactions/, a.

Algorand Developer Portal. Why algo? https://developer.algorand.org/docs/get-started/basics/why_algorand/#the-consensus-protocol, b.

Siae.it. Siae rappresenta i diritti degli autori con asset digitali. https://www.siae.it/it/iniziative-e-news/siae-rappresenta-i-diritti-degli-autori-con-asset-digitali-creati-più-di-4000000.

HELIUM

The People's Network

Irene Capodicasa, Alessio Dongiovanni, Seyedhossein Javadizavieh, Giacomo Tomasi

Introduzione

Il costante sviluppo delle tecnologie *Internet of Things* sta portando ad una profonda evoluzione degli ambiti in cui trovano applicazione. Si stima che entro il 2025 verrano investiti fino a 15 mila miliardi di dollari nel mercato IoT!
Tuttavia, la maggior parte delle soluzioni che attualmente garantiscono una connessione a Internet (reti cellulari, WiFi, Bluetooth), presentano grandi limiti: sono costose, richiedono un elevato consumo di energia e potenza, e hanno un range di copertura limitato.
Helium è una rete wireless decentralizzata che permette ai dispositivi di connettersi ad Internet e di essere geolocalizzati senza necessità di adottare sistemi di localizzazioni satellitari, o piani di offerta per reti cellulari. L'utilizzo di una Blockchain con un protocollo che incentiva i due segmenti del mercato, lato provider (chi fornisce copertura di rete) e lato cliente (chi usufruisce della rete), permette di decentralizzare un'industria che attualmente, al contrario, risulta fortemente monopolizzata.
Da una parte i dispositivi non si appoggiano più ad un singolo provider, dall'altra i Miners guadagnano tokens fornendo copertura di rete, inserendo transazioni nei blocchi e testando l'integrità della rete.
Helium si pone l'obiettivo di garantire una copertura wireless favorita dalla competizione tra i nodi della rete, accessibile in qualsiasi parte del mondo e più economica delle tecnologie attuali.

Capitolo 1

Blockchain, DWN e componenti della rete

1.1 Il protocollo wireless (WHIP)

1.1.1 Motivazioni

La sua continua ed incessante espansione ha portato Helium ad essere la più grande rete LoRaWAN (Long Range Wide Area Network) del mondo. Questo tipo di tecnologia wireless fornisce una comunicazione Internet a bassa potenza e ampio raggio per dispositivi Smart e sistemi IoT. Tipicamente le reti LoRaWAN presentano un Server centrale, o regionale, gestito da una singola entità.
Il progetto Helium tenta di realizzare un sistema decentralizzato che non utilizzzi protocolli e schemi di modulazione proprietari, e che garantisca accesso alla rete senza la necessità del permesso di un'autorità centrale.
Tale obiettivo ha condotto alla realizzazione di un nuovo protocollo: WHIP.

1.1.2 Caratteristiche e vantaggi del protocollo

WHIP è un protocollo bidirezionale, a lungo raggio, a bassa potenza, ed estremamente sicuro: a differenza dei più usati e conosciuti protocolli di rete wireless, è un protocollo *open-source*.
Il meccanismo di autenticazione utilizza sitemi crittografici a chiave asimmetrica, con chiavi pubbliche che vengono memorizzate nella Blockchain per ogni partecipante della rete. WHIP è un protocollo a banda stretta, il che permette al sistema Helium di realizzare i seguenti obiettivi:

- *Efficienza Spettrale*: le frequenze radio sono una risorsa condivisa limitata, e perciò è necessaria una trasmissione efficiente.
- *Co-esistenza delle Performance*: quando il numero di Devices nella stessa area aumenta considerevolmente, garantire una connessione priva di interferenze diventa un aspetto critico.

- *Range*: la banda stretta consente di effettuare comunicazioni a lungo raggio, con un rate di trasmissione dati che varia a seconda della densità degli Hotspots.

I dispositivi hardware compatibili con WHIP sono in grado di comunicare a distanza di parecchie miglia quadrate negli ambienti urbani (data la notevole densità di ostacoli che limitano la propagazione delle onde radio), e fino a centinaia di miglia quadrate nelle zone rurali!
Inoltre, poichè il consumo energetico richiesto per la connessione alla rete risulta molto contenuto, i dispositivi possono funzionare anche per diversi anni utilizzando delle batterie standard.

1.2 Gli attori della rete Helium

All'interno della rete Helium si individuano diverse tipologie di partecipanti: i *Devices*, i *Miners*, gli *Hotspots* e i *Routers*.

1.2.1 *Devices*

I Devices sono dispositivi hardware contenenti un ricetrasmettitore radio compatibile con il protocollo WHIP, che permette loro di comunicare con gli Hotspots della rete. Tipicamente i Devices sono sensori che trasmetono e ricevono dati cifrati (le firme digitali sono memorizzate all'interno della Blockchain) tramite la rete Internet.
Per poter inviare i dati sulla rete, un Device paga ad un qualsiasi Hotspot nelle vicinanze una commissione (*Transport fee*) quantificata in *Data Credits* [Sezione 4].
Uno degli obiettivi del sistema WHIP è quello di garantire che tali dispositivi possano essere prodotti senza componenti hardware proprietari: i Devices sono infatti realizzati da una vasta varietà di venditori autonomi, e per tale motivo sono venduti a prezzi estremamente bassi (alcuni dispositivi sono disponibili persino a 1$!).

1.2.2 *Miners*

I Miners forniscono copertura di rete wireless alla rete Helium attraverso dei dispositivi hardware costruiti appositamente, gli Hotspots. Questi rappresentano il collegamento tra i Devices, che utilizzano il protocollo WHIP, e Internet.
Gli utenti possono partecipare come Miners della rete Helium acquistando, o costruendo, un dispositivo Hotspot che sia conforme al protocollo. Il compenso (in tokens) derivante dal Mining è proporzionale alla densità di Miners che operano nella stessa area.
Come descritto nelle sezioni successive, l'attività dei Miners è verificata tramite il protocollo di *Proof of Coverage*, e la probabilità di essere eletto per l'inserimento di nuovi blocchi diminuisce in funzione di uno score che viene assegnato dalla rete.

1.2.3 *Hotspots*

Gli Hotspots permettono la trasmissione di dati tra i Routers, su Internet, e i Devices, processano le transazioni e forniscono un servizio di *Proof of Coverage* per la rete Helium

[Sezione 2.2].
Ogni Hotspot è in grado di supportare migliaia di Devices connessi, e fornire copertura su distanze considerevoli. Sono dispositivi che possono connettersi a Internet utilizzando qualsiasi rete TCP/IP, come Ethernet, WiFi o reti cellulari. Contengono un chip capace di ricevere diversi MHz dello spettro di frequenze radio nello stesso istante; l'aspetto positivo di tale struttura è che gli Hotspots possono ascoltare il traffico dati di qualsiasi Device che sia stato trasmesso nello stesso range di frequenze, rendendo non necessaria alcuna sincronizzazione tra Hotspot e Device.
I meccanisimi di localizzazione degli Hotspots, e di ricezione dei paccheti di dati sono descritti in dettaglio nella [Sezione 3].

Attualmente esistono 3 tipologie di Hotspot:

- *Full Hotspots*: rappresentano i *full nodes* della rete. Mantengono una copia completa della Blockchain Helium, prendono parte alla *Proof of Coverage* di altri Hotspots e inoltrano i pacchetti dati sulla rete.
  Svolgono anche il ruolo di *Validators*, entrando a far parte del *Gruppo di Consenso* ([sezione 5]) per inserire un blocco e validando le transazioni prima che vengano inserite nella Blockchain.

- *Light Hotspots*: sfruttano i *full nodes* per ottenere le informazioni sulla Blockchain, intervengono nel protocollo di *Proof of Coverage*, e inoltrano, anch'essi, i pacchetti alla rete.

- *Data Only Hotspots*: sono Hotspots che, a differenza dei primi due, non prendono parte al processo di *Proof of Coverage*. Si limitano a trasmettere i pacchetti di dati.

1.2.4 *Routers*

I Routers sono applicazioni Internet che acquistano dai Miners i dati cifrati dei Devices, e li decrittano. I Devices registrano, all'interno della Blockchain, quali sono i Routers a cui possono essere inviati i propri dati, affinchè qualsiasi Hotspot possa trasmetterli al Router appropriato.
I Routers svolgono diverse funzioni all'interno della rete Helium:

- autenticano i Devices;

- ricevono i pacchetti dati dagli Hotspots e li instradano su Internet;

- inviano messaggi ai Devices attraverso gli Hotspots;

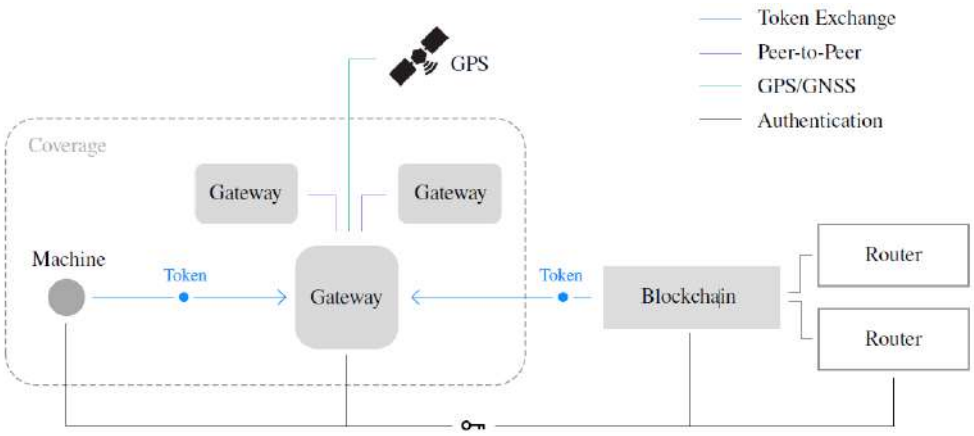
- sono responsabili di fornire conferma della consegna dei pacchetti di dati, in modo da assicurare che le transazioni/operazioni di trasporto siano oneste;

- si accertano che il Miner venga pagato per il proprio servizio;

- forniscono meccanismi di autenticazione e instradamento a servizi cloud di terze parti, come Google Cloud Platform o Microsoft Azure;

- memorizzano e rendono disponibile una copia intera del registro Blockchain operando come dei *full nodes*.

Dopo aver ricevuto un pacchetto dati da un Device, l'Hotspot interroga la Blockchain per determinare quale Routers utilizzare, attraverso l'indirizzo di rete Helium del Device. Chiunque è libero di possedere/ospitare un proprio Router e definire il traffico dei Devices che dovrà essergli consegnato da un Hotspot. In questo modo gli utenti sono in grado di consegnare i dati cifrati solo ad un Router (o un insieme di Routers) specificato.
É una funzionalità analoga a quella fornita da una Virtual Private Network (VPN).



1.3 La blockchain

La rete Helium è una lista immutabile di transazioni, il cui consenso è raggiunto utilizzando un nuovo protocollo (il Protocollo di Consenso di Helium, [Sezione 5]), costruito specificatamente per la DWN (Decentralized Wireless Network).
In un certo periodo, o epoca, un blocco è composto da:

- versione del blocco;
- altezza del blocco;
- hash del Blocco precedente;
- l'hash Merkle delle transazioni al suo interno;
- la firma (*Threshold signature*) digitale del *Gruppo di Consenso* attuale.

Uno degli aspetti più vantaggiosi del meccanismo di validazione delle transazioni è il tasso di inserimento dei blocchi all'interno della Blockcahin: dal momento che il *Gruppo di Consenso* non deve fornire una prova del blocco, è praticamente assente il tempo di "regolamento" previsto da Nakamoto.

Capitolo 2

Proof-of-Coverage e *Proof-of-Serialization*

Uno degli aspetti fondamentali e più innovativi della rete Helium è la *Proof-of-Coverage*. Tale protocollo richiede ai Miners di dar prova della copertura wireless che forniscono ai Devices per comunicare con Internet.
Il sistema di *Proof-of-Serialization*, invece, assicura una corretta sincronizzazione degli eventi registrati sulla Blockchain.
Con la combinazione di *Proof-of-Coverage* e *Proof-of-Serialization* è possibile verificare, in maniera approssimativamente certa, la geolocalizzazione dei dispositivi che costituiscono la rete.

2.1 Motivazione

Un sistema come *Proof-of-Work*, utilizzato da Bitcoin e Ethereum, nonostante l'estremo livello di sicurezza che garantisce, presenta dei limiti: la maggior parte del lavoro richiesto non è riutilizzabile e, inoltre, l'attività di Mining, che tipicamente necessita di una potenza computazionale consistente, consuma grandi quantità di energia elettrica.
Helium, invece, si serve del protocollo *Proof-of-Coverage* per mettere a disposizone degli utenti della rete una copertura wireless affidabile ed economica.
Proof-of-Coverage è il primo sistema che prova l'onestà dei Miners all'interno di una rete fisica e per farlo sfrutta le proprietà uniche della comunicazione a radiofrequenze (RF):

- le RF hanno una distanza di propagazione limitata;
- la forza di un segnale RF ricevuto è inversamente proporzionale al quadrato della distanza dal trasmettitore;
- le RF viaggiano alla velocità della luce senza (effettivamente) nessuna latenza;

2.2 Costruzione della *Proof-of-Coverage*

Per verificare se i Miners agiscono onestamente e forniscono copertura di rete wireless in una data regione fisica, un Challenger C costruisce un pacchetto di dati multistrato O, che viene trasmesso ad una sequenza di nodi Target (Beaconers, o Challengees). Sia C che i Target operano come Miners, e sono individuati tramite i rispettivi Hotspots. Ogni Beaconer, che, qualora sia il destinatario previsto, è in grado di decrittare solamente il livello più esterno di O, firma una "ricevuta", la consegna a C e, dopo aver rimosso lo strato, lo trasmette al prossimo Target.

2.2.1 Costruzione della Challenge multi-layer

Il set di nodi candidati è selezionato all'interno di un'area geografica di raggio pari a T_{radius}, valore stabilito dalla rete, e centrata in T, il target iniziale relativo al Challenger. Quest'ultimo viene individuato da C generando un valore di entropia η, all'interno del processo di selezione, verificabile mediante la firma dell'hash del blocco corrente con la propria chiave privata.
All'interno dell'insieme T_n dei nodi Target, vengono individuati T_1 e T_L, i target con gli scores più alti (il meccanismo di assegnazione dello score è descritto nella Sezione [2.2.3]) e che si trovano a maggiore distanza da T.
Ogni strato O_l, è rappresentato da una tupla di tre elementi *E(S,ψ,R)*:

- E è una funzione crittografica che utilizza il protocollo *Diffie-Hellman* su curve ellittiche (ECDH);
- S è un nonce;
- ψ è il tempo impiegato per trasmettere il livello successivo della challenge;
- R è l'insieme dei livelli restanti di O, costituito da tuple di tre elementi ricorsive;

Ogni target crea uno strato O_l, che viene aggiunto ad O, e cifra S secondo ECDH, in modo da condividerlo solamente con C.

2.2.2 Creazione della Prova

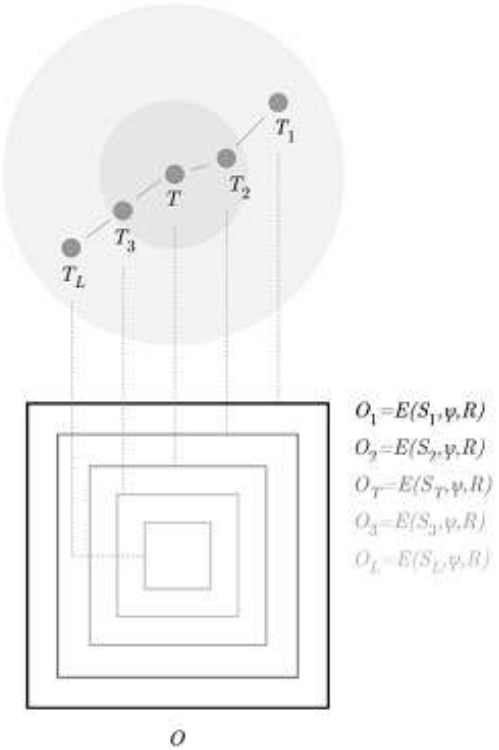
Una volta creato, O viene inviato a T_1. Essendo Helium una rete fisica a radiofrequenze, O è ascoltato anche dai Miners, tramite gli Hotspots che si trovano geograficamente vicini a T_1. Questi testimoniano l'esistenza del pacchetto di dati, e per tale motivo sono detti Witnesses.
Tuttavia, per quanto detto sopra, solamente il nodo previsto è in grado di decrittare E e inviare una ricevuta valida al Challenger. T_1 decifra lo strato più esterno di O e trasmette immediatamente R alla rete. Un generico nodo T_i nelle vicinanze cerca di decifrare il valore di E utilizzando la propria chiave privata p_k: se il tentativo ha successo, T_i crea la ricevuta K_s cifrata attraverso la sua chiave privata s, $K_s = (S||\beta||\nu)$, dove β è il tempo dopo il quale T_i ha ricevuto O, mentre ν è l'intensità del segnale.

Il target, dunque, invia la ricevuta a C attraverso la rete e, dopo aver rimosso il livello più esterno, trasmette in maniera wireless il resto di O.
Quanto descritto accade per ogni target da T_1 a T_l, attraversando il target iniziale T.
Le peculiarità delle radiofrequenze permettono a C di stimare un tempo soglia λ, trascorso il quale la *Proof-of-Coverage* viene considerata conclusa. Dal momento che C è l'unico nodo che conosce O nella sua interezza, i valori massimi di β e ν sono assegnati da C stesso. Il tempo di ricezione del segnale è limitato dalla velocità di propagazione delle onde tra due nodi target, τ.
Il pacchetto di dati arriverà al grafo dopo un tempo pari a $\mu = \tau \times (D + \epsilon)$, dove D è la distanza geografica e ϵ rappresenta i ritardi dovuti alla riflessione del segnale. Per ν è possibile calcolare il massimo RSSI (Received Signal Strength Indication) di un pacchetto, che è inversamente proporzionale al quadrato della distanza D.
In questo modo viene impedito ai Miners malintenzionati di mentire sulla locazione geografica reale dei propri Hotspots, dato che non conoscono la posizione del prossimo layer da decifrare. Dunque, una volta che T_l ha inviato la ricevuta a C, oppure dopo la scadenza di λ, la *Proof-of-Coverage* è completata, e la collezione delle ricevute K_s rappresenta la prova effettiva che C deve trasmettere alla rete.

2.2.3 Allocazione dello Score e selezione dei Target

Ad ogni Miner viene assegnato uno score ϕ_m che rappresenta il paramentro con cui ne viene valutata l'affidabilità; qualunque Miner che presenti un valore superiore a ϕ_m è conisderato onesto.
Lo score diminuisce in funzione del numero di verificazioni e all'aumentare del tempo trascorso dall'ultima verificazione a cui il Miner è stato sottoposto con successo. La rete Helium è progettata in modo tale da testare continuamente l'onestà dei Miners: al diminuire dello score, infatti, aumenta la probabilità che il Miner M sia selezionato come target per un dato C.
Si definisce uno *staleness-factor* δ, che viene utilizzato per determinare lo score di ciascun Miner:

$$\delta_m = \begin{cases} -(8.h')^2 & v' = 0 \\ v'.\left(1 - \frac{h'^2}{min(0.25, v')}\right) & v' > 0 \\ v'.(1 - 10.v'.h'^2) & v' < 0 \end{cases}.$$



I valori di v' e h' rappresentano rispettivamente la differenza tra il numero di verificazioni eseguite con successo e quelle fallite da un miner M, e il numero di blocchi aggiunti dall'ultima verificazione corretta, riscalate rispetto all'intervallo ideale di verificazione.
Il fattore di staleness permette di individuare tre tipi di Miners candidati:

1. Un v negativo è indicativo di un Miner che fallisce le verificazioni costantemente. Maggiore è il tempo che intercorre dall'ultima verificazione con successo e più rapida è la decrescita dello score. In questo modo aumenta la probabilità che tali Miners vengano selezionati per le successive verificazioni, dando loro la possibilità di aumentare il proprio score;

2. se $v = 0$, non si possiedono particolari informazioni sul Miner;

3. Un valore positivo di v è associato ad un Miner che spesso conclude le verificazioni con esito positivo. Dunque la decrescita dello score relativo a tali Miners rallenta in funzione di h.

Come anticipato, tali caratteristiche trovano spiegazione grazie alla definizione della funzione di *scoring*, che assume valori compresi tra 0 e 1, in relazione al fattore di *staleness*:

$$\phi_m = \frac{arctan(2.\delta_m) + 1.58}{3.16}$$

Sono due gli aspetti che assicurano che il sistema favorisca Miners legittimi a discapito dei disonesti:

- I nodi della rete, e quindi i Miners, sono connessi tramite archi il cui peso è pari a $1-(\text{score}(T_a)-\text{score}(T_b))$. I cammini minimi sono individuati mediante un algoritmo che utilizza tali pesi;

- Il meccanismo di selezione del target;

Quest'ultimo, infatti, è studiato in modo da assegnare una probabilità maggiore di essere selezionati come target ai Miners il cui score decresce più velocemente:

$$P(m) = \frac{1 - \phi_m}{n - \sum_{i=1}^{n} \phi_{m_i}} \tag{2.1}$$

dove n è il numero dei Miners. La relazione di proporzionalità inversa tra la probabilità di selezione e lo score di un Miner permette di selezionare target con score potenzialmente bassi, migliorando l'equilibrio globale nel sistema di *scoring*.

2.2.4 Verifica della Prova

Quando la *Proof-of-Coverage* viene considerata terminata, C invia l'insieme di tutte le ricevute K_s tramite uno speciale tipo di transazione che viene pubblicata all'interno della rete Helium.

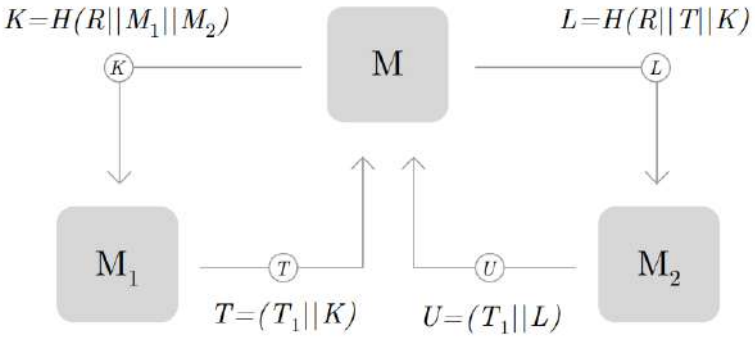
Un Miner verificatore, che vede la transazione contenente la Prova, ricostruisce il set di Miners e, innanzitutto verifica che il seed sia stato generato da C ad un tempo approssimativamente corretto: utilizzando lo stesso valore di entropia il processo di selezione del target restituirà lo stesso target iniziale T.
Dunque, dopo aver ricomposto il set dei candidati T_n, e dopo aver ricostruito il grafo T_g, il Miner verificatore V è in grado di verificare che le ricevute K_s, contenute nella Blockchain, siano state firmate con le chiavi private di $T_1, \ldots, T, \ldots, T_L$.
Se la verifica della *Proof-of-Coverage* ha avuto esito positivo, lo score dei Miners viene ricalcolato in maniera appropriata.

2.3 Costruzione della *Proof-of-Serialization*

Proof-of-Serialization rappresenta una forma semplificata del Roughtime utilizzato da Google, ossia un protocollo che permette di ottenere una sincronizzazione approssimativamente sicura senza la necessità di un Time Server.

2.3.1 Creazione della Prova

Un Miner M genera un nonce R, che è un'hash SHA-512 della *Proof-of-Coverage*, e invia $K = H(R||M_1||M_2)$ ad un primo Miner (con M_1 e M_2 vengono indicate le chiavi pubbliche dei Miners). Il primo Miner, dunque, restituisce a M un messaggio firmato T, contenente K e, soprattutto, il tempo corrente T_1. M ha la certezza che tale messaggio non sia pregenerato perchè contiene il nonce R. Dopodichè M genera un nuovo nonce R e invia $L = H(R||T||K)$ al secondo Miner. Allo stesso modo del primo, anch'esso cifra un messaggio U che contiene L e il tempo T_2. U rappresenta la prova della serializzazione tra M_1 e M_2.
Con un numero maggiore di Miners interrogati, M non solo è in grado di individuare un comportamento disonesto, bensì anche di stabilire in maniera sufficientemente accurata il reale tempo T.



2.3.2 Verifica della Prova

La risposta del secondo Miner dimostra implicitamente che è stata creata successivamente, dal momento che è M a costruire il nonce.
Pertanto se i tempi dichiarati dai due Miners risultano significamente diversi, e se T_2 è precedente rispetto a T_1, M ha la prova di un comportamente scorretto.
Per verificare il tempo esatto, il processo necessita di essere replicato con un numero di Miners sufficiente a raggiungere un consenso: perciò M seleziona n Miners in maniera pseudo-casuale e ripete lo scambio di messaggi con ciascuno di essi, finchè la sequenza di risposte, T_n, non risulta monotona almeno tre volte.
Questo permette di provare, con relativa certezza, che la *Proof-of-Coverage* è stata costruita tra b_t, il tempo relativo al blocco precedente, e il tempo verificato, T_t.

Capitolo 3

Proof-of-Location

Il consenso ottenuto dalla combinazione dei protocolli di *Proof-of-Coverage* e *Proof-of-Serialization* viene sfruttato da Helium per determinare la geolocalizzazione dei dispositivi compatibili con WHIP. Il sistema di verifica utilizzato prende il nome di *Proof-of-Location*.

3.1 Motivazione

Il tracciamento della posizione è una delle funzioni più usate dalle tecnologie a bassa potenza: si stima che entro la fine del 2022 ci saranno almeno 70 milioni di dispositivi in grado di effettuare il tracciamento della posizione. Oggi il comunemente noto GNSS (Global Navigation Satellite Systems) è usato dalla maggior parte dei dispositivi che richiedono servizi di geolocalizzazione, attraverso il GPS che è la più popolare delle implementazioni. I sistemi GPS usano una tecnica chiamata *Time-of-Arrival* (ToA) che determina la locazione di un ricevitore in relazione a 20 o più satelliti che orbitano attorno alla terra.
I satelliti sincronizzano il tempo usando degli orologi di bordo ad alta precisione, attraverso una sincronizzazione regolare e costante con i server a terra. I ricevitori GPS ottengono così un TimeStamp della data da un certo numero di satelliti e usano la trilaterazione per fornire una precisa geolocalizzazione sulla terra. Il GPS col tempo è diventato un sevizio ampiamente utilizzato in moltissime applicazioni che forniscono dati di localizzazione e servizi temporali.
Tuttavia, esistono significativi punti deboli di tale sisetma, a cui Helium tenta di trovare una soluzione. Ad esempio GPS può impiegare fino a due minuti per raggiungere un numero sufficiente di satelliti tale da inviare i dati correttamente, traducendosi in un drastico consumo di batteria; ipotizzando che un dispositivo debba trasmettere la sua posizione circa 25 volte al giorno, la durata di una batteria AA si ridurebbe da diversi anni ad un mese!
La tecnologia GPS non può essere utilizzata in luoghi chiusi, dato che necessita di una linea continua con almeno 3-4 satelliti per calcolare una posizione accurata.
Inoltre, i dati trasmessi spesso non sono criptati, esponendo il sistema ad attacchi di vario tipo.

3.2 Costruzione della *Proof-of-Location*

L'obiettivo di Helium è quello di verificare la posizione di un dispositivo D senza l'uso di hardware GNSS. Per farlo si serve delle verifiche ottenute attraverso i protocolli di *Proof-of-Coverage* e *Proof-of-Serialization*.

3.2.1 TimeStamp dei dati

Sistemi come ToA e TDoA sostituiscono GNSS con meccanismi basati sull'intensità dei segnali di ricezione, RSSI (Received Signal Strength Indication). Sfruttano la trasmissione di radiofrequenze che vengono captate da uno o più ricevitori e che vengono combinate con vari algoritmi basati su differenti caratteristiche di trasmissione.

TDoA è il più accurato dei sistemi, ma anche uno dei più complessi da implementare: si basa sulla variazione di informazioni sincronizzate dal trasmittente e registrate dai ricevitori.

Un esempio di flusso del TimeStamp è il seguente:

1. il dispositivo D carica un pacchetto P di dati sulla rete Helium;

2. i Miners M_n avvertono P e registrano un TimeStamp T_n dell'istante nel quale hanno ricevuto P;

3. T_n viene creato sulla base del time ricevuto tramite GNSS in nanosecondi, usando dati ricevuti via radio dall'Hotspot;

4. la transazione tra P e T_n viene firmata e inviata al router R appartenente al dispositivo D, dai Miners M_n;

5. ora R ha ricevuto le varie copie di P ognuna con il relativo valore di T_n.

Solitamente è difficile registrare i vari TimeStamps dal momento che anche una variazione di un millisecondo può portare a una diversa localizzazione.
Per raggiungere livelli tali di precisione vengono utilizzati dispositivi hardware in grado di campionare i dati in maniera efficiente, identificare il giusto pacchetto e registrare il corretto TimeStamp.
Il processore tipicamente usato è il FPGA (Field Programmable Gate Array) poiché è in grado di processare dati in modo deterministico. Dato però l'elevato costo di questo processore, la produzione di calore e il consumo elevato di potenza, l'hardware dell'Hotspot dei Miners fa uso di una nuova tecnologia low-cost in grado di raggiungere tali livelli di precisione: *LoRaWAN*. Esso è un protocollo che definisce le regole di comunicazione e l'architettura di sistema della rete grazie al *LoRa*, un modulatore wireless che permette di avere un raggio di copertura per le comunicazioni più ampio: poichè le RF viaggiano alla velocità della luce, anche in un nanosecondo percorrono circa 300,000 metri, segnando di fatto la necessità di una vasta area di copertura.

3.2.2 I TimeStamp per la derivazione della geolocalizzazione

Ora che il Router R è in possesso di vari messaggi firmati che includono il preciso TimeStamp T_n, è possibile ottenere la localizzazione del dispositivo D. Esistono vari algoritmi TDoA che assolvono tale compito che qui non menzioneremo. É importante ricordare che se un numero sufficiente di T_n vengono registrati per un determinato pacchetto, allora la localizzazione di D può essere determinata con un eventuale errore di pochi metri che dipende da altri fattori.

3.2.3 Verifica della *Proof-of-Location*

Dopo che R ha ottenuto la localizzazione di D, può essere necessario verificare che la posizione di D sia accurata in un preciso istante di tempo. Essendo la *Proof-of-Location* deterministica e derivata da informazioni pubbliche disponibili sulla blockchain, è possibile ricostruire i vari step:

1. dalle firme contenute nei pacchetti con i relativi TimeStamp T_n ogni Miner M_n coinvolto nel fornire i TimeStamps può essere verificato;
2. andando a consultare la transazione **assert-location** che contiene le coordinate geografiche dell'Hotspot, la posizione GPS di tali Miners può essere determinata;
3. infine la *Proof-of-Coverage* e gli scores di ogni Miner possono essere ottenuti dalla blockchain e consultati.

In questo modo il Router R può crittograficamente provare la localizzazione di ognuno dei Miners coinvolti, fornendo le componenti della *Proof-of-Location* per uno specifico dispositivo D. L'accuratezza di tale prova dipenderà prevalentemente dal numero di Miners coinvolti e, rispettivamente, di T_n ricevuti. In aggiunta i fattori RF come la riflessione e il multipath possono significativamente influenzare l'accuratezza del calcolo della localizzazione

Capitolo 4

Transazioni

Le transazioni all'interno della rete Helium, oltre a permettere il trasferimento di token da protoccolo in maniera *address-to-address*, forniscono anche ciò che è necessario per il funzionamento stesso della *DWN*.

4.1 La necessità di microtransazioni

Le commissioni (fees) pagate dai Devices ai Miners per il trasporto di dati su Internet, sono misurate per singolo pacchetto, in modo da garantire la massima flessibilità. Per inviare o ricevere un pacchetto di dati non è richiesta alcuna connessione precedente con il Miner e un Device può interagire con ogni Miner. Tutte le transazioni che avvengono sulla rete sono memorizzate all'interno della Blockchain, per questo motivo il costo di mining deve essere basso e i blocchi devono essere estratti con alta frequenza, affinchè le transazioni possano essere processate velocemente. Poiché la rete Helium ricompensa i Miners per un servizio specifico (DWN), i blocchi devono essere in grado di memorizzare le impronte digitali dei dati inviati dai Devices insieme alla transazione. Le varie fees vengono pagate agli Hotspot sotto forma di Data Credits (DC). I Data Credits vengono a loro volta prodotti bruciando HNT, e grazie a un meccanismo di *Implicit Burn* non è necessario che i Devices brucino esplicitamente gli HNT per inviare dati e pagare le fees, garantendo che non sia necessario l'intervento di alcun utente. Tale relazione tra HNT e DC garantisce un equilibrio *Burn and Mint*, e dunque che la quantità di HNT esistente rimanga costante mese dopo mese. Ogni Data Credits ha sempre un valore fisso di 0,00001 $, mentre il valore di un HNT è variabile, e dipende esclusivamente dall'andamento del mercato.La quantità di DC prodotta bruciando un HNT dunque varia nel tempo, e dipende solo dal suo attuale valore di mercato.

4.2 Tipi di commissioni in Helium

Consideriamo ora i tipi di costi richiesti nella rete Helium e le soluzioni che sfruttano le caratteristiche uniche del Protocollo di consenso.

4.2.1 Transport fees

I Devices che utilizzano la rete Helium per inviare e ricevere dati su Internet devono pagare una *transport fee* ai Miners. Tale commissione non ha nulla a che fare con la *transaction fee* che un Miner riceve dopo aver estratto un blocco. Poichè i Devices non sono collegati direttamente alla Blockchain, la commissione è negoziata tra il Router e il Miner. Quest'ultimo stabilisce il prezzo per il quale è disposto a prendersi in carico il trasferimento dei dati. Ciò significa che i Miners ricevono le commissioni per il trasporto dei dati dal Router prima che la transazione sia minata e registrata nella Blockchain, rappresentando un rischio per il Miner stesso. Tuttavia, dato che il costo *per-byte* è contenuto, tale rischio sembra essere tollerabile.

4.2.2 Transaction fees

La commissione per una nuova transazione è rappresentata dalla mediana delle commissioni pagate per il trasferimento degli ultimi δ pacchetti precedenti. Lo scopo principale è quello di permettere agli utenti di usufruire della rete in maniera pratica e agevole. Durante il processo di invio del blocco, i Miner nel gruppo di consenso [Sezione 5] verificano la correttezza del blocco e si assicurano che nessun addebito si discosti dalla soglia accettabile δ. Tutte le transazioni con commissioni errate (troppo alte o basse) vengono rifiutate prima che il blocco venga aggiunto alla Blockchain. Come descritto nella sezione successiva, il Protoccolo di Consenso di Helium non prevede alcun incentivo a includere transazioni più onerose. Infatti, a differenza di sistemi come Bitcoin, i Miners non possono vedere il contenuto delle transazioni senza collaborare con altri membri del del gruppo di consenso.

4.2.3 Staking fees

La commissione per le transazioni di *assert-location*, con cui viene certificata la posizione di un Hotspot sotto forma di coordinate geografiche, viene calcolata in maniera dinamica: poichè l'efficienza della rete Helium è funzione della densità degli Hotspots, la commissione di transazione è calcolata in modo da incentivare la rete ad ottenere una densità prossima a quella ideale:

$$y = (x - D)^4 + F$$

dove D è la densità ideale degli hotspot, F il costo unitario per una transazione e x e y sono le coordinate (possono essere identificate come i punti di una curva). Gli Hotspots vicini alla densità di rete ideale sono economici da aggiungere, ma risulta costoso creare una nuova rete o espanderne eccessivamente una già esistente. I Miners che non hanno annunciato la loro posizione, e che quindi non hanno pagato le staking fees, non sono considerati per l'inclusione nel gruppo di consenso.

4.3 Light Clients e Full Nodes

Un altro aspetto importante è la gestione della dimensione della Blockchain. Dal momento che tutti i Miners sono dispositivi Hotspot relativamente limitati in termini di potenza

di calcolo e spazio di archiviazione, Helium consente di operare come *light clients* sulla Blockchain: possono quindi eliminare i blocchi meno recenti e le transazioni contenute al loro interno, memorizzando solamente gli ultimi valori contenuti nel registro Helium. Tali nodi comunicano attraverso una rete peer-to-peer, con i *full nodes*, che, invece, mantengono una cronologia completa della Blockchain per verificare le transazioni. Dal momento che i Router sono applicazioni *software-only*, con accesso a dispositivi di archiviazione cloud-based scalabili, Helium chiede loro di operare come *full nodes*. La rete, inoltre, gestisce una serie di Router ospitati (hosted) in modo che gli sviluppatori non debbano necessariamente realizzare un proprio Router dedicato. In questo modo viene costruita una rete di *full nodes* in grado di supportare Hotspot con risorse limitate e *light clients* che operano sui wallet.

Capitolo 5

Protocollo di consenso della rete Helium

5.1 Motivazione

L'elevata potenza computazionale richiesta da un protocollo come *Proof-of-Work*, oltre a rappresentare un problema dal punto di vista del consumo energetico rischia di vanificare molti dei vantaggi della decentralizzazione di una rete. Molte blockchain hanno Mining Pools in cui gli utenti effettuanno l'estrazione dei blocco in parallelo e condividono le ricompense. Grandi Pools impediscono l'estrazione di blocchi da parte di gruppi indipendenti e, ovviamente, tendono a centralizzare il sistema.
La rete Helium utilizza un protocollo di consenso con le seguenti caratteristiche:

- è una rete permissionless: i nodi partecipano alla rete senza il permesso o l'approvazione di qualsiasi altra entità;
- il consenso è progettato in modo da rendere inefficace e costoso l'acquisto di più hardware in un solo luogo;
- il protocollo è tollerante a *difetti Bizantini*: il consenso è raggiungibile al di sopra di una soglia di nodi che agiscono onestamente, negli interessi della rete.
- sfrutta un lavoro riutilizzabile dalla rete.
- il protocollo di consenso di Helium può elaborare un gran numero di transazioni al secondo.
- il protocollo prevede che, idelamente, i Miners non siano in grado di scegliere transazioni prima di estrarle quindi le transazioni non vengono filtrate, ma sono tutte incluse nella Blockchain.

5.2 HBFT

Per la validazione delle attività che hanno luogo all'interno della rete, Helium combina la verifica di *Proof-of-Coverage* e una variante del protocollo *HBFT (Honey Badger Byzantine Fault Tolerant protocol)*.
Il protocollo presuppone un Set di N nodi, che prende il nome di *Gruppo di Consenso C*. Tale gruppo riceve le transazioni e tenta di raggiungere un accordo sull'ordine delle transazioni da inserire nei blocchi. Il protocollo presenta diversi *turni*, all'inizio di ognuno dei quali il gruppo seleziona un sottoinsieme di transazioni nella sua coda e lo presenta come input per un protocollo di consenso, al cui termine viene selezionato il set di transazioni da inserire nella Blockchain.
Le transazioni sono cifrate utilizzando una *chiave pubblica partizionata*, in modo tale che il *Gruppo di Gonsenso* sia obbligato a collaborare per raggiungere un accordo.

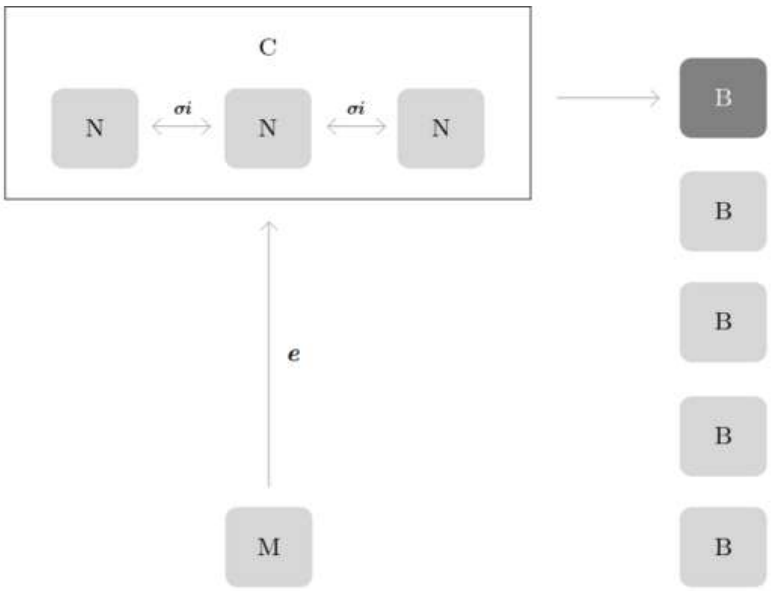
5.2.1 Applicazione della *Proof-of-Coverage* a HBFT

Le *Proofs-of-Coverage* che i *Miners* inviano alla rete in un certo periodo di tempo, Δp, sono registrate come un tipo di transazione all'interno della Blockchain. I Miners con uno score più alto eletti a far parte del *Gruppo di consenso* HBFT: in questo modo Helium utilizza la *Proof-of-Coverage* per ricompensare i Miners più onesti in una data *epoca*.

5.2.2 Il *Gruppo di consenso* e il processo di *Mining*

Il *Gruppo di Consenso* eletto in un certo periodo è responsabile della creazione dei blocchi, che avviene ad un intervallo costante Δ_b, e del loro inserimento nella Blockchain. La ricompensa per ogni blocco, insieme alla somma di tutte le commissioni associate alle transazioni, viene distribuita come token tra i membri di C.
Dopo la selezione del *Gruppo di Consenso*, vengono generate e distribuite le chiavi per realizzare la cifratura con schema a soglia delle transazioni.
Il sistema TPKE, *Threshold Public Encryption Key*, garantisce che una transazione possa essere recuperata solamente con la collaborazione di un sottoinsieme onesto di C, di cardinalità almeno pari a $f + 1$ (f è un parametro del protocollo che indica il numero di *difetti bizantini* tollearibili).
Una volta che la Master Public Key PK è stata generata, un blocco che la contiene viene immediatamente inviato alla Blockchain. Ogni membro N_m riceve una *secret key share*, SK_i, di PK.
I Miners, quindi, inviano nuove transazioni t al *Gruppo di Consenso C*. Ciascun membro seleziona un sottoinsieme casuale delle prime transazioni nella sua coda e applica la funzione di cifratura, $\text{TPKE.Enc}(PK, t) \rightarrow e$. Dunque, e viene inviato agli altri membri di C e una volta che ognuno ne riceve almeno $N - f$, utilizza la funzione $\text{TPKE.DecShare}(SK_i, e) \rightarrow \sigma_i$ per produrre e trasmettere il proprio *crittogramma*. Una volta che $f + 1$ membri hanno ricevuto le condivisioni σ_i, possono ripetere la funzione di decifratura usando PK, e e le σ_i e tentare di decrittare la transazione. Siccome i membri del gruppo non possono decifrare e autonomamemte, un singolo membro non può censurare una transazione t prima della sua inclusione nel blocco candidato senza che $f + 1$

membri di C siano consenzienti: qualsiasi membro onesto di C che abbia t nelle prime B transazioni in coda può includere t in un blocco, poiché gli altri membri di C non possono decrittare la transazione fino a quando non è stato concordato.
Anche se più Miners cercassero di accordarsi per inserire t, essendo i membri di C selezionati in base alle *Proofs-of-Coverage* presentate in una certa epoca Δ_c, è impossibile prevedere quali Miners prenderanno parte a C, rendendo di fatto questo tipo di manipolazione molto difficile da realizzare. Quando almeno $f+1$ nodi hanno raggiunto il consenso sulle transazioni da inserire nel blocco, viene ottenuta una firma di soglia *TPKE*: in questo modo si certifica che un numero sufficiente di nodi è in accordo sul blocco da aggiungere. I membri di C che sono in disaccordo sul contenuto del blocco producono una condivisione di firma incompatibile che non può essere utilizzata per raggiungere il valore di soglia di firme valide.
Una volta raggiunta la soglia, il blocco viene inviato a tutti i Miners della rete Helium e aggiunto alla Blockchain.



Bibliografia

[1] Technical Marketing Workgroup 1.0. *LoRaWAN what is it?* LoRa Alliance, 2015.

[2] N. Garg A. HaleemAndrew, A. ThompsonMarc. Helium, a decentralized wireless network. 2018.

[3] Helium Community. Helium docs. https://docs.helium.com/, .

[4] Helium Community. Helium hotspot docs. https://docs.helium.com/mine-hnt/, .

[5] Helium Community. Helium official website. https://www.helium.com/, .

[6] Helium Miners Europe. Helium proof of coverage. https://helium-miners.eu/helium-proof-of-coverage-what-is-it-and-how-does-it-work/.

[7] Helium System Inc. Helium proof of coverage. https://docs.helium.com/blockchain/blockchain-primitives/, 2022.

PROPAGAZIONE DELL'INFORMAZIONE NELLA RETE BITCOIN

Alice Colombatto, Alessandro Giacchetto, Nicola Lombardi, Gabriele Vernetti

Capitolo 1

Introduzione

Una *blockchain* è un registro digitale di dati distribuito su di una rete decentralizzata *Peer-to-Peer* (P2P). Le operazioni eseguite sulla blockchain sono registrate in blocchi, concatenati in ordine cronologico in un ambiente trustless. Ciò viene realizzato mediante l'uso della crittografia, che in combinazione alla decentralizzazione della rete rende ogni dato tracciabile, immutabile e immune alla censura.

All'interno di un contesto informatico di questo genere ci sono molti modi per comunicare: questo si può fare attraverso una serie finita di operazioni decise comunemente a priori (*protocollo*). A seconda della tipologia di protocollo, gli utenti danno vita a diverse blockchain, ognuna delle quali quindi possiederà le sue caratteristiche.

In questo lavoro analizzeremo il protocollo caratterizzante la prima e più famosa blockchain, Bitcoin - più volte paragonata all'oro digitale - in tutte le sue caratteristiche, quelle positive e quelle che, forse, si potrebbero migliorare. Il motivo di questa scelta ricade sulle sue dimensioni e sulla quantità di informazioni reperibili. Ci focalizzeremo su tutti i tipi di nodi Bitcoin, capendone le differenze, soprattutto in termini di protocollo di comunicazione; a seconda della tipologia, un nodo dovrà svolgere un lavoro diverso. Da queste analisi emergeranno problematiche, sia di tempo (di esecuzione delle operazioni), che di spazio (occupazione di memoria e banda), quindi di fruibilità. Verranno proposte infine delle modifiche che potrebbero essere adottate per ovviare, almeno parzialmente, a queste problematiche.

Capitolo 2

La rete Bitcoin

L'architettura della rete che permette l'esistenza di Bitcoin è di tipo *Peer-to-Peer* (P2P). Questo significa che ogni nodo partecipante alla rete stessa è uguale agli altri, e coopera insieme agli altri fornendo i servizi e le funzionalità definite dal protocollo condiviso, analogamente eseguito da parte di tutti i nodi. Essendo l'antitesi dell'architettura più conosciuta e maggiormente utilizzata nel contesto attuale, definita *Client/Server* (C/S), la rete Bitcoin non necessita di server centralizzati per fornire alcun tipo di servizio: al contrario, ogni nodo costituisce un punto della rete, attribuendo al protocollo stesso decentralizzazione e resilienza che solo reti *Peer-to-Peer* possono garantire. Esempi di reti P2P che hanno riscontrato grande successo sono quelle adibite al *file-sharing*, diffuse inizialmente con *Napster* nel 1999, evolute poi in protocolli migliori, come *BitTorrent*.
Al pari delle suddette implementazioni, come già detto, Bitcoin è nato per essere un sistema *Peer-to-Peer* di gestione e utilizzo di denaro digitale, in grado di funzionare senza l'intervento di autorità centrali, con lo specifico scopo di essere uno strumento incensurabile e resiliente al controllo centralizzato, distribuito tra i nodi che vogliono partecipare alla rete.
Per questa serie di caratteristiche il design scelto da Bitcoin non poteva che essere una rete P2P.

2.1 Nodi della rete Bitcoin: tipologia e ruoli

Le funzionalità che i nodi possono eseguire, per far parte del network, sono quelle definite dal protocollo Bitcoin e si possono identificare in Figura 2.1.
In base alle funzionalità che ogni nodo decide di implementare, vengono delineate alcune cateogorie di nodi:

- Full Node
- Simplified Payment Verification Node (SPV)
- Miner Node

Un *full node* è un nodo che si occupa di conservare una copia completa della blockchain di Bitcoin, mantendola aggiornata attraverso la costante comunicazione con gli altri nodi della rete. Possedendone una copia locale, esso è in grado di verificare ogni nuova transazione o blocco in arrivo, senza dover dipendere da nodi di terze parti. Al momento della stesura, i requisiti tecnici per poter implementare un full node rimangono notevolmente accessibili, sia in termini di hardware (2GB di RAM, 500GB di spazio libero su disco) che di *know-how* tecnico, grazie alla grande disponibilità di guide online e implementazioni in stile *"plug-and-play"* (Figura 2.2) sviluppate negli anni. Vorremmo sottolineare quanto sia fondamentale, ai fini di una vera decentralizzazione, una più bassa barriera tecnologica possibile: più il numero di *full nodes* è alto, più il network è distribuito, con il seguente aumento del livello di robustezza e resilienza dell'intera rete. I dettagli relativi alla comunicazione tra i vari full nodes della rete verranno descritti più approfonditamente all'interno della prossima sezione.

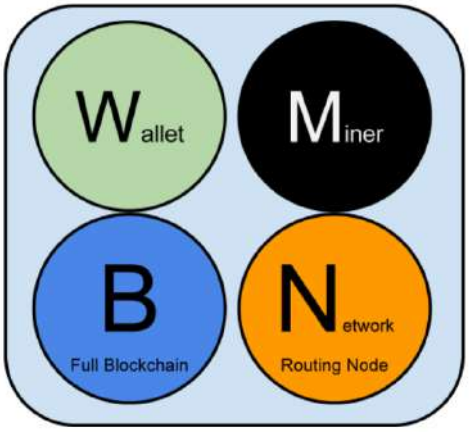


Figura 2.1: Funzionalità che può avere un nodo partecipante al network Bitcoin.

Un *Simplified Payment Verification (SPV) node*, invece, contiene una copia di tutti gli *headers* dei blocchi, ma non le transazioni e gli altri dati relativi ad essi. Esso si occupa di verificare la validità degli headers dei nuovi blocchi; oltre a ciò, un nodo SPV è in grado di verificare le transazioni di proprio interesse, con l'aiuto di un *full node* con cui è connesso. Per questo motivo i nodi di questo tipo vengono anche chiamati *lightweight node* o nodi "leggeri". Il vantaggio principale di questa categoria di nodi consiste nel minor utilizzo di risorse hardware (spazio su disco) rispetto ad un full node, rendendo questi ultimi più adatti a contesti in cui vi è una più forte limitazione nell'utilizzo di risorse (e.g. smartphones). Il maggior svantaggio dei nodi SPV deriva dalla necessaria dipendenza da altri full nodes, nel momento in cui richiedono a questi ultimi una determinata serie di blocchi che non si ha localmente. Durante questa procedura, si potrebbe andare incontro ad un *Sybil attack*, che potrebbe compromettere la privacy di un client SPV. Per ovviare e mitigare il suddetto rischio, sono stati introdotti i cosidetti *bloom filters*, che verranno approfonditi all'interno del capitolo 3.

Un *Miner node*, a differenza dei precedenti, ha lo scopo specifico di risolvere il problema della *proof-of-work (POW)*, cercando di aggiudicarsi la ricompensa del nuovo blocco attraverso l'utilizzo di hardware sempre più specializzato, che da diversi anni a questa parte è costituito da ASIC (Application Specific Integrated Circuit, v. Figura 2.3). Una volta risolto il blocco su cui sta lavorando, un *miner* comunica la propria soluzione al resto della rete attraverso il proprio *full node*, oppure trasmettendo il nuovo blocco ad un nodo del network a cui esso è connesso.

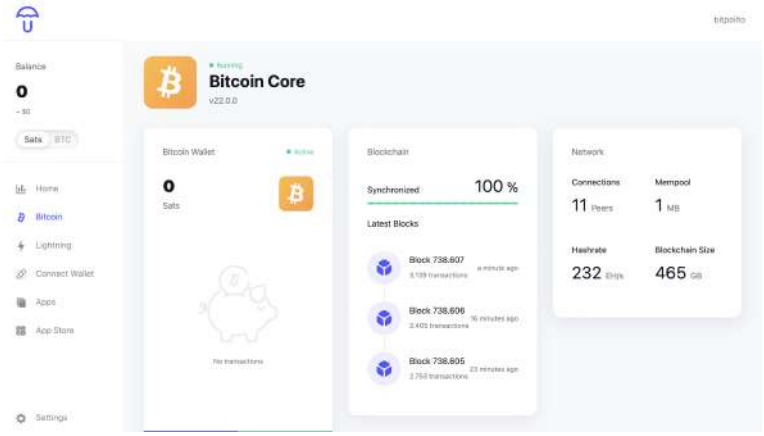


Figura 2.2: Dashboard di un full node implementato attraverso la soluzione sviluppata da Umbrel.

Figura 2.3: Antminer S19 Pro, uno degli ASIC più efficienti sul mercato.

2.2 Rete Bitcoin estesa

La composizione della rete appena descritta è quella necessaria al funzionamento base del protocollo P2P di Bitcoin. Nella realtà, però, la rete Bitcoin è arricchita ulteriormente da altri nodi che eseguono alcuni protocolli specifici (e.g. Stratum, Pool Mining Protocol, FIBRE).
Una visione d'insieme della cosidetta *Extended Bitcoin Network* può essere meglio compresa attraverso la Figura 2.4. Analizzando la mappa, si possono notare tre protocolli (contraddistinti da colori diversi) completamente compatibili gli uni con gli altri, che permettono le varie interazioni tra nodi di vario tipo, a seconda delle funzionalità che ognuno decide di implementare e mettere a disposizione della rete estesa.
Si noti come, ad esempio, una porzione della rete sia fortemente collegata ad un *Pool Server*: si tratta di una serie di nodi che si occupa di eseguire le operazioni di mining aggregando la propria hashpower in una mining pool (con lo scopo di diminuire l'instrinseca varianza relativa alla proof-of-work), che gestirà la comunicazione e l'interazione attraverso un proprio protocollo sviluppato ad hoc per tali operazioni. L'antitesi del cosidetto "pooled-mining" è costituita dai nodi definiti *Solo Miners*, i quali, non basandosi su alcuna mining pool per le loro operazioni di mining, necessitano di una copia locale della blockchain (indicata dal pallino blu all'interno dei nodi), grazie alla quale possono verificare autonomamente le nuove transazioni da inserire nel blocco, prima di iniziare la ricerca del *nonce*. Il protocollo contraddistinto dalle connessioni in rosso, chiamato *Stratum Protocol*, nato intorno al 2012, costituisce l'alternativa al precedente modello di pooled-mining. L'obiettivo di Stratum è quello di definire una specie di standard per la gestione delle comunicazioni tra server delle mining pool e miner(s). Pur non essendo mai stato ufficializzato attraverso dei BIPs, è diventato negli anni lo standard "de facto", condiviso e utilizzato dalla maggior parte delle mining pool che operano attualmente.

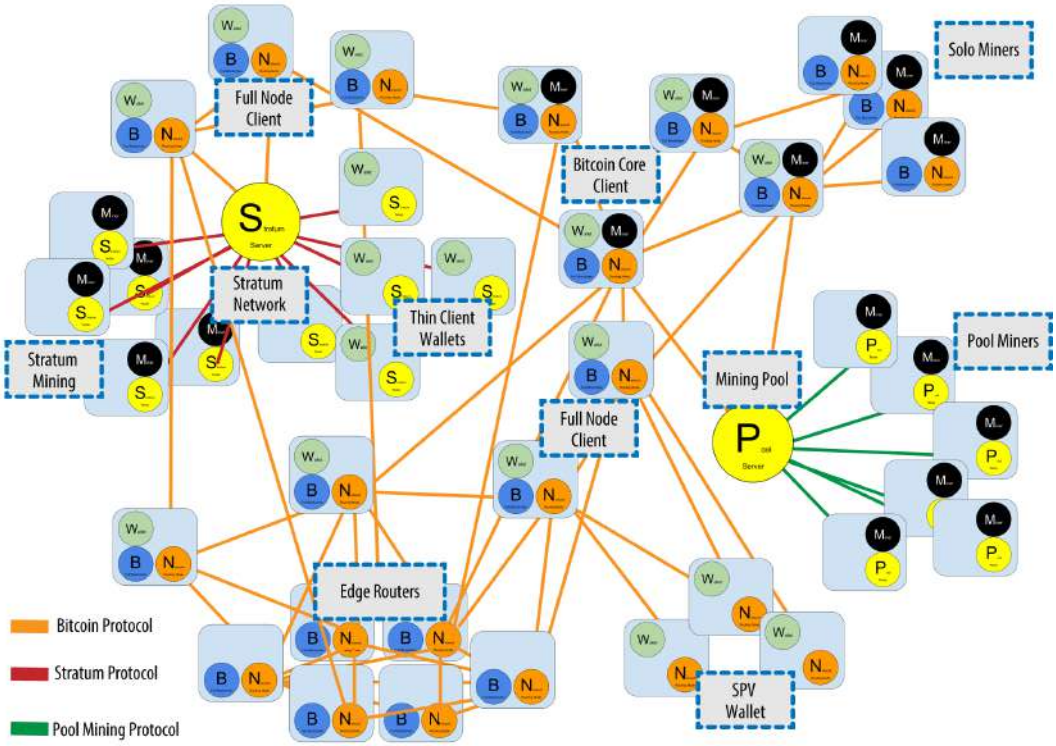


Figura 2.4: Mappa della "Extended Bitcoin Network".

2.3 Estensione geografica e statistiche varie

Utilizzando alcune funzioni definite all'interno del protocollo Bitcoin, implementate e messe a disposizione della maggior parte dei nodi, è possibile effettuare una ricerca ricorsiva delle connessioni presenti tra i nodi, e ottenere alcune statistiche relative all'estensione geografica globale della rete Bitcoin. Oltre alle premesse dello stesso Bitnodes.io, presenti sul proprio sito, ci teniamo a sottolineare come oramai molte implementazioni tra le più utilizzate per creare un *personal full node* in modo più "user-friendly" (umbrel, raspiblitz, mynode or ronindojo), funzionino attraverso rete TOR. In questi casi, quindi, l'indirizzo IP rilevato da Bitnodes non geolocalizza il vero punto in cui è veramente presente il nodo, ma l'exit node di TOR a cui esso è collegato. Basandosi sui dati raccolti dal suddetto sito, possiamo affermare che, al momento della stesura, l'intera rete Bitcoin è costituita da circa 16.000 *reachable nodes*. Con il termine *reachable* si intende identificare quei nodi che accettano nuove connessioni in ingresso, fornendo quindi accesso ai nuovi nodi, garantendo il "download" dell'intera blockchain, a partire dal blocco genesi.

A questo link è possibile consultare la stima relativa al numero totale di nodi della rete, sia *reachable* che *unreachable*, il quale, al momento della stesura, supera i 200.000 nodi totali.
Oltre alle statistiche relative a Stati e città di tutto il mondo, un altro dato interessante è la percentuale di nodi aggiornata all'ultima versione del protocollo Bitcoin (22.0.0): circa il 60%. Per quanto riguarda i dati sugli ASNs (Autonomous System Number) individuati dai crawler di Bitnodes.io, si può notare come circa il 52-54% dei nodi comunichi attraverso rete TOR, mentre solo il 3-4% è basato sui server di AWS.

Figura 2.5: Screenshot della "live map" di Bitnodes.io.

Capitolo 3

Il protocollo della rete Bitcoin

Per spiegare in modo approfondito come comunicano tra loro i nodi di Bitcoin, abbiamo suddiviso l'analisi del protocollo in tre macro sezioni, che sono rivolte rispettivamente a tre scopi diversi:

1. Flusso dell'informazione
2. Interazione tra i nodi
3. Verifica delle informazioni

3.1 Flusso dell'informazione

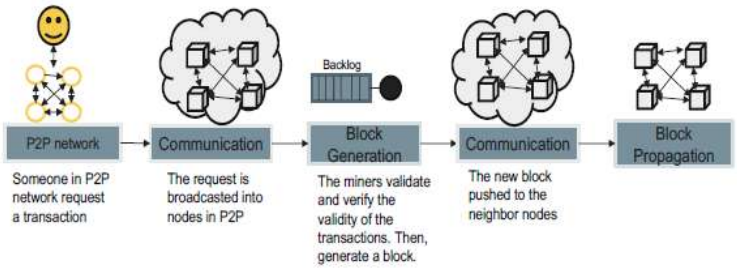


Figura 3.1: Protocollo per l'inserimento di una nuova transazione nella rete Bitcoin.

La Figura 3.1 illustra il flusso dell'arrivo delle transazioni, della formazione di blocchi, della propagazione e della convalida nella Blockchain. Quando un dispositivo contenente un nodo - di qualsiasi tipo esso sia - si accende e si vuole connettere alla rete Bitcoin, usa un nome DNS, codificati in Bitcoin Core.

L'acronimo DNS è la sigla di Domain Name System, un sistema mediante il quale si accede tramite Internet all'indirizzo IP del server a cui si richiede l'accesso. Agisce come se fosse una rubrica o una piattaforma dedicata alla traduzione dei nomi di un

sito web in un IP con cui localizzare il web server. Ciò consente agli utenti di accedere rapidamente e facilmente ai servizi ospitati su server connessi a Internet. Quando un nodo si unisce alla rete, questo interroga i server DNS: questi, mediante le query fatte dai nodi, restituiscono l'insieme di nodi che stanno partecipando alla rete in quel momento; il collegamento alla rete Peer-to-Peer è così eseguito ed il nodo è a tutti gli effetti connesso alla blockchain.

Una volta in rete, il nodo può vedere tutto ciò che è stato fatto: dopo che le transazioni sono state generate dagli utenti, vengono inviate a tutti i nodi di convalida, ovvero i *full node*. Quando arriva una transazione in un nodo completo, il nodo memorizza la transazione nel suo mempool (ovvero il pool di memoria), in attesa di conferma. Inoltre, il miner node può scegliere delle transazioni non confermate nel mempool per impacchettarle in un nuovo blocco. Se la ricerca ha successo, questo nuovo blocco appena generato viene aggiunto alla Blockchain. Questa informazione viene inviata a tutti i nodi. In ogni nodo, la validità del nuovo blocco generato viene verificata. Se la validità è confermata con consenso, il blocco è accettato e le nuove transazioni nel blocco vengono convalidate. Tali transazioni convalidate vengono rimosse dal mempool di ogni nodo completo, che poi ripete il processo di cui sopra.

3.2 Interazione fra i nodi

I nodi di Bitcoin formano una rete Peer-to-Peer, mentre ogni nodo per impostazione predefinita ha almeno una lista di otto nodi collegati. È un collegamento logico che consente ai peer di eseguire nuovi aggiornamenti (sia di tipo push che di tipo pull) ai suoi vicini.

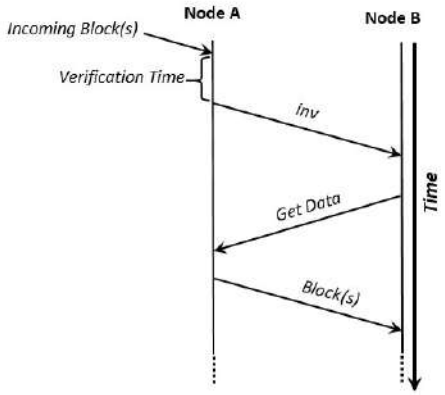


Figura 3.2: Scambio di messaggi tra nodi per comunicare la conoscenza dei blocchi.

La Figura 3.2 mostra una sequenza di scambio di un messaggio da nodo a nodo: in breve, il nuovo blocco in arrivo (o transazione) ha raggiunto il nodo A. Quindi, un

blocco/transazione viene convalidato (la barra grigia in verticale) dal nodo A, che quindi invia un messaggio di tipo *inv* al nodo B, chiedendo il permesso per inviargli il blocco. Il nodo B risponde con una richiesta (*getdata*) per il blocco/transazione, ed il nodo A lo invia.

Per evitare l'invio di transazioni e di messaggi dei blocchi ai nodi che li hanno già ricevuti da altri nodi, questi non vengono inoltrati direttamente. Viene infatti annunciata la loro disponibilità ai vicini, inviando loro un messaggio *inv* una volta che la transazione o il blocco è stato completamente verificato. Il messaggio *inv* contiene una serie di hash delle transazioni e quelle del blocco che sono state ricevute dal mittente e sono ora disponibili. Un nodo, che riceve un messaggio *inv* per una transazione o per un blocco che non ha ancora localmente, emetterà un messaggio *getdata* al mittente del messaggio *inv*, contenente le hash del merkle tree di cui non ha corrispondenza.

Ad ogni ciclo di trasmissione il messaggio incorre in un ritardo di propagazione. Il ritardo di propagazione è la combinazione del tempo di trasmissione e la verifica locale del blocco o della transazione. Il tempo di trasmissione include una comunicazione sotto forma di un messaggio *inv*, una richiesta dal gruppo ricevente ed una consegna. Mentre i messaggi *inv* e *getdata* sono di dimensioni relativamente ridotte (61 byte nella maggior parte dei casi, poiché in quanto trasmissioni immediate contengono solo il singolo blocco o transazione annunciato), il blocco intero potrebbe essere molto grande − oltre ad $1MB$ al momento della scrittura. Prima che il blocco venga annunciato ai vicini di un nodo, è verificato. La verifica di un blocco include la verifica di ogni transazione nel blocco, e la verifica delle transazioni, a sua volta, richiede l'accesso ai dati memorizzati sui dischi.

Facciamo ancora un'osservazione sui tempi di cui la rete necessita, che verranno poi analizzati in modo più approfondito successivamente.

Sia $t_{i,j}$ la differenza di tempo tra il primo annuncio dall'origine alla rete ed il tempo in cui il nodo j riceve il dato i. Se il nodo o è l'origine dell'elemento i dei dati, cioè sia il cercatore del blocco sia il nodo che ha creato la transazione, allora $t_{i,o} = 0$. I tempi $t_{i,j}$ in cui i nodi apprendono l'esistenza di un dato segue un comportamento di un doppio esponenziale ($(e^i)^j$). Similarmente alla diffusione casuale di rumore, la propagazione di questo tipo di dato può essere suddiviso in due fasi: una fase iniziale di crescita esponenziale, in cui la maggior parte dei nodi riceventi i messaggi *inv* richiederanno il dato corrispondente come se non ce l'avessero ancora, e una fase di contrazione esponenziale in cui la maggior parte dei nodi che ricevono un annuncio hanno già il dato corrispondente.

3.3 Verifica delle informazioni

Per costruzione i nodi nella rete formano un grafico casuale. Una volta connesso, il nodo conosce gli altri nodi chiedendo ai suoi vicini gli indirizzi di interesse e ricevendo annunci spontanei di nuovi indirizzi. Osserviamo che non esiste un modo esplicito per lasciare la rete: gli indirizzi dei nodi che hanno lasciato la rete indugiano per diversi ore prima che gli altri nodi li eliminino dal loro set di indirizzi conosciuti. Al momento della scrittura circa 16000 indirizzi univoci sono resi noti.

Ad un nodo Bitcoin è consentito mantenere fino a 132 connessioni (maxconnections) di default (e, come detto precedentemente, un minimo di 8). A questo punto, il nuovo nodo aggiorna la sua lista dei peer scoprendo i nodi vicini; in questo modo, i nuovi nodi selezionano quelli che fanno parte della rete. Questa formazione è chiamata distance-based poiché dipende fortemente dal concetto di vicinanza e quindi dall'aggiunta di nodi vicini. Questo elenco di peer viene utilizzato come elenco di riferimento per inviare un inventario o ricevere messaggi dai nodi vicini. Dopo che il nodo si è unito alla rete, partecipa alla propagazione, al consenso ed alla generazione di blocchi. Questi nodi agiscono come un nodo completo, il che significa che gli utenti/proprietari possono creare nuove transazioni e creare un blocco, così come inoltrare i nuovi aggiornamenti al network.

Oltre a quest'analisi della rete in sé, è necessario focalizzarsi sui veri fruitori di Bitcoin, i client che vogliono spostare cripotomoneta, e su come possono farlo considerando i problemi che si presentano.

Bitcoin ha già assistito a una più ampia adozione e attenzione rispetto a qualsiasi altra valuta digitale proposta fino ad oggi; implementa un servizio di timestamp distribuito, che opera sulla rete Bitcoin Peer-to-Peer e garantisce che tutte le transazioni ed il loro ordine di esecuzione siano visibili a tutti gli utenti di Bitcoin. Attualmente, una tipica installazione di Bitcoin richiede circa 500 GB di spazio su disco, e richiede molto tempo per il download dei blocchi e delle transazioni contenute. Dato il suo crescente utilizzo, il volume delle transazioni in Bitcoin ci si aspetta che aumenti ulteriormente, producendo così una crescita considerevole nella dimensione della blockchain. Oltre all'utilizzo dello spazio su disco, la continua crescita del volume delle transazioni di Bitcoin incorre in un notevole sovraccarico sui client Bitcoin che devono verificare la correttezza dei blocchi e delle transazioni trasmesse nella rete. Questo problema diventa ancora più evidente quando gli utenti desiderano eseguire/verificare pagamenti Bitcoin utilizzando dispositivi con vincoli di risorse, come i dispositivi mobili.

Per porre rimedio a questo, gli sviluppatori di Bitcoin hanno rilasciato un lightweight client, chiamato BitcoinJ, che supporta una verifica di pagamento semplificata (abbreviata SPV) in cui si trova solo una piccola parte scaricata in locale della catena di blocchi, supportando così l'utilizzo tipico di Bitcoin su dispositivi vincolati (ad es. Smartphone). I client SPV sono stati originariamente già proposti da Nakamoto, ma sono stati utilizzati solo successivamente, in quanto fanno affidamento sui *Bloom Filters* per ricevere le transazioni rilevanti per il proprio portafoglio locale.

Un Bloom Filter è un filtro di ricerca probabilistico, un modo per descrivere un pattern adatto ai propri interessi, ma senza specificarlo esattamente; i Bloom Filters quindi offrono un modo efficiente per chiedere transazioni di loro interesse senza rivelare esattamente quali indirizzi stanno cercando, tutelando la privacy.

L'obiettivo è quello di avere il proprio wallet che possa segnalare correttamente se ci sono indirizzi di transazioni di mio interesse all'interno di un blocco, ma senza che gli altri possano sapere quello che sto richiedendo. Il Bloom filter, come mostrato nella Figura 3.3, è un array di m bit, e si inizializza vuoto, ovvero con tutti i bit settati a 0. Devono anche essere definite K_i funzioni hash differenti, ognuna delle quali mappa un elemento del set in una delle m posizioni dell'array con una distribuzione uniforme. Per aggiungere un elemento, vengono calcolate tutte le i funzioni hash per ottenere le

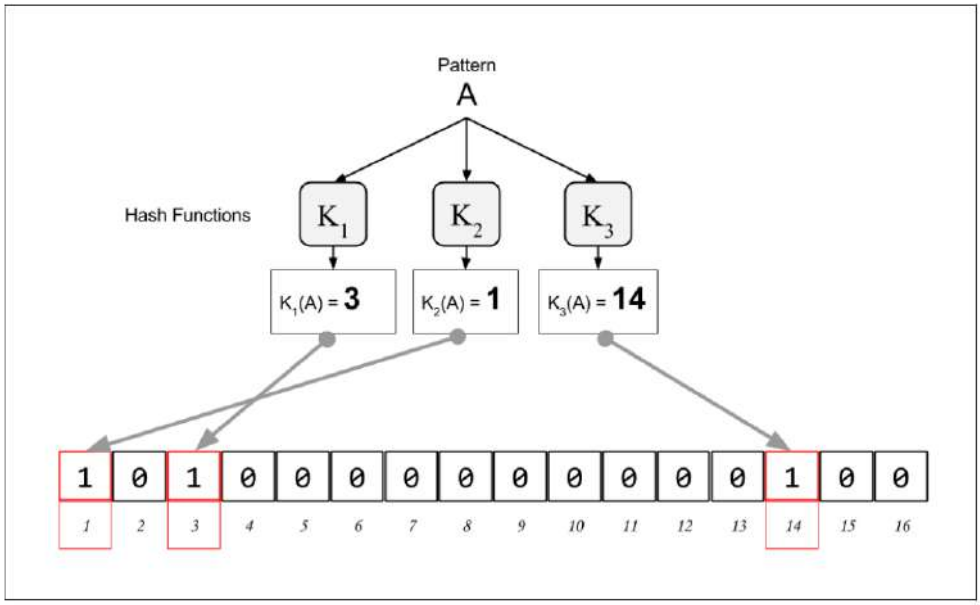


Figura 3.3: Struttura di un Bloom Filter.

i posizioni nell'array. Poi vengono settati a 1 i bit in quelle i posizioni. Per testare un elemento sull'insieme, vengono calcolate le funzioni hash sull'elemento e poi vengono controllate le i posizioni dell'array di m bit. Se anche solo uno dei bit controllati nell'array è 0 allora si può dire con certezza che l'elemento non è all'interno dell'insieme. Se invece tutti i bit controllati sono settati a 1 allora vuol dire che o l'elemento è all'interno dell'insieme oppure i bit sono stati settati a 1 durante l'inserimento di altri elementi, restituendo quindi un falso positivo. Ovviamente bisogna valutare il trade-off tra privacy e accuratezza della ricerca: più posizioni nell'array sono note e più rivelo le mie informazioni, ma ottenendo una ricerca più accurata.

Capitolo 4

Migliorie della rete Bitcoin

Dovendo trasmettere informazioni su una rete Peer-to-Peer, è necessario che questa sia resiliente, ovvero che non si creino situazioni in cui due porzioni della rete sono connesse con pochi collegamenti, o in cui per far comunicare due porzioni della rete è necessario fare molti step intermedi, aumentando quindi i tempi di propagazione. D'altra parte, dobbiamo evitare di avere troppi collegamenti tra i vari peers: la ridondanza di informazioni porterebbe infatti ad una congestione della rete. Un'altra caratteristica della rete Peer-to-Peer di Bitcoin è la presenza di nodi *unreachable*, ovvero nodi che non accettano richieste di creazione di un nuovo collegamento da parte di altri nodi. La presenza di questi nodi potrebbe causare effetti collo di bottiglia, o più in generale di malacomunicazione all'interno della rete.

4.1 Clusterizzazione in base alla posizione geografica

Per aumentare la resilienza della rete, Fadhil, Owenson e Adda [FOA17] hanno proposto un approccio di tipo localizzato. Ciò consiste nel creare cluster di nodi geograficamente vicini molto connessi, e poi connettere questi cluster tra di loro. Ciò permette, localmente, di trasmettere molto efficientemente le informazioni, in quanto i nodi dello stesso cluster avranno un ritado di comunicazione contenuto, e su larga scala la ridondanza viene di molto contenuta.

Inoltre, se i collegamenti tra i vari cluster vengono realizzati in maniera appropriata (ad esempio, imitando uno *small world graph*), ciò permette di far comunicare efficientemente regioni molto distanti nel mondo, quindi di far propagare molto velocemente informazioni nella rete Peer-to-Peer. Una proprietà degli small world graphs infatti è una crescita logaritmica del diametro (intuitivamente, il minor numero di archi che bisogna attraversare per arrivare ad un nodo qualsiasi, partendo da un nodo qualsiasi) rispetto al numero di nodi.

Cosa vuol dire ciò? Cerchiamo di avere una stima di quanto ci vuole per arrivare da un capo all'altro della rete. Dalle ultime stime di bitnodes.io, ci sono circa 16000 nodi reachable. Per contare anche gli unreachable e avere comunque margine di crescita per la rete, supponiamo ci siano 30000 nodi. Supponiamo quindi di avere cluster di 100 nodi ciascuno, $\log_2(300) \approx 8$. Ovvero tramite 8 comunicazioni tra clusters, possiamo diffondere globalmente nuove informazioni, che siano queste un nuovo blocco minato, o una transazione. In Figura 4.2 vengono mostrate le performance di trasmissione delle transazioni nella rete, sulla base del protocollo utilizzato e della distanza massima scelta per formare i cluster. Come si può osservare la crescita in tempo della propagazione delle informazioni rimane molto limitato rispetto all'attuale protocollo Bitcoin.

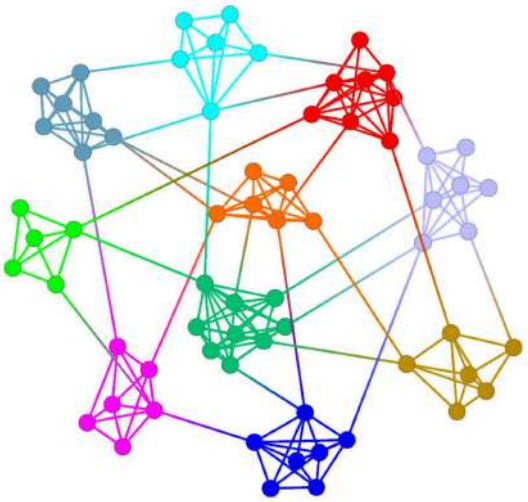


Figura 4.1: Rappresentazione di uno *small world graph*. Ogni colore rappresenta una comunità. (fonte)

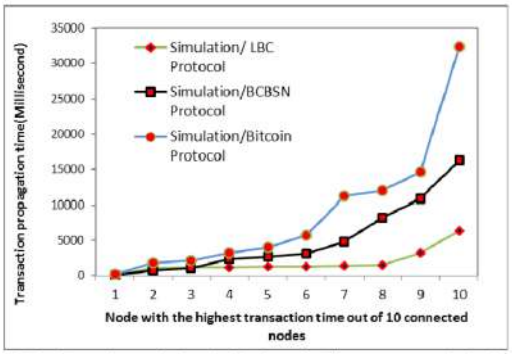


Fig.2: Comparison of the distribution of $\Delta t_{k,n}$ as measured in the simulated Bitcoin protocol with BCBPT protocol and LBC protocol simulation results.(d_t =50km).

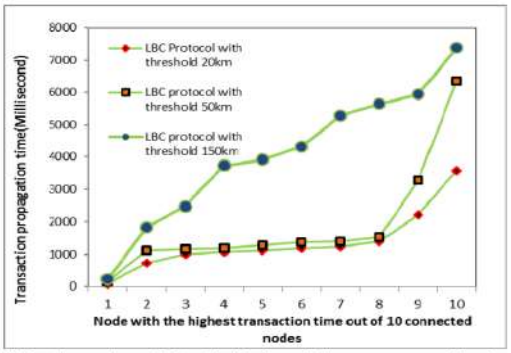


Fig.3: Comparison of the distribution of $\Delta t_{k,n}$ as measured in the simulated LBC protocol with three thresholds (d_t =20km, 50km, 150km).

Figura 4.2: Performance della rete utilizzando clustering geografico.

4.2 Gestione dei nodi unreachable

L'obiettivo di questo paragrafo, è di fornire un'idea di come i nodi *unreachable* possano essere utilizzati per aumentare la resilienza della rete. Non potendo andare attivamente ad influenzare il loro comportamento, possiamo attuare due tipologie di modifiche:

- modifiche al protocollo: possiamo infatti richiedere ad ogni nodo di essere più collegato con altri nodi: dovendo tutti avere più vicini, costringiamo i nodi *unreachable* a contribuire maggiormente alla propagazione delle informazione nella rete. Ciò però ha un costo, ovvero l'aumento di canali di comunicazione in tutta la rete. Ciò porta ad avere ridondanza (che è un problema attuale della rete Bitcoin) più che resilienza, ed impatta negativamente l'efficienza della rete.

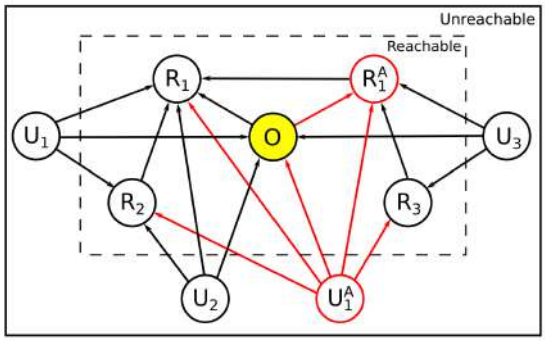


Figura 4.3: Rappresentazione di una porzione locale di una rete. R indica nodi *reachable*, ovvero nodi a cui si può arrivare seguendo le frecce, partendo da O (origine). La A indica nodi avversari, ovvero nodi che vogliono deanonimizzare la provenienza della trasazione. Per approfondire come ciò viene gestito, è possibile consultare [FD20].

- agire sui vicini di un nodo *unreachable*: aumentando il numero dei canali di comunicazione dei vicini di un nodo *unreachable*, si obbliga questo ad essere più partecipe alle comunicazioni sulla rete, in quanto più di frequente questo avrà informazioni da propagare. Ciò non crea problemi di ridondanza delle comunicazioni nella rete, in quanto sono azioni localizzate, ed influenzate dalla presenza di nodi *unreachable*, quindi non condizioneranno la maggior parte dei nodi. Inoltre, ciò si inserisce perfettamente nel contesto degli *small world graphs*, in quanto i nodi *unreachable* potrebbero svolgere il ruolo di nodi interni ad un cluster. Infine, i vicini dei nodi *unreachable* potrebbero essere incoraggiati a comunicare con i nodi che comunicano con l'esterno del cluster. Ciò permette ai nodi *unreachable* di contribuire alla trasmissione di informazioni intra-cluster già dal secondo passaggio di informazioni.

Per quanto riguarda la causa della presenza dei nodi *unreachable*, essa viene approfondita nel lavoro di Franzoni e Daza [FD20]: in larga parte è dovuto alla presenza di NAT (Network Address Translation, dispositivi o software che permettono di mappare indirizzi tra due reti diverse e incompatibili), in parte minore al semplice rifiuto della creazione di un nuovo canale di comunicazione.

4.3 Relay Network: potenziare la comunicazione tra cluster

Una relay network è un insieme di nodi il cui scopo è quello di distribuire efficientemente informazioni. Vediamo quindi come possiamo integrarla nel nostro modello *small world*.

Al momento, abbiamo tanti cluster di nodi geograficamente vicini, che comunicano in modo non ancora meglio specificato con altri clusters distribuiti nel mondo. Dentro ogni cluster, sono presenti dei nodi *unreachable* e dei nodi *reachable*, ma non abbiamo specificato come questi cluster comunicano gli uni con gli altri.

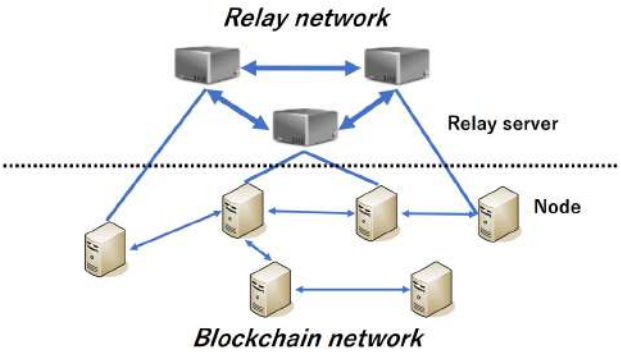


Figura 4.4: Modello di una relay network. I nodi in essa dispongono di collegamenti più performanti di quelli tra gli altri nodi.

Ovviamente, vogliamo evitare che un cluster abbia un solo nodo (o comunque pochi) incaricato di comunicare con l'esterno, altrimenti si rischierebbe di isolare parte della rete, perdendo in resilienza. Contemporaneamente, non tutti i nodi sono adatti per comunicare con altri cluster: essi devono essere molto connessi, e non devono avere restrizioni eccessive sull'ampiezza di banda. Inoltre, questi nodi potrebbero non verificare le informazioni che arrivano loro, ma delegare ciò ai nodi vicini, aumentando quindi la velocità di trasmissione.

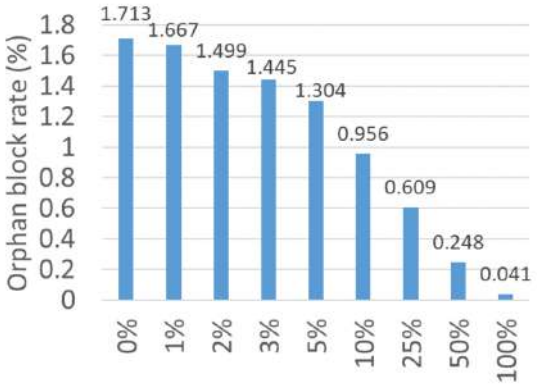


Figura 4.5: Percentuale di blocchi orfani in funzione della percentuale di nodi presenti nella relay network.

Organizzando opportunamente i nodi della relay network, Otsuki, Aoki, Banno e Shudo [OABS19] sono stati in grado di simulare le performance della rete, in particolare la maggior velocità di diffusione dei blocchi minati, permette di ridurre notevolmente il numero di blocchi orfani. In Figura 4.5 viene mostrata la relazione tra nodi nella relay network e blocchi orfani.

L'aumento delle performance della rete, però, viene ad un costo: stiamo aumentando la centralizzazione della rete. Tenendo presente che non tutti i modelli

di relay network presentano questo problema in egual misura (alcuni di questi sono riportati qui), bisogna far sì che questa gerarchizzazione della rete non ne comprometta la decentralità. Un'analisi più approfondita di ciò viene fatta in [SZT22].

Capitolo 5

Migliorie del protocollo della rete Bitcoin

Lo scopo di questa sezione è quello di analizzare i limiti dell'attuale protocollo di Bitcoin e presentare alcune delle migliorie proposte per rendere più efficiente lo scambio di informazioni tra i nodi della rete. Tra i diversi metodi proposti, vengono riportati, nel seguito di questo capitolo, quelli che hanno un maggior impatto in termini di efficienza sulla propagazione dei blocchi all'interno della rete Bitcoin:

- Minimizzazione delle verifiche
- Pipelining della propagazione del blocco
- Compact Blocks
- Graphene

5.1 Minimizzazione delle verifiche

Il ritardo nella propagazione di un blocco è sostanzialmente dovuto alla parte di verifica che ciascun nodo esegue prima di ritrasmetterlo agli altri nodi della rete con cui è collegato. Nel protocollo di Bitcoin, infatti, un nodo deve aver verificato la correttezza del blocco stesso e di tutte le transazioni presenti al suo interno prima di poterlo ritrasmettere. Questo nuovo protocollo suggerisce di inoltrare un blocco appena è stato ricevuto, rimandando la fase di verifica ad un momento successivo. In particolare, la fase di verifica di un blocco, può essere suddivisa in:

1. Controllo della correttezza del blocco;
2. Controllo delle transazioni.

La prima verifica consiste nel validare la Proof-of-Work (si calcola l'hash di tutto il blocco e lo si confronta con il target), controllare che all'interno del blocco vi sia l'hash

di un blocco recente e che non sia un blocco duplicato, ovvero un blocco che è gia stato ricevuto. Il secondo controllo effettuato richiede un tempo molto più lungo rispetto al primo ed è proprio questa fase che rallenta la propagazione dell'informazione tra i diversi nodi della rete.

La modifica del protocollo si basa sul fatto di posticipare la fase di verifica delle transazioni. Quando un nodo riceve un nuovo blocco, controlla la sua correttezza (esegue la verifica 1) e in caso positivo invia il messaggio *inv* ai nodi con i quali è connesso. In questo modo l'informazione dell'arrivo di un nuovo blocco è trasmessa velocemente a tutti i nodi della rete.

E' importante notare che la modifica proposta non incrementa in alcun modo il rischio di attacchi Denial of Service (DoS) ai diversi nodi della rete. Il pericolo di inviare dati non del tutto verificati è che un attaccante potrebbe diffondere un numero arbitrario di informazioni false aumentando il rischio di sovraccarico di alcuni nodi. Tuttavia in questo caso per poter compiere un attacco di questo tipo, un attaccante dovrebbe comunque risolvere la Proof-of-Work.

5.2 Pipelining della propagazione del blocco

Un ulteriore miglioramento delle prestazioni si può raggiungere inviando il messaggio *inv* ai nodi con i quali si è collegati, non appena si è a conoscenza dell'arrivo di un nuovo blocco (quindi ancora prima di averlo verificato). In questo modo l'informazione di arrivo di un nuovo blocco è propagata in maniera ancora più rapida, perchè viene minimizzato il tempo che intercorre nella trasmissione del messaggio *inv* e la ricezione del messaggio *getdata* dal nodo ricevente. Si precisa il fatto che il nodo A invierà l'intero blocco al nodo B solamente dopo averne svolta la verifica. Il messaggio *getdata* ricevuto viene quindi messo in coda finchè la procedura di verifica non è superata. Nel caso in cui questa modifica sia apportata al protocollo suggerito nel paragrafo precedente, allora la verifica che viene fatta prima di inviare il blocco è soltanto relativa alla validità della Proof-of-Work; la verifica della correttezza delle transazioni all'interno del blocco è posticipata ad un momento successivo. Nella Figura 5.1 è riportato lo schema appena descritto supponendo di applicare entrambe le modifiche finora proposte. Si noti, infatti, che la procedura di verifica è divisa in due parti (la prima significativamente più breve della seconda) a differenza di come avviene nel protocollo attuale di Bitcoin (Figura 3.2).

A differenza del caso precedente, l'applicazione di questa modifica potrebbe comportare qualche problema. In questo caso, siccome viene inviata la notifica di un nuovo blocco, senza nemmeno eseguire la verifica dell'hash del blocco ricevuto, è possibile che il blocco si riveli successivamente scorretto. Un attaccante potrebbe annunciare l'arrivo di numerosi blocchi che poi non sarà in grado di fornire. E' possibile che quindi vengano propagati nella rete annunci di nuovi blocchi che in realtà non esistono. Si noti, tuttavia, che l'impatto di questo attacco è relativamente piccolo, siccome la grandezza di un messaggio *inv* è di 61B. Inoltre, questo tipo di attacco è già presente nel protocollo attuale di Bitcoin: un attaccante può creare un certo numero di transazioni false e annunciarle alla rete. Infine, è importante sottolineare il fatto che questa modifica comporta un

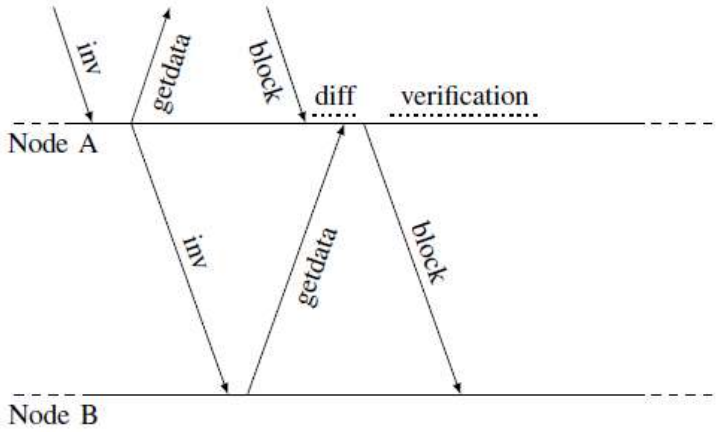


Figura 5.1: Scambio di messaggi tra due nodi della rete a seguito dell'applicazione delle strategie di miglioramento proposte (Minimizzazione delle verifiche e Pipelining della propagazione del blocco).

miglioramento significativo nella velocità di propagazione dell'informazione nella rete, soltanto se implementata da un gran numero di nodi.

5.3 Compact Blocks

L'obiettivo di questa modifica è quello di rendere più efficiente il protocollo di trasmissione delle informazioni nella rete Bitcoin, riducendo la larghezza di banda utilizzata e il numero di dati trasmessi tra i diversi nodi. L'idea sulla quale si basa questo protocollo è che quando un nodo riceve un blocco, esso possiede già gran parte delle transazioni che sono presenti al suo interno. Infatti ogni nodo ha uno spazio chiamato mempool, in cui sono presenti le transazioni che aspettano di essere processate e inserite nella blockchain. Inviare il blocco nella sua interezza è quindi ridondante e ritarda inutilmente la propagazione delle informazioni. La modalità con cui opera il protocollo è la seguente. Dopo aver validato un nuovo blocco, il mittente invia il messaggio *inv* e il ricevente risponderà con il messaggio *getdata* nel caso in cui non è ancora in possesso del blocco in questione. Il mittente, in questo caso, trasmette un *blocco compatto* che contiene le informazioni dell'header del blocco, tutti gli ID delle transazioni presenti nel blocco e le transazioni che crede non siano ancora possedute dal destinatario (come ad esempio la coinbase). Se il ricevente non ha ancora alcune transazioni le richiede al mittente. Nella Figura 5.2 è rappresentato il protocollo appena descritto.

Utilizzando questo protocollo, il blocco compatto che viene trasmesso occupa al massimo 20KB di dati. Questa è una grande riduzione rispetto al protocollo originario, in cui il blocco ha dimensione di circa 1MB. Compact Blocks è attualmente utilizzato nella rete Bitcoin (BIP-152) ed ha un impatto significativo. Tra i principali vantaggi vi è la forte riduzione di larghezza di banda necessaria per trasmettere le informazioni a tutti i nodi. In media, con questa modifica, il consumo di dati da parte della rete raggiunge

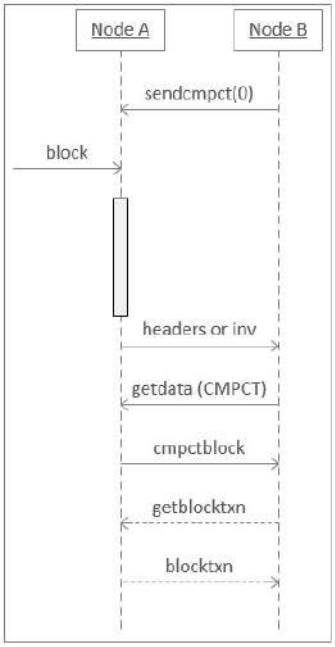


Figura 5.2: Scambio di messaggi utilizzando il protocollo Compact Blocks.

1.4 TB al giorno; ovvero si ha una riduzione di più del 90% rispetto a prima. Inoltre consente una maggiore velocità di propagazione dei blocchi nella rete Bitcoin: ogni nodo della rete impiega circa 15 secondi per ottenere l'informazione del nuovo blocco.

5.4 Graphene

Graphene è un nuovo metodo estremamente efficiente per trasmettere i blocchi all'interno di una rete Peer-to-Peer. L'idea è simile a quella dei blocchi compatti, in quanto si cerca di diminuire la grandezza dei blocchi, in modo da ridurre il ritardo nella loro propagazione. Tuttavia in questo caso la dimensione dei blocchi è ulteriormente ridotta rispetto a quella dei blocchi compatti. Anche il metodo su cui si basa il protocollo è differente. In Graphene viene utilizzata una combinazione di Bloom filters e Invertible Bloom Lookup Tables (IBLTs) come soluzione al problema di riconciliazione delle informazioni nella rete Peer-to-Peer. Per comprendere il protocollo ideato è necessario conoscere i due strumenti su cui si basa.

Bloom filters: Sono delle strutture dati che consentono in modo efficiente di verificare se un elemento appartiene o no ad un insieme. Il prezzo da pagare per questa efficienza è che i bloom filter sono una struttura dati probabilistica: la loro risposta è o che l'elemento certamente non appartiene all'insieme oppure che l'elemento potrebbe appartenervi. Per ulteriori dettagli fare riferimento alla sezione 3.

Invertible Bloom Lookup Tables: Sono delle strutture dati simili ai bloom filter ma che consentono di recuperare i dati mancanti oltre a testare la presenza o meno di elementi in un insieme. IBLTs sono molto utili quando un nodo vuole comunicare un insieme ad un altro nodo, che possiede gran parte degli elementi di questo insieme ma non tutti. Un IBLT può essere utilizzato per identificare gli elementi che mancano al ricevente. Nel contesto della propagazione dei blocchi nella rete Bitcoin, gli IBLTs possono essere utilizzati per 'spremere' insieme tutte le transazioni appartenenti ad un blocco in una stuttura dati fissata. Successivamente viene trasmessa questa struttura ad un altro nodo che si suppone conosca gran parte delle transazioni che sono state compresse, ma che potrebbe averne alcune mancanti o comunque potrebbe aspettarsi la presenza di alcune transazioni che in realtà non sono state inserite nel blocco inviato. L'IBLT è utilizzato dal destinatario per ricostruire l'insieme delle transazioni che sono presenti nel blocco. La grandezza dell'IBLT necessaria per avere una riconciliazione corretta è proporzionale al numero di differenze tra quello che il mittente ha inviato e quello che il ricevente si aspettava.

Siccome il protocollo Graphene fa uso degli IBLTs, per far si che sia efficiente è necessario che essi funzionino correttamente: la differenza tra l'insieme di transazioni che sono presenti nel blocco inviato dal mittente e l'insieme di transazioni che il ricevente si aspetta ci siano all'interno del blocco deve essere piccola. L'idea del protocollo Graphene è la seguente. Il mittente crea un IBLT I dall'insieme degli ID delle transazioni presenti nel blocco. Per aiutare il ricevente a creare lo stesso (o comunque simile) IBLT, il mittente crea anche un Bloom filter S degli ID delle transazioni nel blocco. Il destinatario usa S per escludere alcuni ID di transazioni dal suo mempool (che sicuramente non saranno nel blocco inviato dal mittente) e crea il suo IBLT I'. A questo punto il destinatario prova ad utilizzare I' per 'decodificare' I, in caso di successo otterrà gli ID delle transazioni presenti nel blocco. Il numero di transazioni che in modo errato appariranno in S, e quindi verranno erroneamente aggiunte a I' è determinato da una parametro controllato dal mittente. IBLT I può essere decodificato da IBLT I' con una probabilità molto alta se il numero di celle in I è 1.5 volte più grande della differenza attesa tra le entrate in I e quelle in I'. La differenza attesa tra le entrate dei due IBLT dipende dalla precisione del bloom filter S. Nel protocollo Graphene tutti i parametri sono specificati in modo che le dimensioni di queste strutture dati siano più piccole possibili, garantendo comunque un'alta probabilità di completare la procedura di riconciliazione nel modo corretto.
La maggior differenza tra Graphene e Compact Blocks è che invece di inviare l'header del blocco e tutti gli ID delle transazioni, il mittente invia un Bloom filter e un IBLT al destinatario. E' possibile dimostrare che Graphene performa decisamente meglio rispetto ai blocchi compatti [PABHL17].

Capitolo 6

Conclusioni

In questo documento abbiamo analizzato il funzionamento della rete Bitcoin, soffermandoci sulla topologia della rete e su come l'informazione venga propagata a tutti i nodi del sistema, allo scopo di sincronizzare le copie del registro che ciascun nodo possiede. Lo studio della struttura della rete, insieme all'analisi dei protocolli di propagazione dell'informazione tra i diversi peer, ha consentito di mettere in luce le debolezze del sistema. La diffusione dei blocchi nella rete è un aspetto molto delicato: ritardi nella propagazione causano un maggior numero di fork, che potrebbero compromettere la sicurezza del sistema. E' stato anche sottolineato come la dimensione eccessiva dei blocchi contribuisca ulteriormente alla lentezza della propagazione dell'informazione. Infine, l'enorme ridondanza nelle informazioni trasmesse rende inefficiente il sistema, limitandone le potenzialità.

Raccogliendo gli aspetti negativi, sono state riportate alcune proposte di miglioramento, volte a rendere più veloce ed efficiente il sistema e consentendo quindi una maggiore scalabilità e sicurezza. Le modifiche riportate in questo documento possono essere divise in modifiche al protocollo di comunicazione tra i diversi nodi della rete e modifiche strutturali della topologia della rete. Le modifiche al protocollo consentono di velocizzare la diffusione dei blocchi a tutti i nodi della rete, agendo sulla minimizzazione delle verifiche o sulla riduzione della dimensione blocco, rendendo quindi più scalabile ed efficiente il sistema. L'implementazione delle modifiche riportate potrebbe portare un grande vantaggio alla rete Bitcoin, o più in generale anche alle altre blockchain permissionless, costruite su una rete peer-to-peer. Alcune delle Blockchain in cui il tempo medio che intercorre tra l'arrivo di due blocchi è minore, sono implementate con alcune delle modifiche presenti in questo documento; riescono quindi a velocizzare il sistema, garantendone la sicurezza.

Bibliografia

[Ant17] Andreas M Antonopoulos. *Mastering Bitcoin : programming the open blockchain*. eng. 2nd ed.. O'Reilly, 2017. Cap. 8. ISBN: 9781491954386.

[DPH14] Joan Donet, Cristina Pérez-Solà e Jordi Herrera-JoancomartI´. «The Bitcoin P2P Network». In: vol. 8438. Mar. 2014. ISBN: 978-3-662-44773-4. DOI: 10.1007/978-3-662-44774-1_7.

[DW13] Christian Decker e Roger Wattenhofer. «Information propagation in the Bitcoin network». In: *IEEE P2P 2013 Proceedings* (2013), pp. 1–10.

[FD20] Federico Franzoni e Vanesa Daza. «Improving Bitcoin Transaction Propagation by Leveraging Unreachable Nodes». In: *2020 IEEE International Conference on Blockchain (Blockchain)*. 2020, pp. 196–203. DOI: 10.1109/Blockchain50366.2020.00031.

[FOA17] Muntadher Fadhil, Gareth Owenson e Mo Adda. «Locality based approach to improve propagation delay on the Bitcoin peer-to-peer network». In: *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. 2017, pp. 556–559. DOI: 10.23919/INM.2017.7987328.

[GCKG14] Arthur Gervais, Srdjan Capkun, Ghassan O. Karame e Damian Gruber. «On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients». In: *Proceedings of the 30th Annual Computer Security Applications Conference*. ACSAC '14. New Orleans, Louisiana, USA: Association for Computing Machinery, 2014, pp. 326–335. ISBN: 9781450330053. DOI: 10.1145/2664243.2664267. URL: https://doi.org/10.1145/2664243.2664267.

[GHJ22] Befekadu G. Gebraselase, Bjarne E. Helvik e Yuming Jiang. «Bitcoin P2P Network Measurements: A testbed study of the effect of peer selection on transaction propagation and confirmation times». In: *CoRR* abs/2205.00745 (2022). DOI: 10.48550/arXiv.2205.00745. arXiv: 2205.00745. URL: https://doi.org/10.48550/arXiv.2205.00745.

[MRM19] Joao Marçal, Luis Rodrigues e Miguel Matos. «Adaptive Information Dissemination in the Bitcoin Network». In: *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*. SAC '19. Limassol, Cyprus: Association for Computing Machinery, 2019, pp. 276–283. ISBN: 9781450359337.

DOI: 10.1145/3297280.3297309. URL: https://doi.org/10.1145/3297280.3297309.

[Nak09] Satoshi Nakamoto. «Bitcoin: A Peer-to-Peer Electronic Cash System». In: *Cryptography Mailing list at https://metzdowd.com* (mar. 2009).

[OABS19] Kai Otsuki, Yusuke Aoki, Ryohei Banno e Kazuyuki Shudo. «Effects of a Simple Relay Network on the Bitcoin Network». In: *Proceedings of the Asian Internet Engineering Conference*. AINTEC '19. Phuket, Thailand: Association for Computing Machinery, 2019, pp. 41–46. ISBN: 9781450368490. DOI: 10.1145/3340422.3343640. URL: https://doi.org/10.1145/3340422.3343640.

[PABHL17] A. Pinar Ozisik, Gavin Andresen, George Bissias, Amir Houmansadr e Brian Levine. «Graphene: A New Protocol for Block Propagation Using Set Reconciliation». In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. A cura di Joaquin Garcia-Alfaro, Guillermo Navarro-Arribas, Hannes Hartenstein e Jordi Herrera-Joancomartí. Cham: Springer International Publishing, 2017, pp. 420–428. DOI: https://doi.org/10.1007/978-3-319-67816-0_24.

[SZT20] Yahya Shahsavari, Kaiwen Zhang e Chamseddine Talhi. «A Theoretical Model for Block Propagation Analysis in Bitcoin Network». In: *IEEE Transactions on Engineering Management* (2020), pp. 1–18. DOI: 10.1109/TEM.2020.2989170.

[SZT22] Yahya Shahsavari, Kaiwen Zhang e Chamseddine Talhi. «Toward Quantifying Decentralization of Blockchain Networks With Relay Nodes». In: *Frontiers in Blockchain* 5 (2022). ISSN: 2624-7852. DOI: 10.3389/fbloc.2022.812957. URL: https://www.frontiersin.org/article/10.3389/fbloc.2022.812957.

LIGHTNING NETWORK

Aurora Costantino, Simone Galota, Filippo Grobbo, Giulio Quaglia

Abstract

Lightning Network is a new way to do payments using the Bitcoin blockchain. There are several features that improve some of bitcoin's most notorious problems such as speed and scalability. Lightning Network aims to create a vast network of nodes that allows anyone to move small amounts of money easily, quickly, safely, and inexpensively. The network is built through payment channels between two nodes. The construction of this structure is based on protocols that ensure security and that discourage and punish any attempt at fraud. In addition, every payment made through the network is secure and is not public, unlike on bitcoin, as protocols have been created and used that allow total anonymity. This paper will introduce the Lightning Network, explain the basics of its construction and the main features. In addition, some special and interesting aspects will be explored.

Chapter 1

A first glimpse to Lightning Network

The Lightning Network is a protocol developed to be used as a second layer technology on top of the Bitcoin blockchain. The best opportunities provided to Bitcoin are:

- improved privacy
- speed
- better scaling capability

1.1 Motivation

To understand the reason behind the lightning network implementation, let's try to answer the following questions:

1. Why is bitcoin not enough?
2. Why do we need Lightning Network?

A first consideration is that, nowadays the demand for bitcoin transactions is growing a lot. The nature of bitcoin blockchain implies that every machine participating needs to see, validate and store every transaction executed. Due to this fact bitcoin is becoming difficult to scale because the rise of the number of transactions will lead to saturating the block size limit, leaving the excess transactions to wait in a queue.

As a consequence, there will be a competition for assuring space in a block to obtain validation for its own transaction. This will result in higher fees and, as a result, a higher transaction cost, making micro-payments uneconomical. A currency system could never have allowed something like that to happen.

To solve this issue, the block size could be increased. In this way the costs will be shifted to the nodes and the problem will not be solved. The mining of a block will require more resources and the effect will be the undesired centralization of the system. In fact, this

would reduce the number of node operators leading to few well funded ones that control everything. Moreover, assuming that the network has to process thousands of transactions per second, we can't scale blockchain to validate the entire world's transactions in a decentralized way.

Concisely, Lightning Network is a way to have scalable off-chain transactions without losing the security of the bitcoin network.

1.2 Lightning Network main features

1.2.1 Basic concepts of LN

In order to better comprehend the LN, it is important to understand the difference between on-chain and off-chain payments:

- on-chain: when a payment is registered as a transaction on the underlying blockchain (e.g. Bitcoin). In bitcoin transactions are in broadcast and everyone is able to see them.

- off-chain: when a payment is sent through a channel between Lightning nodes, it is not visible in the underlying blockchain. Also, being a routed network, LN payments are routed among several channels, following a path from the sender to the receiver. In particular, Lightning Network uses the onion routing.

But, what is the role of a transaction when Lightning Network is used?
The LN uses real bitcoins which are always under full control of the user. Hence, LN relies on transactions to track the control of funds. Blockchain is used to load bitcoin onto LN and to settle at the end. In addition, LN works similarly to the traditional payment system in which you pay invoices instead of paying to a bitcoin address. Going into detail, the roles of the receiver and the sender interchange. Whereas in bitcoin the person who wants to receive the money sends the address to the person who wants to send it, in LN the person who wants to receive the money issues an invoice and the payer will pay by invoice

1.2.2 Main ideas

Let's see in detail the three main features.

- Privacy: there is more privacy because payments routed on the LN are transmitted between pairs of node and are not visible to everyone.

- Speed: the users of LN do not need to wait for block confirmations for payment.

- Better scaling: the users of LN can route payments to each other for low cost (few resources used, so cheaper) and (almost) real time. Also, fewer number of transactions are registered on the underlying chain (Bitcoin).

The LN proposes a new network as a second layer, where users can make payments to each other peer-to-peer, without the necessity of publishing the transaction to the bitcoin blockchain for each payment. The overall effects on the system are:

1. Reduced burden on nodes
2. Payments cheaper for user
3. Payments more private, not stored permanently

Chapter 2

Opening channels

In this chapter we will introduce some useful definitions to understand the creation of a Lightning Network channel. Then we will discuss its functioning going to deepen advantages, disadvantages and limitations.

2.1 Introduction

Before starting with the description of the channel opening and closing processes, it is worth to define some fundamental concepts such as channels and to recall some protocols.

2.1.1 Lightning Network channel

As we have seen in the previous chapter, the Lightning Network is made of channels. In order to better comprehend the whole process, we need to define the concept of a *payment channel*. The payment channel is a financial relationship between two nodes that from now on will be identified as Alice and Bob. The aim of the channel is to have many payments back and forth without committing each transaction to the blockchain. Moreover, the payment channel is managed by a cryptographic protocol that ensures that partners cannot cheat.

2.1.2 Hashed Timelock Contract

The Hashed Timelock Contract (from now on it will be referred to as HTLC) is a smart contract used on the blockchain that combines the use of hashes and timelocks. This is useful in order to protect loyal users from cheating ones and it will be clear in a few moments, in section 2.2. Let's focus on how this contract works. If Alice creates a transaction with Bob as recipient and protects it with an HTLC then Bob has to show the secret that unlocks the hash, and he must do this before a certain timeframe. If the deadline passes or if the correct password is not provided, Bob will no longer have access to that money. These types of smart contracts are one of the fundamental tools to build the Lightning Network. In fact, they have the characteristic of reducing counter-party risk.

2.2 Getting Started

2.2.1 How to open the channel

The first element needed to open a channel on the Lightning Network is bitcoin. Lightning Networks, as said before, is not a blockchain with its own currency and it is intended to work on the Bitcoin blockchain. To better understand the opening process, let's assume there are two nodes (or people), Alice and Bob, that want to open a lightning channel between them.

First of all, they need to choose how much bitcoin they want to allocate in the channel. Each part will lock a certain amount of money in the network and the total amount will represent the *capacity* of the channel between A and B.

Observation. *The following chapters will often use several terms that can easily be confused with capacity, so it is good to define and emphasize the differences between these terms:*

- *Capacity: is the maximum amount of value held in the channel, reserve included*
- *Balance: is the actual amount of satoshis held by each channel partner. Note that the balance is the difference between* inbound capacity*, to receive payments (IN) and* outbound capacity*, to make payments (OUT)*
- *Liquidity: is the available balance that can be effectively spent: its value is given by the balance minus the channel reserve and any pending HTCLs committed by the node*
- *Reserve: minimum balance in satoshis that is reserved on each side of the channel*

Let's go back now to our example. We imagine that Alice and Bob want to lock 2 BTC each on the channel so that its capacity will be 4 BTC. The purpose of the Lightning channel is to put only the opening and the closing transactions on the blockchain, the other transactions will take place off chain. The *opening transaction*, or *funding transaction*, is the one that creates formally the channel. The opening or funding transaction is simply a multisignature address 2-2 with Alice and Bob's public keys (clearly they need to be already exchanged), where the two parties will send their share. This transaction will be committed in the blockchain. Going back to the example, Alice and Bob will send 2 BTC each into an address where only with the signatures of both money could be moved.

The entire procedure just described is decided and controlled by the *message protocol* (can be found in the Github repository BOLT #2) that involves the exchange of six messages between Alice and Bob:

open_channel is the message sent by Alice when she decides to open a channel with Bob. It contains all the information for the settings of the channel. Bob can accept or not these settings. Some important parameters defined in this message are: which blockchain (mainnet or testnet) they will use, the amount of satoshis to fund the channel, the reserve, the delay of the self transaction (used in the timelock) and the public key of the 2-2 multisignature address that anchors the channel

accept_channel is the message sent by Bob to accept the request from Alice. Here, Bob can decide the minimum number of confirmations to wait once the funding transaction is written on-chain

funding_created is the message sent by Alice when she constructs the funding and the commitment transaction

funding_signed is the message confirming that Bob sent the necessary signatures (for the commitment not for the funding)

funding_locked is the final message that attests the minimum number of blocks of Bitcoin network to be waited after funding transaction to use the lightning channel

To prevent the situation where one part does not sign the multisignature address and so the other part loses money, each part requires an additional transaction (HTLC) called *refund transaction* that spends *from* the multisignature address to its own address, signed by the other. Once the refunding transaction is signed by Bob, Alice can securely broadcast the funding transaction that starts the channel. Note that the refund transaction will not be committed to the blockchain but each partner will send the signed transaction to the other partner. Creating this transaction allows the two partners at any moment to close the opened channel and not lose money. These two non-committed transactions (one toward self and one toward the partner) are the ones that finalize the balance of the channel. This transactions are also called commitment transactions (note that also the refund transaction is a commitment transaction but it has a different name since it's the first one). Going back to the example of Alice and Bob, after sending 2 BTC each to the multisignature address, Alice will sign a transaction from the multisignature address to Bob and send it to Bob. As collateral, Bob will do the same, so he will sign a transaction with Alice as recipient and with the multisignature address as input. Now the channel is open and can be used.

2.2.2 How the channel works

Once the channel is built, the two parts send each other money changing the balance of the channel. In order to change the balance, the two parts create two new transactions where they refund each one with the correct new amount of money. By doing this, the previous transactions will be revoked, so that it is impossible to regress to a previous state. In our example, let's assume that the first payment of the channel is Alice that wants to send 1 BTC to Bob. To do this we remind that the capacity of the channel is 4 BTC. This money is formally in the multisignature address. Since Alice wants to give 1 BTC to Bob, now 3 of those BTC are intended for Bob and only 1 BTC will go to Alice. So Alice will sign a transaction from the multisignature to Bob with 3 BTC and Bob will sign a transaction of 1 BTC to Alice. Those two transactions are not committed, they are only sent to the partner. In this way, the last balance is the only one we need to look at, all previous ones are revoked.

2.2.3 How the network works

An easy example

The operation of the Lightning Network is not trivial, in fact a whole chapter will be dedicated to it. For now, it is sufficient to make an example that helps to understand the potential. Let's consider that there is another person called Charlie who has already opened a channel with Bob. The capacity of the channel is 4 BTC and it is still unused, so 2 BTC are intended for Charlie and 2 BTC for Bob. At the moment, we have that the channel between Alice and Bob (A-B) has as balance 1 BTC to Alice and 3 to Bob. The channel between Bob and Charlie (B-C) has as balance 2 BTC to Bob and 2 to Charlie. In total then, if the channels were closed at this time, Alice would get 1 BTC, Bob 5 BTC and Charlie 2 BTC. If Alice wants to send 1 BTC to Charlie, she does not necessarily need to open a direct channel with him, she could leverage existing channels. In fact she could send 1 BTC to Bob who will send 1 BTC to Charlie. Let's check the balance of each channel and verify that Alice has 1 BTC less, Charlie has 1 BTC more and Bob has the same BTC as before. In the A-B channel the updated balance will be that Alice gets 0 BTC and Bob gets 4 BTC. In the B-C channel, instead, Bob gets 1 BTC and Charlie gets 3 BTC. So if we closed the channels right now, we would have Alice getting 0 BTC, Bob 5 and Charlie 3, as we wanted.

2.2.4 Some considerations

From this example, it is useful to note that the capacity of a channel is related to the maximum amount of money that can travel in one direction. In fact, currently in the A-B channel, the only possible transactions are those with Alice as the recipient. This is because the balance in the A-B channel is 0 for Alice and 4 for Bob. Therefore, Alice has no possibility to send money to Bob through this channel. A question that might arise is: if Alice does not know about the open channel between Bob and Charlie, how can she send him money? The Lightning Network was created so that you have algorithms that can find the best path between existing channels for the transaction you want to do. This algorithm is called unsurprisingly, *path-finding*. In addition, to prevent the balance information of the various channels from being known and to prevent intermediate nodes from knowing the sender and receiver of the transaction being carried out in the channel, there is a privacy protocol called *Onion Routing*. In Chapter 4 all these details will be fully explained.

How to announce the opening channel

An important step that should not be overlooked is that of channel announcement. In fact, in order to use a particular channel to make a payment through the network, it is necessary at the very least to know that the channel exists. Moreover, since the refunding transactions are not committed to the blockchain until the channel is closed, it is impossible to go back a transaction up to a lightning channel. This means that the channel, if it is intended to be used by the network, needs to be announced in a different way. When the channel partners agree to announce the channel to the Lightning Network, that

particular channel will be a *public channel*. This allows other nodes to use the channel for routing and generates routing fees for partners. On the contrary, an *Unannounced channel* is known only to partners, but it is incorrect to define it as "private" because its existence and capacity will be revealed with the final transaction for the settlement. You can still use an unannounced channel to route payments, but only by nodes that are aware of their existence or if they are included in "routing hint" paths. The announcement of a channel includes metadata like the fees and timelock duration, but not the liquidity.

Chapter 3

Closing channels

To understand how to close a channel is important to see how a commitment transaction works.

3.1 Commitment transaction

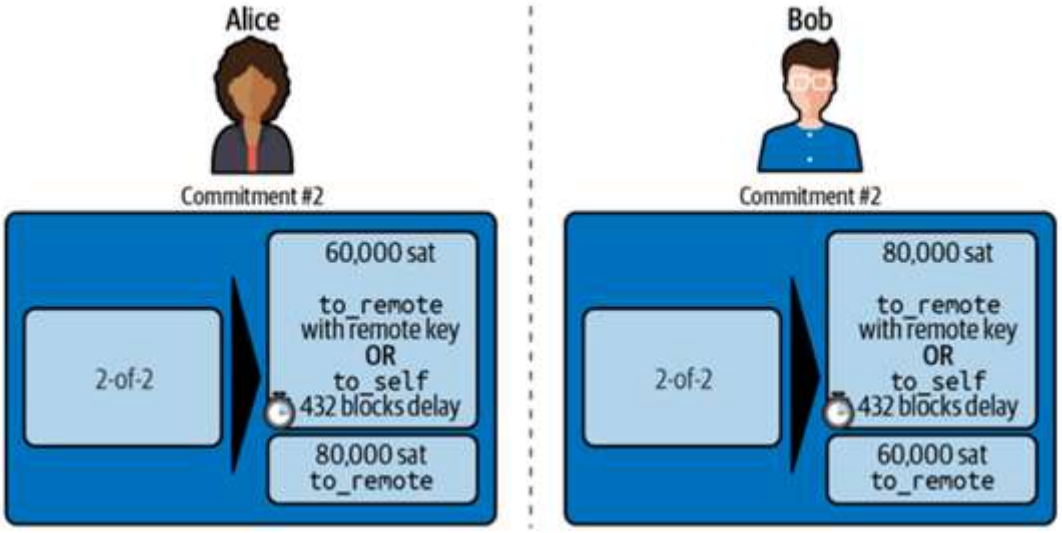
A commitment transaction is a transaction that pays back each channel partner and ensure that they don't have to trust each other, signing a commitment gives the other partner the ability to get their funds back on the current balance even without the cooperation of the other partner. The initial commitment transaction gives back all the funds to the partner that open the channel but the generally the commitment is updated to the last balance.

Alice wants to create a channel with capacity of 100k sats with Bob, let's see how the protocol works:

- Alice creates a public/private pair and informs Bob that she wants to open a channel with him *open_channel* message;
- Bob receives the *open_channel* message and creates a public/private pair and confirm to accept the channel with the *accept_channel* message;
- Alice creates a funding transaction of 100k sats with a multisig address: 2 <PubAlice> <PubBob> 2 CHECKMULTISIG ;
- Alice does not broadcast this transaction, but send the transaction ID with the *funding_created* message with her signature for Bob's commitment transaction;
- Both create their commitment transaction that send back the funds to Alice. They don't need to exchange these commitment transactions, they only need signatures;
- Bob provides a signature for Alice's commitment transaction and sends this with the *funding_signed* message;
- Now Alice can broadcast the funding transaction.

If Bob stops responding Alice can send the commitment transaction and receive her funds back, the only costs are the fees for the on-chain transactions. Commitment transaction are created every time there is a change in the balance, with the relative exchange of signatures

The commitment transaction looks like that:



The first part of the script allows the output to be spent by anyone with the revocation key.

Putting funds in a 2-2 multisignature address carry some risks, what will happen if one of the partner of the channel refuses to sign a transaction to release the funds? What if he broadcast an old commitment transaction? Let's see how the protocol avoids this possibilities.

3.2 Cheating with prior state

Once the channel is opened and some transactions have been done there are multiple *commitment transaction* that represents states of the channels. The only transaction that represents the actual balance of the channel is the last one, but one of the partners of the channel might be tempted to publish a different transaction than the last one that represents an incorrect (old) balance.

Bitcoin transactions do not expire, can't be deleted, stopped or censored once they have been broadcast, so to prevent this behaviour the Lightning Network protocol implements a mechanism of penalties.

There are 3 elements that make up the Lightning protocol revocation and penalty mechanism:

- **Asymmetric commitment transaction**: Alice and Bob transactions are different, Alice has a transaction that pays *to_self* with a timelock and pays *to_remote* (to Bob) immediately, while Bob has the exact opposite of that.

- **Delayed spending**: the payment *to_self* is delayed through HTLC to allow the remote party to exercise a penalty option, the delay can be negotiated at the opening of the channel .

- **Revocation keys**: as seen in chapter 2 even if revocation can be misleading because the transactions on the blockchain can't be revoked, the revocation keys are crucial since if an old commitment transaction is used, a penalty transaction can be created. The commitment transaction has an option to be spent *to_self* immediately if you have the complete revocation key.

It's worth noting that fraud attempts are not automatically detected by the network in fact, both Alice and Bob have to monitor the blockchain searching for commitment transaction related to their channel, if an old commitment is broadcast in the network they have to construct the penalty transaction. There are few ways to detect a cheat:

- A lightning node operating 24/7

- A watchtower node watching for the channel: it can be a Third-party watchtower or a personal watchtower.

3.2.1 Advancing the channel state

To advance the channel state Alice and Bob exchange two messages:

- *commitment_signed*, gives the signature needed for a new commitment transaction. It contains the channel id, the signature, the number of the HTLC and the HTLC signature. Starts from the partner that wants to do a transaction and update the balance;

- *revoke_and_ack*, contains channel id, per commitment secret and the next per commitment point. For example Alice wants to create a new commitment and send the sign, Bob wants to revoke the old commitment to assure that Alice won't use it, Alice will trust the new commitment only if she had the key to revoke the previous one. In the revoke_and_ack Bob gives the per_commitment_secret that can be used to reconstruct the revocation key.

3.2.2 Revocation keys derivation

Every time Alice starts a new commitment transaction Bob doesn't want that Alice can use the old commitment with a different balance in the channel. To do so Alice must give Bob a signature for the new commitment. On the other hand Alice wants the part of the secret of Bob in order to trust the new commitment.

This exchange is done in the revoke_and_ack message. In our example where Alice propose the new commitment Bob gives Alice the per_commitment_secret. This secret can be used to reconstruct the revocation key for the old commitment. How does it work?

- in the initial channel negotiation they exchange the revocation_basepoint, a static point for the lifetime of the channel and the first_per_commitment_point, changed in every advancement in the state of the channel

- the revocationpubkey is derived:

  revocationpubkey = revocation_basepoint *
  * sha256(revocation_basepoint || per_commitment_point) + per_commitment_point
  * sha256(per_commitment_point || revocation_basepoint)

  and finally derive the private key from the public key:

  revocation_priv = (revocationbase_priv * sha256(revocation_basepoint || commitment_point)
  + (per_commitment_secret * sha256(per_commitment_point || revocation_basepoint)
  mod N

In other words the revocation_priv can only be derived (and used to sign for the revocationpubkey) by the ones that knows both his revocationbase_priv and per_commitment_secret.

3.3 Channel management

The principal issue for a Lightning channel is to maintain the balance of the channel.

As soon as you have a node up and running, you can start opening channels with those funds. The partners must be chosen wisely because the ability to send payments across the network depends on how well connected they are with the rest of the network. Usually you want more than one channel to avoid the single point of failure but you don't want too many channels or channels too small. You can use an autopilot software to open and close automatically channels, but is better to do it manually the first times.

In the current design of lightning network is very common to have outbound liquidity before obtain inbound liquidity, there are typically three way for getting inbound liquidity:

- Open a channel and spends the funds;

- Use a submarine swap like Loop in, by lightning labs, that accepts a Bitcoin on chain payment and converts it into Lightning liquidity;

- Pay a third-party service to open a channel with your node.

If someone is frequently routing payments through your node you may exhaust inbound liquidity through channels (or outbound, not be able to receive or to do payments are the same problem). What you want to do is have a balance between inbound and outbound liquidity so you have to *rebalance* the channel, there are three way to do this:

- One way is submarine swap;

- Another way is to wait to payments that flows in the other direction;

- A third way is to rebalance channels creating a circular route that sends payments from your node through the network and back to your node.

3.3.1 How to close the channel

In terms of closing a channel there are several methods and reasons. Three will be shown: mutual close, forced close and protocol breach. In general opening and closing channels many times is not very convenient since the opening and closing transactions are committed to the blockchain and therefore it is necessary to pay the fees. Avoiding fees is, as said before, one of the main reason channels are used and for this reason channel tends to stay opened. Therefore it can be necessary to close a channel for some reason:

- Reduce the balance held on Lightning channels and secure theme in a cold storage (mutual)
- Unresponsive channel partner (force close)
- Channel not used often, the channel partner is not a well connected node (mutual)
- Cheating partner (protocol breach)

Mutual Close

Mutual close is a friendly close, both parties agree to the closing procedure and the final budget. No new routing attempts will be accepted and ongoing attempts will be settled or removed after a time out. Together they decide to commit a transaction that is very similar to the two transaction created to update the balance of the channel called *closing transaction*. The only difference is that the outputs are not locked with a timelock, so the money can be spent immediately, while the output is according with the channel balance. The fees are paid by the partner who started the channel.

The messages involved in this procedure are:

- *Shutdown*, contains the channel id and the bitcoin script corresponding to the address of the wallet. Both partners exchange this message.
- *Closing_sign*, contains the channel id, the transaction fee and a signature. Both partners have to agree on the fee, it starts a negotiation that ends up when a couple of messages with the same fee is exchanged.

Force Close

Force Close is a non-consensual close. Only one partner decides to close the channel and so has to pay the fees. This often happens when one party is not reachable. In this case, the partner that wants to close the channel will publish the last transactions that commits the balance of the channel. In order to prevent people from sending the wrong balance transactions, the partner who publishes the closing transaction will receive the output encumbered by a timelock, while the other's will be spendable immediately. This is a safeguard: in fact if someone wants to cheat and send an earlier commitment transaction, then the timelock will give the partner the opportunity to dispute the transaction and punish the partner for the cheating.

In general a force close is not recommended because the funds will be timelocked and the fees for this type of transactions are very high for several reasons:

- when they create a transaction the fee must be counted in the outputs, but no one can know the price of the fee in the future, so it can be set up to 5 times higher
- pending routing attempts of HTLC must be included in the outputs, so the transaction will be larger (in bytes) and so the fees
- any pending routing attempts must be solved on-chain

A force close is not recommended unless necessary.

Protocol Breach

A protocol breach is a dishonest close. This happens when a partner tries to publish an outdated commitment transaction using a force close. Unfortunately, in order to detect this fraud, the victim node must be online. As seen for the force close, the cheating partner who wants to close the channel will have the payment encumbered by a timelock. During this time the other partner can detect a protocol breach and publish a *punishment transaction* that guarantee (if indeed there is an attempt to defraud) the non-cheating partner all the money of the channel even though he has to pay all the fees. In fact in the structure of the commitment transaction the two outputs can be spent, the one with the timelock can be immediately spent with the revocation keys while the other one is already spendable. If the protocol can't detect the fraud, the committed transaction used for closing the channel will be considered valid and the channel money will be divided according to the stated.

Chapter 4

Pathfinding & Onion routing

4.1 Peer-to-Peer Gossip protocol

The building of a payment channel in the LN can be made public and communicated over what is called the peer-to-peer gossip protocol. In a classic peer-to-peer protocol each node connects directly to a random selection of other nodes called peers. The most important features of a public payment channel are:

- node announcement: it contains the features to identify the node such as the public key and the address
- channel announcement: this contains the capacity of the channel
- channel update: it contains the node's fee and timelock expectation for routing from the node's perspective

Announcements are sent by each node to its peers and after verification the peers will forward announcements to their peers and so on. In order to prevent excessive communication between nodes, announcements are forwarded only once per node. On the other hand, the sharing of channel update can be forwarded approximately four times a day since each node could decide to modify its requests in terms of fees and timelock.

An important feature that is not public is the liquidity of the channel. The knowledge of channel's liquidity is crucial for topology information about the network. In fact, a node can forward as much satoshis as it actually owns within that channel. However, it has been decided to exclude liquidity from the public features for different reasons:

- protect users' privacy
- scale the amount of payments. LN was created because notifying every participant about every payment doesn't scale well
- LN is a dynamic system, so the changes will be valid only for short amount of time. This means that saving and sharing this information will result a waste of memory

4.2 Pathfinding

Pathfinding is the process of finding a path between two distinct nodes that are not directly connected. LN uses a source-based protocol for pathfinding, which means that the sender of the payment has to find the path to the recipient on its own. Since the liquidity of the channel is not publicly known, this problem is completely different from the standard and well known pathfinding algorithm and it is not a completely solved problem. Nodes use information from the gossip protocol to obtain information about the network topology.

Best path selection could be done depending on the definition of *best*. In fact, we could consider the best path in terms of liquidity, lower fees or shorter timelocks if we want to avoid locking funds for too much time. From a mathematical point of view, LN could be seen as a directed graph with capacity constraints since the balance of a channel could not be equally distributed and there is a capacity for each channel of the network. In particular, it will be useful for the next parts to remind two important quantities:

- channel reserve or minimum liquidity: minimum balance in satoshis that is reserved on each side of the channel
- maximum liquidity: it is the capacity minus the channel reserve

4.2.1 How the algorithm works

We can summarize the main idea of the entire algorithm in three steps. The first part is the *channel graph construction*, which is essentially done by the sender using information from LN gossip to discover nodes and channels. This part is done thanks to channel announcements, node announcements and channel updates. In particular, channels with insufficient capacity are already excluded from the list of available channels.

The Second part consists in *finding candidate paths*. Path discovery is done backward, from recipient to sender, in order to accumulate fees and timelocks. The reason for doing this will be clear in the section about onion routing. This can be done using a classical algorithm such as Dijkstra. In addition, we can filter possible routes using fees, timelock, estimated liquidity or some combination such as a cost function for each channel.

The third part is called *payment attempts*. We sometimes refer to it as the trial-and-error loop since it consists of trying each path until payment succeeds. The application of probability theory to payment delivery demonstrates facts that could seem intuitive such as:

- smaller payments have better chance of success
- larger capacity channels give better chance of payment delivery for a specific amount
- the more channels are used, the lower chance of success

The trial-and-error loop starts building HTLCs for onion routing and continues to attempt payment delivery. The onion routing part will be better clarified in the next section.

Right now, it is more important to analyse the possible results of the attempt. A payment, in fact, could return a success, an error or a block if no response has occurred. In case of an error, we can use failed HTLCs to update channels' liquidity gaining more information about the network. Since the *channel graph construction* is done by the sender and thanks to the onion routing, it is possible to understand which channel is responsible for the error. In this way, we can update liquidity estimates and reduce uncertainty. The same could be done in case of success because the sender knows the amount of satoshis and fees sent to each channel. However, all the sender's knowledge is temporary, as each LN node could be involved in other payments at any time, changing its liquidity. Instead, when a block occurs, we define this event as a stuck payment: neither fulfilled nor cancelled by an error. Two possible reasons for a stuck payment could be: a node going offline or a malicious node holding HTLCs without doing anything. In this case, the only thing to do is wait until timelocks expiry, since senders cannot cancel payments. The introduction of Taproot and Schnorr signature's features on Bitcoin in 2021 is helping research areas to solve this limitation of the LN introducing Point Time-Locked Contracts (PTLCs). These are particular payment contracts that use a different cryptographic protocol than HTLCs.

4.2.2 A new feature: Multiparts payment

Another important innovation that has been introduced recently in 2020 is multipart payment. It allows a payment to be split into multiple parts, which are sent as HTLCs over different paths to the same recipient. Atomicity is preserved since either all payments are eventually fulfilled or the entire payment fails. The idea behind each single payment is the same as before, while the main difference from the initial approach is that we also have to consider how to split payment to optimize delivery. The main advantages of these payments are:

- possibility to use paths that were previously unavailable
- if some parts fail with error we can repeat the trial-and-error loop only for the residual amount
- channel graph's update could be done using information obtained both from the successes and errors of previous round.
- it has been shown that they increase the probability of a successful payment compared to single-path payment

An important question that is still an area of ongoing research is how to split payments and if there is an optimal number of splits and an optimal amount of satoshis for each of them. For example, The *zero base fee movement* is a movement founded by Renè Pickhardt whose goal is to simplify payment routing by pushing lightning channels to adopt a zero base fee. It has been shown that this allows the routing algorithm to converge much faster.

4.3 Onion Routing

Onion routing was invented before LN, for example it was used as a communications security protocol by U.S Navy researchers and also implemented in Tor in order to use internet privately and anonymously. The aim of this method is to send payment by building successive nested layers of encryption where the innermost layer is intended to be the payment's recipient. All the other intermediaries are supposed to peel off one layer at a time, such as the skin of an onion. A fundamental hypothesis of this procedure consists of having path available from payer to receiver. This could be done by the sender thanks to pathfinding. In addition to this, onion routing ensures that the sender knows the destination and length of the path while every intermediary only knows the previous and next node.

In order to understand the following, it is useful to define three concepts:

hop: each intermediary node between the sender and the recipient

hop payload: the information communicated to a node by the sender

onion: the final message which consists of encrypted hop payloads put together

After path selection, the sender starts constructing payloads backward from the receiver. We can distinguish two different types of payloads: the final hop payload and every other hop payload. The final one will be the payload for the recipient and contains information such as the amount of payment in satoshis, timelock and payment secret. This last is a sequence of 256 bits taken from the initial invoice, which allows receiver to recognize the incoming payment. Every other hop payload instead contains only channel id, amount of satoshis to forward and timelock.

The amount of satoshis and timelocks must be fixed according to the channel update given by the gossip protocol. This should be done increasingly while proceeding backward. For example, let's say Alice wants to send 5000 satoshis to Dina using the path composed by Alice-Bob-Carl-Dina. Alice must consider the following channel updates:

- Bob: 10 satoshis for fees, 20 blocks to expiry timelock. This means that if right now the Bitcoin blockchain has recorded 700 blocks, the 10 satoshis wouldn't be spendable until the block number 720
- Carl: 10 satoshis for fees, 20 blocks to expiry timelock
- Dina: 18 blocks, satoshis for fees doesn't matter since she is the recipient

The payloads to satisfy the above constraints are:

- Dina'payload: payment secret and information about timelock, fees. The last two aren't important in this case because Dina is the recipient. (dina ha timelock perchè fino a quel momento non potrà avere i soldi sulla liquidità)
- Carl's payload: 718 blocks, 5000 satoshis, Carl-Dina's channel id

- Bob's payload: 738 blocks, 5010 satoshis, Bob-Carl's channel id

The process ends correctly since Alice sends 5020 satoshis to Bob with 758 blocks timelock. Every other node will follow the instruction given in the hop payload to build an HTLC for the next node of the path. The increasing number of blocks for the timelock is a key aspect to prevent fraud. Thanks to the fact that other hop's payload are higher in terms of blocks, all path's member have time and opportunity to get back their satoshis. In addition, it is useful to observe that in each payload there is only one id of a channel. Every hop will consequently know only the previous and subsequent node of the path without understanding which is its position in the path. Just the receiver knows it is the final node thanks to the payment secret that is shared initially in the invoice.

Once every payload is available to the sender, the onion is ready to be built. The onion's wrapping consists in generating a 1300 byte onion payload for each node of the path. This part is done by the sender using cryptographic tools such as HMAC, XOR operations, Chacha20 and a filler (like padding, it fills onion payload with a pseudorandom byte stream). The unwrapping part is possible thanks to an initial sharing of three keys done in the wrapping phase for each hop. In few words, to peel the onion it is necessary to de-obfuscate hop payload, take information to construct the next HTCL and construct the new onion packet for the following hop. Reconstructing the onion is necessary because some parts of the onion are removed during the de-obfuscate phase. Onion packet received by each hop indeed must be the same size because it prevents intermediary nodes from knowing their position in the path.

Chapter 5

LN vs Bitcoin

The LN is a peer-to-peer protocol that could be seen from different points of view. On the one hand, it is a peer-to-peer network that uses the gossip protocol to propagate information such as the topology of the network. On the other hand, it is a network of payment channels between channel partners. It is important to note that these two interpretations are linked because communication between peers exists. In fact, The noise Protocol Framework is used to exchange the so called *Lightning messages* based on the construction of encrypted communication. Noise protocol ensures also that every message on the network is authenticated, increasing privacy and resistance to traffic analysis.

Although the Lightning Network and Bitcoin have some common aspects (being LN on top of Bitcoin), there are also a lot of architectural differences that it is worth highlighting.

5.1 Similarities

1. **Monetary Unit**
   Both Bitcoin and LN use the same monetary unit: the bitcoin.

2. **Irreversibility and Finality of Payments**
   For both system there is no *chargeback* operation. So, a sender has to act carefully, but the receiver has the guarantee about the finality of the transaction.

3. **Trust and Counterparty Risk**
   In both systems, you have to trust only mathematics, encryption and that the software does not have risky vulnerabilities.

4. **Permissionless Operation**
   Both can be used by anybody, just having an internet access and a wallet.

5. **Open Source and Open System**
   Both are global, open and free

5.2 Differences

1. **Addresses Versus Invoices, Transactions Versus Payments**
   On Bitcoin system, a user who has to make a payment needs to get the receiver address (e.g. scanning a QR code). Then, using its own wallet, it can create a transaction to sends money. Instead, on the LN the receiver of a payment creates an invoice, sending it to the sender. Thus, while address are reusable (even though it is not suggested), in LN a new invoice must be created for each payment.

2. **Selecting Outputs vs Finding a Path**
   On Bitcoin, to make a transaction, a sender needs to select one or more UTXOs. In contrast, LN uses a series of channels to route and find a path from sender to receiver. Each channel must have sufficient capacity to route the payment. Therefore, each payment is an update of the channel balance. Funds are moved from one end to another.

3. **Change Outputs on Bitcoin vs No Change on Lightning**
   UTXOs can be spent exclusively in full. Thus, a user having a 2 BTC UTXO needs to make two transactions on bitcoin network to spent only 1.5 BTC. One for the real payment (1.5 BTC) and one for accrediting himself the change (0.5 BTC). The last one creates a new UTXO, the "change output". On LN, once bitcoins are locked in the channel, portions of them can be sent, without the need to have change.

4. **Mining Fees vs Routing Fees**
   On Bitcoin, users pay fees to miners for having their transaction included in a block. Fees are based on the transaction size in bytes and on how quickly the user wants this transaction mined. On the Lightning Network, users pay fees to other intermediary nodes to route payments through their channels. There is a base fee for each payment and a fee rate based on the value of the payment.

5. **Varying Fees Depending on Traffic vs Announced Fees**
   The market fee on bitcoin depends on the available space in a block. Because the scarce resource is space. So, if there are many transactions in queue, users have to pay an higher fee to be included in the next block. In contrast, in the LN the scarce resources are channel liquidity and channel connectivity.

6. **Public Bitcoin Transactions vs Private Lightning Payments**
   Bitcoin transactions are public and stored forever. Even though the addresses are not tied to an identity, there is the chance, with blockchain analysis, to execute mass surveillance. In LN payments, only the sender and the receiver are fully aware of the source, destination and amount exchanged. But the receiver may not even know the source of the payment. Moreover, the users who route are only aware of the amount exchanged. Eventually, when the channel is closed the information about the payment are not stored anymore.

7. **Incentives for Large Value Payment vs Small Value Payments**
   The different fee structures in the two systems led to different usages of the network

in relation to the amount of payment. Bitcoin will be used for large value payments, having fee independent from amount. Instead, users will prefer LN for small value ones.

8. **Satoshis vs Millisatoshis**
   The Lightning network overcomes the micropayments limit because, unlike bitcoin bitcoin, the smallest spendable amount is the milli-satoshi. A satoshi divided by 1000. When the channel is closed, balances are rounded to the nearest satoshi.

TERRA (LUNA)

Annalisa Deiana, Emanuele Formento, Davide Leone, Michele Vioglio

Terra (LUNA)

7 giugno 2022

1 Introduzione

1.1 Contenuti

Terra (LUNA) è una blockchain decentralizzata e open-source, costruita utilizzando Cosmos SDK, che ad oggi fornisce i tre primitivi del mondo finanziario: possibilità di pagamento, possibilità di investimento (e scambio di titoli) e accantonamento risparmi.
Alla base del funzionamento di Terra troviamo il token di governace Luna, il quale ricopre diversi ruoli all'interno della chain, che vedremo di seguito.
Terra differisce dagli altri ecosistemi perché non è la solita blockchain scalabile, ma si propone come una vera alternativa ai pagamenti tradizionali.

Questo paper si pone l'obiettivo di far comprendere al lettore il modo in cui funziona la blockchain Terra(LUNA), approfondendo in particolar modo i delicati meccanismi dietro ai quali i prodotti della chain, ovvero le stablecoin algoritmiche, riescono a mantanere stabile nel tempo il proprio prezzo legato alle varie valute FIAT.
Ma prima di fare ció é importante fare una disamina delle varie tipologie di stablecoin che oggi il mercato ci offre per comprendere la vera utilitá di questo ecosistema.
Inoltre si dará una panoramica generale sull'attivitá DeFi presente on chain.

1.2 Stablecoin

Le stablecoin sono criptomonete che mantengono il proprio valore stabile, ancorato a quello di un altro asset. Per mantenere questa stabilità si utilizzano dei collaterali.
Le stablecoin sono state create con l'obiettivo di avere una criptomoneta dal valore meno volatile delle classiche criptovalute (come Bitcoin, col valore dettato dalla domanda e dall'offerta sul mercato), risultando maggiormente utilizzabili come mezzi di pagamento o come riserve di valore, il che incoraggia il loro utilizzo nelle transazioni quotidiane.
Nonostante questa differenza, le stablecoin mantengono alcune importanti caratteristiche ereditate dalle criptovalute non ancorate. In particolare, sono sempre accessibili tramite internet, globali e possono essere utilizzate negli smart contracts.

Esistono due tipi principali di stablecoin:

- **Centralizzate**: questa tipologia di stablecoin viene emessa e regolata da un'azienda che si fa carico di tutte le responsabilità. Una stablecoin centralizzata è tipicamente ancorata a una valuta fiat, per esempio il dollaro, con cui stabilisce un cambio fisso 1:1.
  Dunque, per avere a disposizione un determinato importo di stablecoin è necessario pagare il medesimo importo in dollari. Il collaterale sottostante viene depositato in riserva presso un emittente centrale o un'istituzione finanziaria e deve rimanere proporzionale al numero di stablecoin in circolazione.
  Nonostante la collateralizzazione risulti stabile, viene a mancare totalmente la decentralizzazione, cioè il motivo per cui le criptovalute sono nate.

- **Decentralizzate**: in questo caso le stablecoin sono emesse e gestite tramite l'utilizzo di smart contract e piattaforme DeFi; dunque, non c'è nessun ente centrale che le regolarizza.
  Le stablecoin decentralizzate si dividono in due categorie:
  - Sovra-collateralizzate: hanno come collaterale un asset volatile. Vengono create tramite smart contract bloccando una quantità maggiore di criptovalute rispetto all'ammontare di stablecoin creato. Nel momento in cui viene restituita la somma di stablecoin creata, le criptovalute impiegate per la creazione vengono sbloccate.
  - Algoritmiche: non utilizzano valute fiat o criptovalute come collaterale ma la loro stabilità dei prezzi deriva dall'uso di algoritmi gestiti da smart contract e dall'arbitraggio. Alla base di questa tipologia di stablecoin ci sono meccanismi per coniare e bruciare il token di governance e la stablecoin ancorata.

Le stablecoin di Terra appartengono alla categoria delle stablecoin algoritmiche. Il token di governance è Luna, mentre le stablecoin sono quelle ancorate alle valute fiat, per esempio UST.

1.2.1 Vantaggi

Il principale vantaggio delle stablecoin centralizzate é il fatto che siano controgarantite dalla controparte FIAT, quindi ad esempio per ogni token del valore di 1$ é presente 1$ di moneta FIAT nelle riserve dell'ente centrale che lo emette. Questo permette di avere stabilitá e continuitá nel prezzo della stablecoin.

1.2.2 Svantaggi

Ovviamente questo presenta un enorme svantaggio, appunto la centralizzazione, poiché permette a chi emette il token di averne il controllo; quindi in alcuni casi l'ente puó, a sua totale discrezione, congelare i fondi blacklistando gli address che li detengono.
Questo é giá accaduto in passato con Tether, azienda dietro a USDT, la quale dopo un attacco hacker che ha prosciugato un pool di liquiditá, é internvenuta freezando i fondi rubati.
Magari ció viene inteso come un vantaggio ma di fatto si ritorna alla vecchia retorica in cui ci si deve fidare dell'organizzazione dietro.

1.2.3 Scopo stablecoin algoritmiche

Le stablecoin algoritmiche hanno come scopo principale proprio evitare che sia possibile avere il controllo dei token emessi, garantendo così la decentralizzazione.

2 Protocollo di consenso

2.1 Algoritmo di consenso

Terra segue un algoritmo di consenso basato sulla *Delegated Proof of Stake* (DPoS), in cui i validatori, persone o pool, hanno l'onore e l'ònere di inserire i blocchi nella blockchain. A differenza di Bitcoin, il profitto di chi inserisce i blocchi è quindi legato al valore di Luna messi in staking da parte sua, e non dipende solo da un evento estremamente randomico come il raggiungimento con una hash del target di '0' richiesti dalla proof of work; infatti, dal punto di vista dei miner il profitto è in un certo senso predicibile, quasi deterministico, e attira sia gli investimenti di grandi pool, che di singole persone che dal proprio investimento in Luna vogliono avere un ritorno sicuro e non legato al caso.

2.2 L'ambiente: Cosmos SDK

L'intera blockchain è collegata ad altre blockchain grazie all'ambiente su cui è stata implementata: Cosmos SDK. Questa è anche nota come "l'internet delle blockchain", in quanto fornisce un supporto stabile per tutte quelle blockchain che non vogliono essere un ecosistema autonomo, ma che vogliono interfacciarsi e comunicare con altre realtà.
Nella pratica, Terra sfrutta un sistema di verifica dei blocchi nativo di Cosmos: Tendermint. Questo garantisce una buona sicurezza nel processo di inserimento dei blocchi, dato che è resistente anche se 1/3 delle macchine coinvolte nel processo diventa difettosa o malevola.

Visualizzazione grafica IBC

2.3 Validatori

I validatori sono il cardine del sistema Terra; di per sè chiunque potrebbe diventarlo, ma è necessario essere in possesso di un gran numero di Luna (visto l'algoritmo basato sulla DPoS) o alternativamente far sì che molti si affidino al validatore in questione, per far fruttare i propri Luna.

2.3.1 Ranking dei validatori

Dunque essere validatori in Terra non è semplice e immediato: è necessario essere tra i "migliori" 130 candidati validatori per poter prendere parte alla dinamica del consenso. In Bitcoin, a livello teorico chi possiede un pc è alla stregua della mining pool più grande: stessi diritti, stesse possibilità di profitto (proporzionate alla potenza di calcolo).
In Terra, il sistema dà l'idea di essere più centralizzato, dato che i validatori sono gli unici che possono inserire i blocchi, verificare la correttezza delle transazioni, ma anche accettare i blocchi proposti da un altro validatore.
Il ranking dei validatori dipende dalla quantità totale di Luna in staking sul validatore stesso. Questi possono essere posseduti dal validatore stesso (Self-Bonding), oppure possono essere stati loro "affidati" da utenti comuni, che prendono il nome di delegators.

2.3.2 Delegators

I delegators concedono la loro potenza di mining al validatore, rimanendo comunque in possesso dei Luna in oggetto ed essendo liberi di scegliere a quale validatore affidarsi. Le due discriminanti principali per scegliere un validatore sono:

- La **commissione** che il validatore trattiene ai propri delegators.
- Il **ranking**, cioè la presenza affermata sulla rete di un validatore, misurabile nella quantità di Luna che esso ha in staking

2.4 Il meccanismo del consenso

L'inserimento dei blocchi è un processo deterministico. Ogni validatore possiede parte della mining power e la % sul totale rappresenta proprio la frequenza con la quale verrà scelto da Tendermint per inserire il prossimo blocco. Il validatore che è scelto per inserire il blocco (proposer), dopo aver inserito delle transazioni, sperabilmente corrette, invia il blocco alla rete. A questo punto si susseguono due round di votazioni tra i validatori, che possono portare a due scenari:

- Votazione **favorevole**: il proposer chiude il blocco e lo firma, inserendolo nella blockchain. Tutti i reward sono distribuiti
- Votazione **negativa** per due round: il blocco viene bocciato e si passa, deterministicamente, al turno del prossimo proposer

Il vantaggio di essere proposer è quello di ricevere un extra reward per ricompensare lo sforzo nel chiudere il blocco con transazioni corrette. Come evidenziato in precedenza, non è conveniente per un validatore inserire transazioni non buone, altrimenti se qualcuno se ne accorge, questo perde il diritto di inserire il blocco, lasciando sul piatto un guadagno che sarebbe andato non soltanto a lui, ma anche ai suoi delegators, rischiando quindi di perdere il loro staking, a beneficio di un altro validator affidabile.

2.5 Reward

I reward derivanti dalla chiusura dei blocchi sono il motivo trainante per i miners e per tutti quelli che decidono di mettere in staking i propri luna. Come in Ethereum, ogni transazione può rappresentare un semplice passaggio di criptomonete da un address all'altro, oppure la risoluzione di uno smart contract. Quindi serve ovviare al problema caratteristico di molte blockchain 2.0, cioè quello degli spam e dei contratti con loop infiniti, atti solamente a far collassare il sistema.
Come per ETH, più la transazione è lunga e complessa, più il gas da pagare per completarla sarà in quantità elevata; quindi sarebbe alquanto dispendioso attaccare la rete con spam di questo genere.
D'altra parte, i validatori possono decidere che nei loro blocchi possano entrare solamente transazioni con una fee (in **gas**) minima, in modo da ottimizzare lo spazio all'interno del

blocco e ottenere più reward.
Un altro tipo di introito per i miner è rappresentato dalle **swap fees**: tasse applicate su un particolare tipo di transazione, cioè gli scambi tra stablecoin o tra Terra e Luna. E' un tipo di costo da pagare che è presente quando si fa trading anche sulla Borsa Azionaria, cioè la differenza tra Bid e Ask price, ossia tra quanto si riceve vendendo un'azione e quanto si deve pagare per ottenere quella stessa azione.
La prima è detta **Tobin Tax** e può variare a seconda delle stablecoin tra cui un utente sta "swappando"; In media vale 0.35% della transazione, ma può avere picchi anche del 2%.
La seconda è la cosiddetta **Spread Fee**, che ha solo un valore minimo dello 0.5%, ma che in periodi di grande volatilità cresce per mantenere in equilibrio Terra e Luna.
Le swap fees, tuttavia, non vanno direttamente ai validatori e ai loro delegators, bensì vengono assegnate alla Oracle Reward Pool, una riserva di Terra che viene utilizzata per remunerare i validators quando si trovano a votare per il valore dei tassi di cambio reali da applicare alle transazioni all'interno della blockchain. I più onesti, ricevono un compenso proprio da questa pool, mentre quelli che cercano di deviare il tasso di cambio reale vengono puniti.
Fino all'inizio del 2022, veniva applicata anche una "Stability fee" a tutte le transazioni di Terra, variabile da 0.1% ad 1%, con un tetto massimo di 1 SDT. Quest' ultima andava di diritto ai validatori, sempre proporzionalmente alla loro quantità di Luna in staking, ma è stata eliminata, a maggioranza schiacciante (99% sì), in seguito alla Proposal 172.

2.5.1 Schema dei reward

Un semplice esempio può spiegare meglio il funzionamento dei reward. Se un blocco ha come provvigione 1000 SDT e sono presenti 10 validatori, ogni validatore ha diritto a 100 SDT. Data una commissione applicata dal validatore dell'1% e dati 20% self-bonded, cioè di proprietà del validatore stesso, i reward saranno così distribuiti:

- Commissione: 100 SDT*80%*1% = 0.8 SDT
- Ogni validatore riceve: 100 SDT*20% + Commissione = 20.8 SDT
- L'insieme dei delegators riceve: 100 SDT*80% - Commissione = 79.2 SDT

2.6 Fasi Lunari

Tre sono le fasi in cui può trovarsi Luna:

- **Unbonded**: la fase di libertà del token, in cui è molto liquido e può essere scambiato su qualsiasi exchange per altri token o criptomonete. E' una fase poco conveniente per un investitore, e solitamente non dura per molto tempo. Giusto il tempo di capire in quale parte dell'universo Terra "legare" i propri Luna per farli fruttare.
- **Bonded**: la fase in cui il token perde il suo nome originario in seguito ad uno staking su un validator, diventando bLuna, un token sempre commerciabile liberamente. Può essere usato anche come collaterale in certe operazioni su Terra, legate ad esempio ai due protocolli più famosi: Anchor e Mirror.
- **Unbonding**: è una fase di transizione in cui un utente decide di slegarsi da un validatore, per rivendere i suoi Luna o farne un uso diverso. Questa operazione dura 21 giorni e permette al sistema Terra di essere più stabile a lungo termine, non consentendo movimenti improvvisi ed enormi di token. L'unico modo per fermare questo processo è operare una redelegation, cioè decidere di mettere in stake nuovamente i Luna, ma su un validatore diverso da quello precedente.

2.7 Slashing

Il sistema Terra prevede anche delle punizioni (dall'inglese "slash", tagliare) per chi non si comporta correttamente. Ci riferiamo principalmente ai validatori che, come già detto, portano sulle spalle il peso di tutto il progetto e indirizzano pesantemente le scelte di tutta la community, come vedremo nella parte dedicata alla governance. Questi hanno perciò un codice "etico" da rispettare, pena la diminuzione della loro potenza di mining, e di quella dei loro delegators. Alcune pene comprendono anche l'esclusione dal protocollo di consenso, il cosiddetto "jailing".
Una peculiarità è che non esistono delle forze dell'ordine che controllano i validatori, ma sono i validatori stessi che si denunciano tra di loro, per loro interesse individuale, ma anche per mantenere alto il livello del progetto e di chi lo dovrebbe sostenere in prima persona. Alcuni controlli, vengono invece affidati al software della blockchain, che all'inizio di un blocco, verifica che tutti i validators siano in regola con certi parametri.

2.7.1 Cosa causa uno slashing?

Esistono principalmente 5 modi di infrangere le regole:

- **Double Signing**: operazione in cui un miner firma un blocco alla stessa altezza su due catene parallele con un antenato in comune, presumibilmente per effettuare operazioni di double spending .
- **Downtime**: accade quando un validator scompare per un certo periodo di tempo, mostrando disinteresse per il progetto.
- **Unavaliability**: il validatore non firma blocchi per N volte consecutive e riceve una penalità proporzionale ad N. Se N è maggiore di una certa soglia, allora il validatore perde tutti i Luna in staking su di lui, cioè viene "unbonded".
- **Missed Votes**: letteralmente "voti mancanti", quelli relativi alle proposte della governance e quelli relativi agli oracoli che forniscono i tassi di cambio alla blockchain.
- **Wrong votes**: il validatore vota per un oracolo, affermando che un tale tasso di cambio è almeno una deviazione standard più lontano rispetto alla mediana degli altri validatori.

2.8 Governance

La governance di Terra è il processo democratico che permette a Terra di cambiare i propri standard ed i propri protocolli, senza che sia un'autorità centrale a proporre il suddetto cambio. Ogni proposta viene messa quindi ai voti e se supera un certo scoglio di voti, viene accettata da tutta la rete e diventa una "legge" immutabile nella blockchain Terra.
Chiunque può fare delle "proposals" e può proporre di fatto qualunque cosa, a suo rischio e pericolo: infatti, per evitare spam, Terra prevede che chi "drafta" una proposta debba anche allegare un deposito di 50 Luna per renderla valida. Questa quantità di moneta non verrà rimborsata nel caso la proposta venga etichettata come spam.
La procedura di voto è intuitiva: tutti votano ed ogni bLuna in staking equivale ad un voto. I voti possibili sono: sì, no, no con veto, astenuto. Affinchè una votazione sia valida va raggiunto un quorum del 40% dei votanti e di questi il 50% deve aver votato sì. Altrimenti la votazione fallisce e il deposito messo a collaterale viene restituito ai legittimi proprietari. Può succedere anche, come preannunciato, che un proposer veda i suoi Luna svanire se almeno 1/3 dei votanti si è espresso con un no con veto.

3 Funzionamento stablecoin

3.1 Stablecoin (dualità UST-Luna)

Una delle caratteristiche principali di Terra è l'utilizzo di diverse stablecoin, ciascuna ancorata a una delle valute fiat principali. Questa scelta è stata fatta perché, nonostante il dollaro statunitense domini il commercio internazionale, per alcuni utenti risulta troppo volatile rispetto alla loro unità scelta di conto. A seconda della valuta fiat a cui sono ancorate, le stablecoin di Terra prendono nomi differenti: TerraUSD (UST), TerraCNY, TerraJPY, TerraGBP, TerraKRW, TerraEUR sono le stablecoin ancorate rispettivamente al dollaro americano, allo yuan cinese, allo yen giapponese, alla sterlina britannica, al vinto sudcoreano e all'euro. La stablecoin con minore volatilità utilizzata su Terra è TerraSDR, ancorata all'unità di conto del Fondo Monetario Internazionale. Le criptovalute di Terra sono stablecoin algoritmiche e il rapporto tra queste e i token Luna è l'aspetto fondamentale che rende possibile il funzionamento dell'intero protocollo. Per mantenere il valore delle stablecoin ancorato al valore della valuta che tracciano, vengono sfruttate le forze di mercato della domanda e dell'offerta.

In questo paper, per capire il meccanismo che sta alla base del protocollo, prenderemo come stablecoin di riferimento UST. Si può immaginare l'intero ecosistema Terra come composto da due pool di liquidità: uno contenente UST e l'altro contenente Luna. Il livello di liquidità contenuto in ciascuno dei due pool varia in base all'andamento del rapporto domanda-offerta della stablecoin. In particolare, la liquidità contenuta nel pool Luna viene utilizzata per aumentare o diminuire il livello di liquidità nel pool UST, quindi per mantenere il valore di UST ancorato al valore del dollaro americano. Il meccanismo può essere suddiviso in due fasi:

- **Fase di espansione**: si verifica quando il prezzo di UST è più alto del peg, ciò significa che la domanda è elevata rispetto all'offerta ridotta. In questo caso, il protocollo incentiva gli utenti a bruciare Luna e coniare UST. Per ogni dollaro di Luna bruciato, ne viene coniato uno di Terra. Così facendo, la liquidità del pool Terra aumenta a discapito della liquidità del pool Luna che diminuisce, cioè vengono coniati nuovi UST dai Luna bruciati affinchè UST raggiunga il valore target del proprio peg. Al termine del processo, Luna aumenta di valore in quanto vi è minore disponibilità.
- **Fase di contrazione**: si verifica quando il prezzo di UST è più basso del peg, ciò significa che la domanda è ridotta rispetto all'offerta elevata. Il procedimento sarà quindi l'opposto del caso precedente, infatti gli utenti sono incentivati a bruciare UST e coniare Luna. Così facendo, la liquidità del pool Luna aumenta a discapito della liquidità del pool Terra che diminuisce, di conseguenza il valore di Luna diminuisce. Riducendo il numero di UST, il prezzo aumenta fino al raggiungimento del valore del peg.

Luna è la controparte variabile delle stablecoin di Terra, risulta quindi indispensabile per il funzionamento del protocollo.

3.2 Mantenimento del PEG

Per rendere possibile la creazione di token che tracciano il prezzo delle controparti in FIAT in maniera completamente decentralizzata, denominate stablecoin algoritmiche, ci si avvale principalmente di due meccanismi: l'arbitraggio ed il signoraggio.

3.2.1 Signoraggio

Il signoraggio oggi come in passato viene largamente utilizzato dagli stati e dalle banche centrali per emettere nuova moneta, grazie al quale è possibile generare ricchezza per chi si avvale di questo diritto. E' un meccanismo tramite il quale è possibile coniare nuova

moneta controgarantita da un sottostante; ad esempio fino al 1971 prima che il presidente americano Richard Nixon decretasse la fine della parità monetaria, il valore del dollaro era sostenuto dall'oro, o meglio dalla riserva aurea.
Oggi la stampa di nuova moneta viene garantita dai titoli di stato che vengono acquistati dalle banche centrali vendendo di fatto la moneta appena creata allo stesso, generando debito pubblico per lo stato ed un flusso di denaro continuo in entrata per la banca centrale.
Lo stesso meccanismo viene sfruttato dal mondo Terra per coniare nuovi token ancorati al valore di una valuta FIAT: si utilizza come sottostante il token nativo della blockchain Terra, Luna, per coniare nuove stablecoin.
Il token Luna viene incassato come guadagno derivante dal signoraggio che in parte viene ridistribuito tra la community e la oracle rewards pool ed in parte distrutto; questo è ciò che accadeva fino all'introduzione dell'aggiornamento Columbus-5, che oggi consente di distruggere tutto il ricavato diminuendo di fatto la supply del token Luna ma sortendo un effetto positivo sul valore della coin.

3.2.2 Arbitraggio

Per rendere possibile da parte delle stablecoin di replicare fedelmente il prezzo delle valute FIAT a cui sono ancorate si sfrutta l'arbitraggio, che può essere eseguito o da un trader oppure da un protocollo decentralizzato. Tale operazione è priva di rischio in quanto consente di ottenere un profitto certo per chi la effettua; principalmente si può effettuare l'arbitraggio tra le varie stablecoin oppure tra una stablecoin ed il token Luna.
Il protocollo di Terra utilizza come valore di riferimento per calcolare constantemente gli esatti spread tra le diverse stablecoin del mondo Terra una speciale valuta, replicata dal token terraSDR e ideata dal FMI (Fondo Monetario Internazionale); essa viene calcolata su un paniere di valute e utilizzata come riferimento di scambio internazionale in sostituzione all'oro.
Grazie a ciò è possibile eseguire facili operazioni di arbitraggio fra più stablecoin tramite delle velocissime operazioni di atomic swap in grado di far assorbire in modo più rapido eventuali oscillazioni di mercato di una o più stablecoin ancorate alla valuta tradizionale o ad altre valute.
Facciamo un esempio concreto: se 1 TerraUST = 0.99 USD si può scambiare per 1 USD di valore di Luna su market swap, funzionalità offerta dal wallet terra station, quindi di fatto effettuando l'operazione di mint di 1 token Luna e contestualmente il burning di 1 token UST, per poi rivenderlo a mercato guadagnando lo spread; viceversa se 1 TerraUST = 1.01 si può scambiare 1 USD di valore di Luna su market swap per ottener 1 TerraUST da rivendere a mercato ed incassare lo spread.
Questo meccanismo va avanti finche non si raggiunge la parità con la valuta FIAT di riferimento che in questo esempio è il dollaro.

3.2.3 Elastic money supply

Dall'unione di questi due meccanismi ne consegue la stretta connessione tra il token Luna e tutte le stablecoin dell'ecosistema Terra. Le stablecoin create non sono altro che dei token che in linea teorica dovrebbero mimare il prezzo della controparte in FIAT; per fare ciò è di fondamentale importanza conoscere costantemente il valore della valuta in questione, ma questo essendo un dato off chain, ovvero un dato reale esogeno alla blockchain, si necessita dell'utilizzo di oracoli decentralizzati in modo da ricevere con continuità il giusto feedback di prezzo on chain. In questo modo è possibile controllare l'uguaglianza di prezzo tra la valuta di riferimento ed il token creato.
Questo principio è estendibile a qualsiasi asset del mondo Terra, ad esempio una commodity, una stock o un'altra crypto.
Infatti se il valore della stablecoin dovesse risultare superiore al prezzo corrente della valuta di riferimento, il protocollo interverrebbe creando nuovi token della stablecoin aumentandone la supply totale e bruciando il token Luna diminuendo la supply di quest'ul-

tima riportando verso il basso il prezzo; viceversa se il prezzo dovesse risultare inferiore al feedback dell'oracolo si distruggerebbe i token della stablecoin riducendone la supply e creando nuovi luna aumentandone la supply riportando verso l'alto il prezzo.
Dunque è evidente come il token Luna sia di fondamentale importanza per la sopravvivenza dell'ecosistema e di come assorba le fluttuazioni di mercato (volatilità) in favore della stabilità delle stablecoin.

3.3 Mass adoption

Al fine di far acquisire una certa posizione di dominanza all'interno del mercato alla principale stablecoin dell'ecosistema Terra, é fondamentale creare degli use cases per incentivarne l'utilizzo e la detenzione, ovvero incrementare la cosidetta mass adoption.
Perció é di vitale importanza che una grossa quantitá di protocolli DeFi renda disponibile la fruizione dei loro servizi anche tramite la stablecoin UST, per incentivare l'utente a scambiare parte delle proprie stablecoin in UST al fine di incrementare la domanda su quest'ultima. Ma al coltempo, se non ci sono molti utenti che utilizzano UST come valuta, molti protocolli decentralizzati non saranno incentivati ad utilizzarla nei servizi offerti.
Per ovviare a questo problema la blockchain di Terra ha a disposizione una Treasury gestita da una DAO in grado di finanziare i progetti piú promettenti che rispettano rigidi requisiti. Questo ha come scopo ultimo attirare team di sviluppatori con grande esperienza in campo smart contracts e DeFi per creare e lanciare nuovi protocolli decentralizzati in grado di fornire svariati servizi finanziari utilizzando come coin di riferimento UST, alcuni di essi sono Anchor Protocol, Mirror Protocol e TerraSwap che vedremo piú in dettaglio nel prossimo capitolo.
Questo ha permesso ad UST di raggiungere una certa massa critica sia di utilizzatori che di Market Cap e di conseguenza ha facilitato le trattative da parte delle aziende dietro a TerraLuna, la Terra Form Labs e la Luna Foundation Guard, per far si che i loro token, in particolare Luna ed UST, potessero andare sia crosschain, quindi ad esempio essere utilizzati dai piú famosi protocolli DeFi come Curve finance su blockchain Ethereum o da TraderJoe su blockchain Avalanche(sidechain di Ethereum), sia scambiati nei piú grossi exchange al mondo come FTX o Binance.
Questo, come si evince dal grafico sotto, ha permesso ad UST (banda blu) di aumentare notevolmente la propria supply.

4 DeFi

Il network Terra è strettamente legato al concetto di DeFi; oltre ad accogliere denaro sotto forma di criptovalute depositate in smart contract dagli utenti, ripagandoli dando interessi variabili nella loro criptovaluta nativa, vengono sviluppati molti altri progetti, quali piattaforme di prestiti, beneficenza, assicurazioni e scommesse, fornendo un ecosistema completo per la finanza decentralizzata, offrendo tutto quanto siamo abituati a vedere nelle banche classiche.
Infatti Terra oggi fornisce i tre primitivi del mondo finanziario: possibilità di pagamento, possibilità di investimento (e scambio di titoli) e accantonamento risparmi.

4.1 Sistema di pagamenti

L'aspetto di base del sistema Terra (LUNA) è network di pagamenti, che è già molto popolare attraverso l'App CHAI in Corea del Sud e MemePay in Mongolia. Il sistema è diffuso ubiquamente, viene accettato da moltissimi shop online e muove già circa 1 miliardo di dollari ogni anno. Gli utenti attivi sono oltre 2 milioni, per un progetto che è in fortissima espansione. In questo caso Terra si comporta da intermediario decentralizzato, che permette di spostare le stablecoin da un wallet all'altro.
Grazie a questa offerta, è evidente come l'ecosistema Terra si stia preparando all'adozione di massa della tecnologia blockchain in pagamenti e scambio di capitali.
Il case study più interessante è quello della Corea del Sud; questo paese ha costruito il suo benessere su uno sviluppo tecnologico di stampo futuristico, perciò le compravendite elettroniche trovano un terreno molto fertile. La piattaforma di pagamento Chai (fondata da Daniel Shin, uno dei due creatori di Terraform Labs) è partner di Terra e fa ampio uso di TerraKRT, stablecoin peggata al valore della valuta locale, il Won. Numerosi rivenditori, negozianti e commercianti accettano questa forma di pagamento, inclusa Nike Corea; questo è la dimostrazione di come la blockchain potrebbe muovere i capitali in un futuro non così lontano, e in questo ambito Terra si pone come punto di riferimento.
Infine proprio con l'obiettivo principale di favorire e facilitare un punto di incontro tra chi paga e chi deve essere pagato (consumatori e creatori, investitori e imprenditori, debitori e creditori...) è stato sviluppato Pylon protocol, una piattaforma che propone diversi servizi di pagamenti DeFi e prodotti di risparmio.

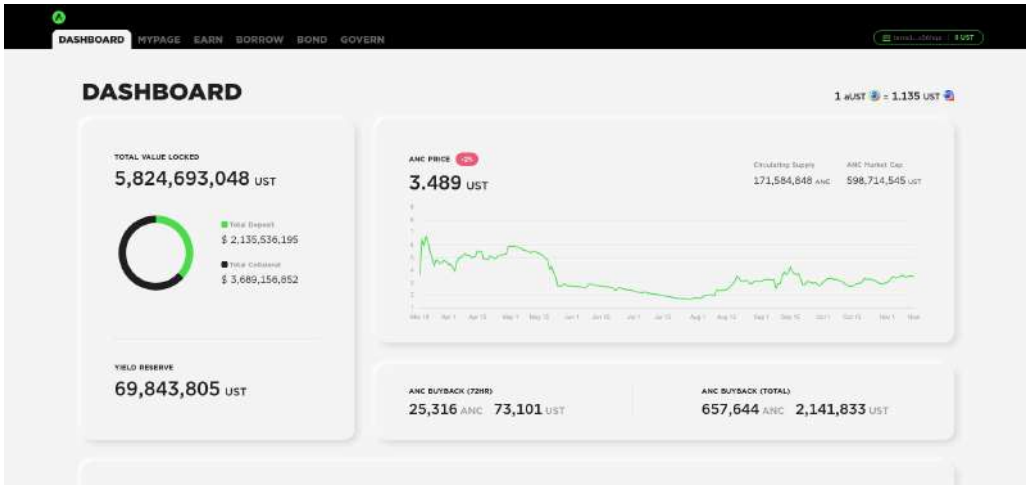
4.2 Indice TVL

Il valore totale bloccato (in inglese Total Value Locked), è un importante indicatore utilizzato per misurare e monitorare il valore complessivo del mercato DeFi, cresciuto esponenzialmente nell'ultimo anno, a tal punto da essere considerato quasi al pari della capitalizzazione di mercato. In pratica rappresenta il valore detenuto da una piattaforma DeFi all'interno dei suoi smart contract, ovvero la somma di tutti i fondi presenti su di essa in termini di indebitamento, concessione del credito e capacità di transazione; fornisce dunque una misura del successo di un'app DeFi nell'attirare l'interesse di utenti attivi nelle transazioni.
La particolarità e utilità di questo indicatore sta nel fatto che sia specifica per i progetti DeFi, diversamente dalla capitalizzazione di mercato, applicabile a quasiasi piattaforma blockchain avente il proprio token.
Inoltre esiste il rapporto TVL, ovvero quella tra la capitalizzazione di mercato di una piattaforma ed il suo TVL; un valore basso indica la sottovalutazione del progetto, che dunque potrebbe avere un buon potenziale di crescita futura. Infatti il TVL è un ottimo indicatore delle prestazioni attuali, mentre la capitalizzazione è una misura più orientata alle prospettive future.

Crescita TVL sulla blockchain Terra

4.3 Anchor

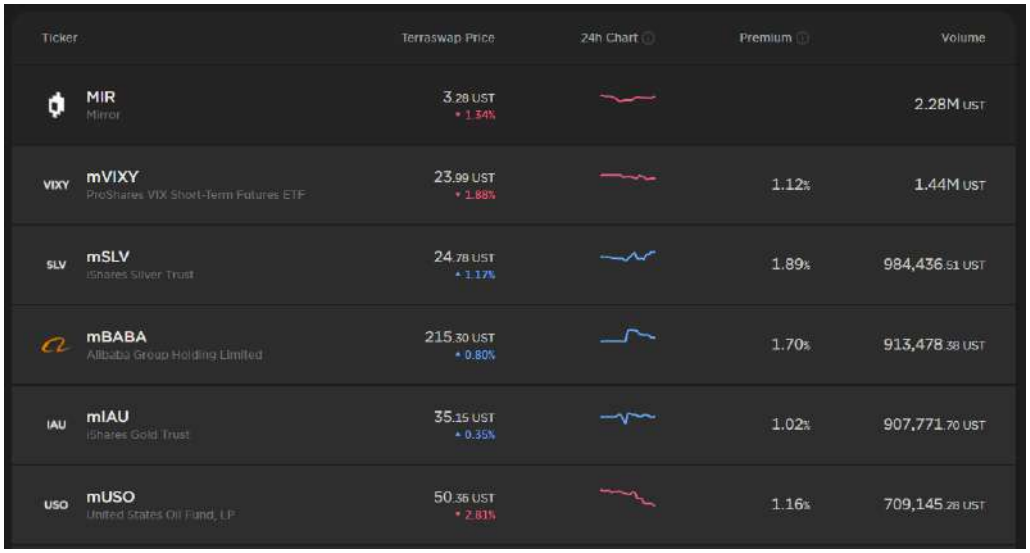
Il principale protocollo della chain Terra è Anchor Protocol, come dimostrato anche dal suo enorme TVL di circa 17 miliardi di dollari.
Esso offre ai suoi utenti la possibilità di prendere in prestito UST pagando un certo tasso di interesse mettendo semplicemente a collaterale altri asset come Luna, Eth o più recentemente anche Atom, Sol e Avax. La particolaritá di tutti questi crypto assets é il fatto di generare un certo interesse nel tempo grazie alla possibilitá di poter essere messi in staking sulle varie chain di appartenenza; il protocollo sfrutta tale caratteristica facendo convertire all'utente l'asset in questione nella versione bond, quindi bEth, bLuna, bSol, bAtom e wasAvax, in modo tale che l'utente rinuncia alla reward derivante dallo staking in favore di un tasso di interesse del prestito piú vantaggioso, facendo guadagnare tali rewards al protocollo, che li incassa come profitti destinandoli poi alla yield reserve.
Inoltre é possibile semplicemente depositare i propri UST mettendoli di fatto a disposizione di chi vuole prenderli in prestito guadagnando una percentuale di interesse stabile nel tempo di circa il 20%. Tale percentuale di interesse deriva dalla percentuale di interesse pagata dal borrower e dalle rewards dei collaterali nella loro versione bond. Inoltre la stabilitá del tasso di interesse é garantita dalla yield reserve che funge da cuscinetto di liquiditá per sopperire ai periodi in cui il protocollo genera meno profitti, in genere quando le quotazioni di mercato dei vari asset sono basse e gli utenti riducono i propri UST presi in prestito per evitare il rischio di liquidazione.
Il successo di Anchor Protocol deriva proprio dal fatto che offre un tasso di interesse stabile nel tempo sulla stable terraUSD, caratteristica non scontata in ambito DeFi in quanto solitamente i rendimenti offerti sui vari crypto assets, anche se piú alti, sono molto variabili ed esposti anche alla volatilitá della crypto messa a rendita ed in alcuni casi anche ad impermanent loss, mentre i rendimenti sulle stablecoin, oltre che variabili, sono anche inferiori al tasso di interesse offerto da Anchor.



Esempio di interfaccia Anchor

4.4 Mirror

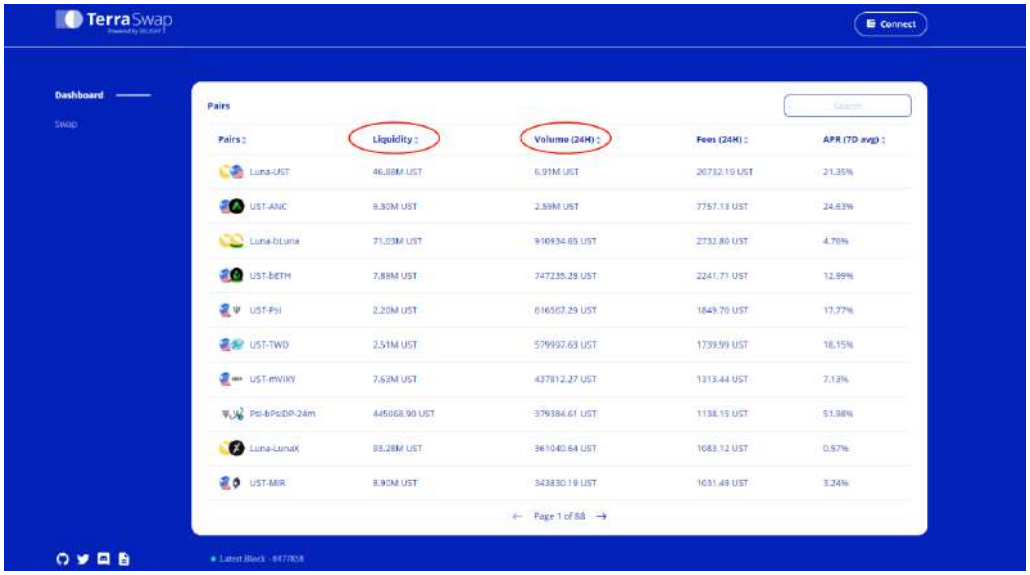
Mirror è il protocollo della chain Terra dedicato alla compravendita di asset sintetici che replicano il prezzo di altre crypto, commodities e principalmente stocks di grandi compagnie internazionali; sfogliando gli asset proposti si trovano infatti nomi come Amazon, Apple e Coca-Cola.
Il principio che c'è dietro è identico ai derivati tradizionali: si acquista qualcosa (nel nostro caso un token) che ha l'esatto valore del suo sottostante (ad esempio le azioni di Facebook). Così facendo si ha la possibilità di comprare e vendere sui mercati senza ricorrere a intermediari e conti appositi, cosa non banale se pensiamo che molti utenti nel mondo per vari motivi non hanno la possibilita di aprire un conto su un broker che permetta di fare tali operazioni.
Il sistema Mirror è stato una delle prime aggiunte al network ed è stato sviluppato dalla stessa casa madre che si occupa di gestire la blockchain Terra; esso permette di creare degli asset tokenizzati che rappresentano il valore di un asset finanziario esterno alla blockchain.
In particolare il protocollo offre la possibilitá di acquistare l'asset desiderato nella sezione trade tramite altri asset oppure di aprire delle posizioni short su tali assets andando a prenderne in prestito la quantitá desiderata e vendendola a mercato.
Per effettuare tale operazione peró é necessario fornire un collaterale a garanzia del prestito non inferiore ad un certa soglia percentuale di copertura, in genere il 150%. Tale tasso é strettamente legato alla volatilitá dell'asset che é deciso tramite il sistema di governance per i possessori del token nativo del protocollo, il token Mir.
All'interno del network Terra è possibile anche scambiarsi questi token, permettendo almeno in via teorica la creazione di un mercato di derivati molto efficiente e con costi di transazione estremamente più bassi rispetto ai broker OTC (Over The Counter). Questo aspetto è uno dei più interessanti del progetto Terra, anche se probabilmente nel futuro prossimo attirerà le attenzioni di alcuni regolatori, sopratutto se il volume di transazioni generato diventerá molto grande.



Esempio di interfaccia Mirror

4.5 TerraSwap e Astroport

TerraSwap è il primo scambio decentralizzato nativo (DEX) sull'ecosistema Terra, che consente agli utenti di scambiare risorse direttamente on chain.
Come molti scambi decentralizzati nello spazio crittografico, anche TerraSwap utilizza il modello Automated Market Maker (AMM) sperimentato da Uniswap; in pratica i pool calcolano i prezzi in base alla formula invariante del prodotto costante di X*Y = K. Essendo una delle prime applicazioni di DeFi sull'ecosistema Terra, ha rapidamente ottenuto il sostegno della comunità ed è diventata un hub di liquidità per l'ecosistema. Come la maggior parte dei DEX, TerraSwap addebita anche una commissione di base dello 0,3% per ogni operazione sulla piattaforma.
Un altro importante DEX nato da poco é Astroport, un market maker automatizzato di nuova generazione costruito sull'ecosistema Terra e considerato il successore di TerraSwap; è stato sviluppato da una joint venture di alcuni dei più grandi nomi della scena crittografica, dal gigante fintech Terraform Labs alla principale società di ricerca crittografica Delphi Digital.
La filosofia di progettazione alla base di Astroport è semplice: consentire liquidità decentralizzata e non detentiva e rilevamento dei prezzi per qualsiasi asset. Per raggiungere questo obiettivo, Astroport dà la priorità assoluta alla flessibilità, combinando vari tipi di pool specializzati e muovendosi agevolemente tra di essi.



Esempio di interfaccia TerraSWAP

5 Attacco a UST

L'8 maggio 2022 moriva uno dei protocolli piú ambiziosi ed innovativi mai creato nella breve storia della DeFi 2.0, TerraLuna.

5.1 Fattore scatenante

Tutto ha inizio con una grossa vendita di UST su Curve di 85 milioni di dollari, che ha causato un forte sbilanciamento del 3-pool facendo perdere momentaneamente il peg ad UST.
La notizia di quanto accaduto diffondendosi velocemente sul social Twitter ha contribuito ad alimentare la fud degli investitori che si sono precipitati a ritirare circa 2 miliardi di dollari da Anchor Protocol dando inizio ad una bank run ovvero una vera e propria corsa agli sportelli per prelevare liquiditá, portando il peg tra i 0,987 ed i 0,995; evento già verificatosi in passato sia durante la crisi finanziaria del 2008 causata dalla banca rotta della Lehman Brothers Holding e più recedente in Ucraina subito dopo lo scoppio della guerra da parte della Russia.

5.2 Tasselli mancanti

Prima di proseguire nella trattazione bisogna venire a conoscenza di alcuni tasselli di fondamentale importanza.

- La LFG(Luna Foundation Guard) tra marzo ed aprile acquistava bitcoin per collateralizzare in parte UST rendendo più stabile il peg della stablecoin.
- Successivamente avveniva l'annuncio che il pool su Curve contenente UST sarebbe passato da un 3-pool ad un 4-pool.
- L'attaccante preparandosi all'attacco prendeva in prestito circa 100.000 bitcoin dall'exchange Gemini, che di fatto per l'exchange equivale ad avere una vendita allo scoperto su Bitcoin; successivamente l'attaccante utilizzando i BTC presi in prestito ha effettuato un accordo OTC del valore di 1 miliardo di UST.

5.3 Inizio della fine

La LFG inizió a procedere rimuovendo 150 milioni di UST dal 3-pool Curve in preparazione al passaggio del 4-pool, l'attaccante ha sfruttato tale momento per poter vendere 350 milioni di UST su Curve di fatto prosciugandone letteralmente il pool di liquiditá.
Questo ha portato ad avere un prezzo per UST su Curve prossimo allo zero innescando un meccanismo di arbitraggio tra Curve ed altri DEX ed Exchange riducendo ulteriormente il prezzo a mercato di UST portandolo tra i 0,97 ed i 0,98 centesimi di dollaro.
Così facendo si é innescata nuovamente una bank run da Anchor facendo scendere il valore depositato sul protocollo, di circa 14 miliardi di dollari, ad un ritmo di 10 milioni di dollari al minuto.
Quindi il valore di UST oscillava intorno ai 0,97$ portando un panico generale tra gli investitori.
Inoltre i principali indici azionari stavano crollando in particolare il NASDAQ che essendo fortemente correlato ai mercati crypto ha portato le quotazioni di Bitcoin e di altre altcoin tra cui LUNA verso il basso.
A questo punto all'attaccante per concludere l'attacco non rimaneva che vendere i restanti 650 milioni di dollari su Binance, principale exchange per la compravendita spot e di derivati crypto, questo ha contribuito ulteriormente a far abbassare notevolmente il valore di UST a circa 0,70$.
La LFG é intervenuta vendendo BTC per acquistare UST cercando di far recuperare il peg ma non ha fatto altro che aumentare la pressione di vendita su BTC e di conseguenza facendo svalutare la parziale collateralizzazione di UST.

Inoltre considerando il modo in cui funziona il protocollo di Terra, l'evento di depeg ha portato ad un elevatissima diluizione del token Luna facendo vedere ai suoi holder una svalutazione del proprio investimento e di conseguenza portandoli a vendere facendo calare ancor di più il valore di Luna per singolo token e di conseguenza a non avere sufficiente liquiditá in token Luna per far assorbire l'enorme distruzione di UST.
Il susseguirsi di tutti questi eventi, sicuramente ben pianificati, ha portato l'ecosistema in una spirale da cui non è tuttora riuscito ad uscire, facendo di fatto collassare sia il prezzo di Luna che di UST.

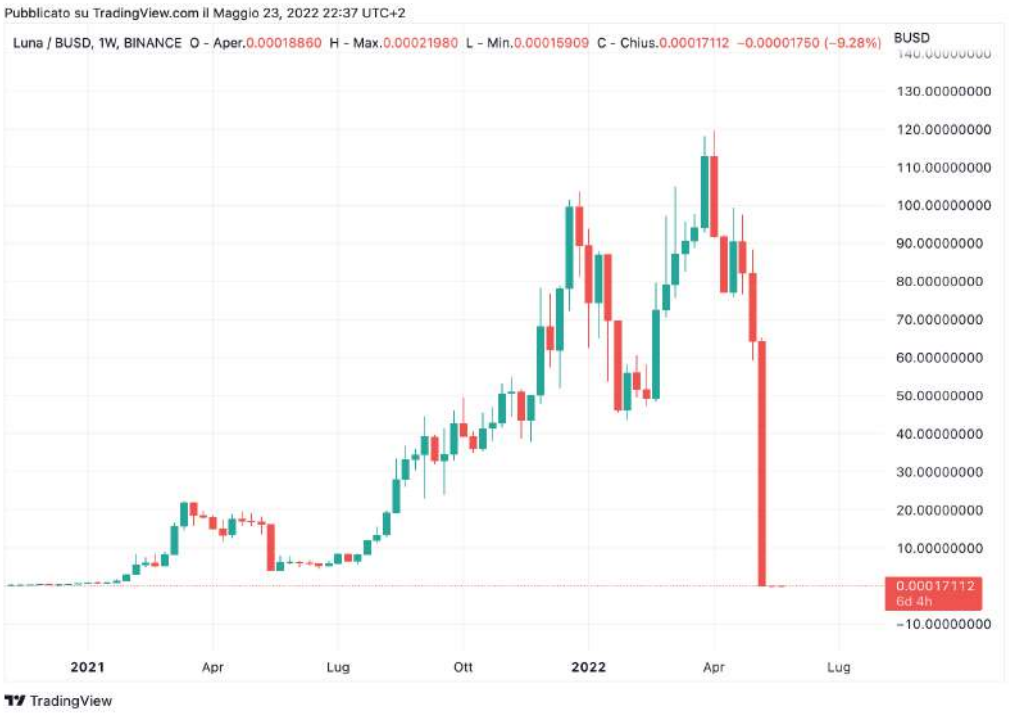


Grafico LUNA/BUSD settimanale

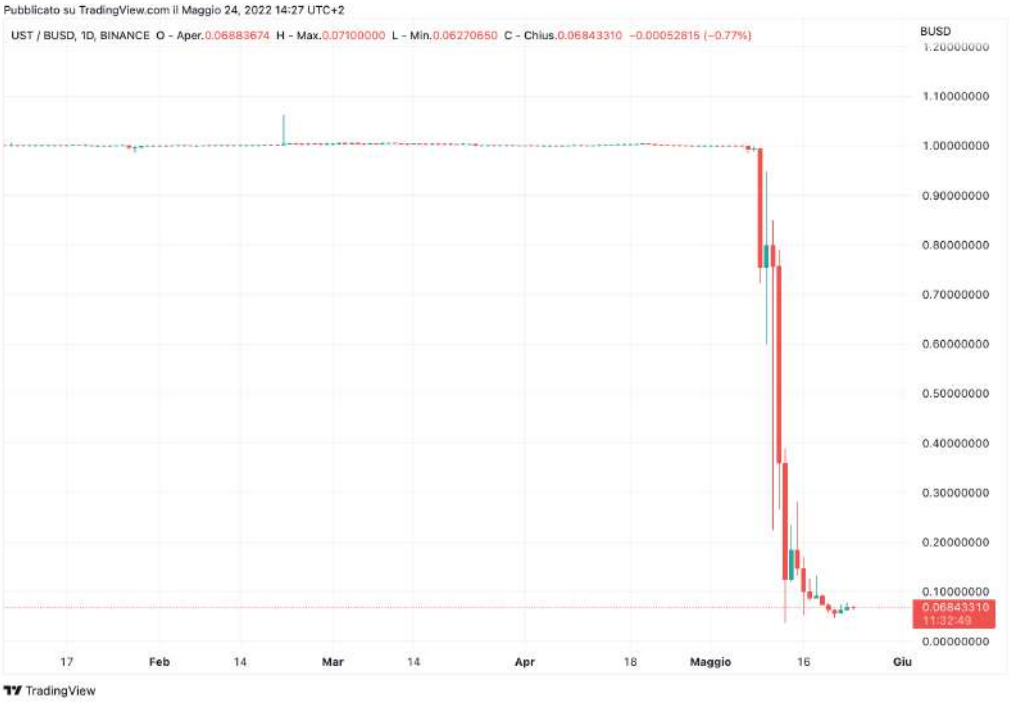


Grafico UST/BUSD giornaliero

6 Conclusioni

Il mondo delle crypto grazie a Bitcoin prima ed Ethereum dopo che ha dato il via alla creazione di token ERC20 ed all'esecuzione di smart contracts é in continua espansione e vive ogni giorno profondi mutamenti sociali e tecnologici.
In questo periodo abbiamo visto la nascita della DeFi 2.0 susseditrice della DeFi nata nei primi mesi del 2019, caratterizzata da protocolli innovativi ad esempio come dei venture capital decentralizzati (vedi Wonderland progetto dell'italiano Daniele Sesta), protocolli di bribes (vedi Curve Wars e Convex) alle stablecoin decentralizzate come MIM(Magin Internet Money), FRAX o appunto UST.
Alla luce di quanto successo siamo ben distanti dall'avere una stablecoin decentralizzata stabile e sicura, ma questo non deve scoraggiare l'innovazione e tutto il processo di sperimentazione perché senza fallimento non c'é successo. Da quanto successo bisogna prendere ció che é stato fatto di buono e valutare meglio tutti quei progetti che ancora stanno reggendo come ad esempio MIM la stablecoin di abracadabra sovracollateralizzata da interesting bearing token che nonostante lo scandalo legato a Wonderland ed il suo Treasury manager con lo pseudonimo su Twitter di 0xSifu ha retto egregiamente il colpo, oppure la stessa FRAX che nonostante non mantenga costantemente il peg sembra un progetto promettente.
Agli occhi dei meno esperti una stable coin decentralizzata potrá sembrare superflua e rischiosa data la vasta offerta di altre tipologie piú sicure, ma se si vuole operare in un contesto totalmente trustless é necessaria.

7 Sitografia

- https://www.criptovaluta.it/terra-luna
- https://www.criptovaluta.it/28491/terra-luna-finanziera-la-defi-139-milioni-di-dollari-per-5-progetti
- https://portalcripto.com.br/it/cos%27%C3%A8-la-definizione-dell%27indicatore-tvl%3F/
- https://docs.terra.money/docs/develop/dapp/smart-contracts/README.html
- https://chaindebrief.com/astroport-vs-terraswap-yield-terra/
- https://docs.terra.money/docs/learn/protocol.html
- https://entrepreneurshandbook.co/luna-brothers-inc-712ec5abe199
- https://www.criptovaluta.it/stable-coin
- https://assets.website-files.com/611153e7af981472d8da199c/618b02d13e938ae1f8ad1e45_Terra_White_pap

BLOCKCHAIN E METAVERSO

Leonardo Barale, Federica Lorenzo, Matteo Montrucchio, Lorenzo Tamietti

1 Introduzione, storia e futuro

1.1 Che cos'è il Metaverso?

Ad oggi il Metaverso non ha una vera e propria definizione universale, cioè considerata da tutti come tale, bensì ne esistono diverse interpretazioni e visioni.

- L'interpretazione più futuristica vede il Metaverso come l'internet del futuro: non più una rete di pagine web, ma di luoghi immersivi. Quindi si pensa ad esso come ad un insieme di mondi dove muoversi virtualmente, lasciando segni inalterabili (ad esempio se si taglia un albero, non sarà possibile ricrearlo) e interfacciandosi con altri fruitori. Questa visione ha però dei limiti: costruire un'infrastruttura del genere richiede uno sforzo enorme in termini di investimenti e di lavoro di aziende specializzate.

- Un'altra interpretazione vede il Metaverso come una forma di realtà aumentata. Questa visione prevede non una realtà digitale "alternativa" a quella reale, ma un'integrazione fra le due.

- L'ultima interpretazione è anche, ad oggi, la più diffusa e accreditata, e descrive il Metaverso come una realtà virtuale: una sorta di grande videogioco dove sperimentare esperienze immersive.

Seguendo quest'ultima idea si può immaginare il Metaverso come un grande mondo virtuale in cui ci si immerge e si compie qualsiasi attività. Quindi ci saranno le città, le strade, i negozi, le case... Si potrà andare al cinema, a fare una passeggiata, alle feste, stare con gli amici. O anche seguire una riunione con i colleghi, fare shopping come se si fosse al supermercato, frequentare un corso. Si potranno anche comprare oggetti virtuali sfruttando la tecnologia delle Blockchain o gli Nft per sbloccare contenuti in esclusiva. Entrare nel Metaverso sarà come vivere una seconda vita, grazie ai propri avatar.

1.2 Un po' di storia

Il concetto di Metaverso (pensato come nella terza interpretazione riportata nella sezione precedente) ha origine nel lontano 1838, anno in cui uno scienziato britannico di nome Charles Wheatstone diede vita al concetto di visione binoculare. Secondo Wheatstone, su ogni occhio si potevano combinare due immagini per dar

vita a una loro copia in 3D. A seguito della scoperta di questo concetto scientifico, iniziò lo sviluppo di strumenti come gli stereoscopi, il cui meccanismo è esattamente paragonabile ai visori VR moderni. Questi ultimi consentono infatti di riprodurre un'immagine 3D in maniera molto realistica grazie alle loro tecnologie avanzate.
Per quanto riguarda l'utilizzo dei termini "meta" e "verso" insieme, invece, bisogna fare un salto di quasi cento anni, arrivando al 1982. Nel romanzo cyberpunk "Snow Crash", lo scrittore Neil Town Stevenson menzionò il Metaverso, parlandone come uno spazio virtuale tridimensionale all'interno del quale gli individui si rifugiano per sfuggire alla propria realtà. Col passare degli anni, il significato di Metaverso ha preso sempre più forma, passando dall'utilizzo di visori VR per i videogiochi, alla nascita degli NFT.
Una tappa fondamentale, che ha fatto esplodere il mercato dei metaversi già esistenti e ha portato questo concetto sulla bocca di tutti, è avvenuta il **28 ottobre 2021**. In questa data Mark Zuckerberg ha annunciato il cambio di nome di Facebook in Meta e contestualmente ha lanciato il Metaverso.

1.3 Metaversi Blockchain e non Blockchain

Metaverso e blockchain non sono nati insieme. Anzi, la blockchain è nata con obiettivi totalmente differenti e soltanto in un secondo momento si è aperta ai servizi, quelli che consentono di utilizzare i suoi principali elementi costitutivi per dare vita a nuovi modelli di business.
Il metaverso si può contraddistinguere in molte versioni e, di conseguenza, sono altrettante le manifestazioni tecnologiche, che spaziano dagli ecosistemi multiplayer fino ai social VR. Quindi questa varietà produce molte esperienze differenti, contraddistinte peraltro da un'ampia forbice per quanto riguarda la maturità tecnologica delle soluzioni. Perciò attualmente, tra le tecnologie considerate parte dei metaversi, ne esistono solo alcune che già utilizzano le blockchain, mentre altre sono indipendenti da esse.

1.3.1 Metaversi senza Blockchain

- **Second Life**: nato nel 2003, è un famoso esempio di "life simulator", ovvero di mondo virtuale in 3D del tutto alternativo rispetto al mondo reale, dove è possibile costruire la propria sede, la propria casa, vestire i propri avatar e tutto ciò che è necessario per garantire le interazioni sociali di una community online. Second Life ha vissuto i suoi anni d'oro nei primi anni 2000, quando milioni di giocatori hanno popolato il suo mondo virtuale generando una fiorente economia relativa ai contenuti personalizzati. La popolarità di

Second Life ha attirato moltissimi brand, che hanno implementato un'attività di marketing con il placement dei loro prodotti e l'organizzazione di eventi in-game. Addirittura nel 2008 diversi Stati vi aprirono le loro ambasciate virtuali. Attualmente Second Life esiste ancora, ma è ben lontano dai fasti originali raggiunti in quegli anni.

- **Fortnite**: è forse l'esempio più famoso e in voga del momento. Uscito nel 2017, Fortnite è diventato un fenomeno transmediale capace di arrivare ad oltre 350 milioni di utenti iscritti nel 2022. Esso è un esempio di gioco multiplayer, ma a differenza della connotazione classica dei multiplayer competitivi, punta sulla formazione di una community all'interno della piattaforma, dove non trova spazio soltanto il gioco, ma anche varie forme di interazione sociale tra i partecipanti. Per esempio proprio su Fortnite è stato organizzato il primo concerto virtuale della storia. Nel febbraio 2019, infatti, DJ Marshmello si è esibito per circa 10 minuti davanti ad oltre 10 milioni di utenti. L'iniziativa ha riscontrato un successo senza precedenti, dimostrando la grande potenzialità di queste piattaforme.

- **Roblox**: differisce dai comuni giochi in multiplayer in quanto consentono una libertà pressoché totale nel generare contenuti, dando modo agli utenti di condividere le loro creazioni. Roblox di recente ha ottenuto una capitalizzazione prossima ai 50 miliardi di dollari. La sua community è caratterizzata da un pubblico compreso tra gli 8 e i 13 anni. Il target di giovanissimi rende Roblox assolutamente interessante per vari brand, che attivano campagne di marketing all'interno della sua piattaforma.
  Nella stessa tipologia di piattaforma si può anche citare **Minecraft**.

1.3.2 Metaversi con Blockchain

Ad oggi i numeri delle piattaforme basate su blockchain non sono certamente paragonabili con i casi appena presentati: le community di Fortnite e Roblox vantano decine di milioni di utenti al mese, invece le community di **Decentraland** e **The Sandbox**, i due blockchain metaverse più popolari, viaggiano attualmente nell'ordine di alcune decine di migliaia di lander (utenti). Però le potenzialità di questi ultimi appaiono molto più intriganti, in quanto consentono di fare letteralmente ciò che si vuole all'interno del mondo virtuale, di rivivere pertanto le emozioni di Second Life in un contesto tecnologico molto più evoluto, finalmente pronto per arrivare laddove Second Life era riuscito soltanto in parte.
Se un metaverso gaming come Roblox unisce sapientemente le dinamiche multiplayer con la possibilità di creare contenuti da parte degli utenti, un blockchain metaverse come The Sandbox consente di andare ben oltre, consentendo ai partecipanti di possedere delle proprietà, in maniera del tutto simile al mondo reale,

sulle quali avviare delle vere e proprie iniziative imprenditoriali. In altri termini, il metaverso sfrutta la tecnologia blockchain soprattutto per creare vari modi con cui monetizzare l'esperienza, seguendo dinamiche simili a quelle del mondo reale, pur in un contesto fantasy distopico.

1.4 Futuro del Metaverso

Una domanda molto interessante è quella di come sarà davvero il Metaverso in futuro e se si riuscirà a trovare una sua definizione univoca. É ragionevole pensare che l'obiettivo sia di creare un Metaverso mondiale, che sarà costituito da diversi livelli, in maniera simile a come è strutturato l'attuale internet. Questa realizzazione è però ancora lontana, allo stato attuale, soprattutto perché richiede una potenza tecnologica estremamente avanzata, non disponibile al momento. Inoltre non tutte le idee convergono, ma permangono diverse visioni su come potrebbe evolversi e, da un certo punto di vista, nascere questa tecnologia.
É emerso un ampio consenso sul livello di presentazione. Ci si aspetta che l'interfaccia utente assomigli meno ad una finestra del browser piena di testo e grafici informativi e più a un videogioco. Non si tireranno giù i menù e non si cliccherà sulla barra dei collegamenti per visitare siti diversi o utilizzare servizi diversi. Invece gli avatar personalizzati cammineranno, voleranno o si teletrasporteranno da un luogo all'altro in un mondo visuale popolato da biblioteche, edicole, banche, sale da concerto e centri commerciali. Al livello della presentazione, Decentraland e The Sandbox offrono già ottimi esempi.
Non è una sfida difficile creare i livelli superiori del Metaverso. Decine di videogiochi forniscono già le funzioni di base. Aggiungere una bella interfaccia 3D ai siti web esistenti o alle piattaforme di social media non offre però gli stessi benefici che ci si aspetta dal Metaverso. Perché il metaverso sia una piattaforma veramente trasformativa, le cose devono cambiare a livelli più profondi.
Da qui emerge anche un'idea che vede il Metaverso ideale come un ibrido tra mondo reale e mondo virtuale: sfruttando le tecnologie della realtà aumentata, ad esempio, o nuove possibili tecnologie future, si potrebbe vivere il Metaverso anche restando direttamente "connessi" con il mondo reale.
Comunque, è fondamentale che ogni spazio virtuale nel metaverso presenti tutti gli avatar nello stesso modo. Ovunque bisogna poter acquistare e raccogliere oggetti e portarli con sé in altri spazi. Ci dovrebbe essere un unico *login* quando si entra nel metaverso, non una procedura di accesso diversa per ogni attività nel mondo virtuale. Inoltre la valuta da usare online dovrebbe essere universalmente accettata o convertita in modo invisibile e automatico in modo da non dover tornare indietro nel vecchio internet per scambiare fondi sul sito di una banca. Infine non dovrà mancare la persistenza tra le caratteristiche base del Metaverso: infatti sarà molto

importante che tutto prosegua in maniera continua anche mentre l'utente è disconnesso. Questa è una grande differenza rispetto alla maggior parte dei videogiochi presenti ad oggi, dove nel momento in cui ci si disconnette il mondo virtuale entra in una sorta di "freeze", che si sblocca solamente una volta che il giocatore torna a connettersi. In questa idea di Metaverso entra in gioco fortemente la tecnologia blockchain.

1.4.1 Ruolo delle Blockchain

Ci sono tre modi principali in cui la tecnologia blockchain può giocare un ruolo importante in un metaverso mondiale.

1. In primo luogo, il metaverso potrebbe integrare la tecnologia blockchain come servizio di basso livello per assicurare che la realtà di consenso emergente sia veramente decentralizzata. Senza tale decentralizzazione, il metaverso rischia di essere implementato come una serie di giardini recintati incompatibili. Per esempio, si visiterà il metaverso di Google o il metaverso di Apple o il metaverso di Meta, ma non ci sarà una vera connessione tra di loro. L'interoperabilità richiederà protocolli e decentralizzazione che potrebbero limitare le società tecnologiche dall'ottenere i profitti a cui sono abituate. Ma questa interoperabilità sarà essenziale affinché il metaverso raggiunga il suo potenziale.

2. In secondo luogo, il metaverso avrà bisogno di una valuta mondiale, basata ovviamente sulla blockchain. Il metaverso potrebbe anche utilizzare più valute, ma la conversione dovrà essere automatica, invisibile e istantanea.

3. Infine, il mondo della blockchain offre una soluzione ordinata alle questioni di personalizzazione e proprietà. Si potrebbe visitare uno shop virtuale per personalizzare il proprio avatar o decorare la propria casa nel metaverso. L'aspetto fondamentale è il bisogno di un modo per stabilire la proprietà degli oggetti digitali che si acquistano: la soluzione a questo problema è data dai **Token Non Fungibili (NFT)**. Gli NFT di oggi potrebbero servire come tecnologia di collegamento per affrontare una serie di esigenze tecniche del metaverso.

2 L'economia del Metaverso

L'economia del Metaverso è uno dei suoi aspetti più affascinanti. Il Metaverso infatti non è solo un mondo digitale che, grazie a tecnologie di creazione di ambienti tridimensionali e di avanzata immersione sensoriale, promette esperienze ed interazioni realistiche con persone da tutto il mondo per mezzo di avatar (cioè loro rappresentazioni virtuali), ma l'utilizzo della blockchain apre anche a interessanti possibilità che stanno rivoluzionando il commercio digitale, mettendo in rete nuove opportunità di business. La blockchain è infatti il vero fattore che rende l'esperienza del Metaverso la più completa possibile, fornendo garanzia e trasparenza sulle transazioni effettuate e mettendo a disposizione tutte le sue funzionalità. Di seguito analizziamo nel dettaglio l'economia del Metaverso e il suo legame con la blockchain.

2.1 Criptovalute

La tecnologia della blockchain ha consentito la nascita e la diffusione delle criptovalute. Esse sono il denaro dell'economia dei Blockchain Metaverse. Le cosiddette crypto metaverso sono infatti unità di valuta virtuali utilizzate per effettuare transazioni digitali all'interno del Metaverso e servono come collegamento tra il Metaverso e il mondo fisico, permettendo di realizzare profitti in valuta fiat per mezzo delle piattaforme exchange, come Binance o Crypto.com.
Proprio come ci sono diversi Metaversi, ci sono anche diverse crypto metaverso. Esse sono infatti token proprietari: una sorta di gettoni virtuali che possono essere usati come monete virtuali, ma che sono basati su una blockchain esistente, e in cui tutte le transazioni avvengono soltanto utilizzando la criptovaluta proprietaria di ciascun Metaverso. Le crypto del metaverso non sono molto diverse dalle altre criptovalute e token già sul mercato, ma trovano applicazione in questo particolare settore. Funzionano in modi diversi e sono legate a giochi specifici, offrendo come già detto la possibilità di guadagnare mentre si gioca e/o fare investimenti in universi virtuali.
In Figura 2.1 è riportata una classifica recente delle prime 7 crypto metaverso per capitalizzazione di mercato. É bene osservare che numerosi importanti progetti di Metaverso sono costruiti sulla blockchain di Ethereum, come Decentraland, the Sandbox, Axie Infinity e Enjin Coin, presenti in questa classifica.

#	Name	Price	24h %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days	Dominance
1	ApeCoin APE Buy	$8.36	-7.92%	$2,380,014,034	$664,780,571 79,561,964 APE	284,843,750 APE		0.1844%
2	Decentraland MANA	$1.21	-7.25%	$2,227,194,701	$539,638,306 446,813,779 MANA	1,844,089,405 MANA		0.1725%
3	The Sandbox SAND	$1.35	-5.50%	$1,661,117,880	$396,911,310 293,311,166 SAND	1,227,539,778 SAND		0.1287%
4	Theta Network THETA	$1.37	-6.98%	$1,369,924,360	$101,416,347 74,030,618 THETA	1,000,000,000 THETA		0.1061%
5	Axie Infinity AXS	$20.66	-11.14%	$1,258,128,017	$372,510,348 18,033,677 AXS	60,907,500 AXS		0.0975%
6	Stacks STX	$0.5645	-6.76%	$741,667,843	$11,641,312 20,621,812 STX	1,313,815,452 STX		0.0575%
7	Enjin Coin ENJ	$0.7244	-4.54%	$644,383,759	$101,736,883 140,433,586 ENJ	889,481,956 ENJ		0.0499%

Figura 2.1. Classifica attuale delle crypto metaverso per capitalizzazione di mercato (fonte CryptoMarketCap).

Il motivo di questo successo di Ethereum nello sviluppo di Metaversi è da attribuire, oltre che alla sua diffusa adozione globale, alla funzionalità degli smart contracts da lei supportata.
Tramite l'utilizzo di **smart contracts** (programmi informatici mediante i quali alcune azioni vengono eseguite automaticamente all'avverarsi di condizioni predefinite) è infatti possibile regolare le relazioni economiche e sociali del Metaverso, stabilendo delle leggi di base per il mondo virtuale.
In conclusione, per riassumere possiamo dire che le criptovalute sono il carburante che alimenta il Metaverso: esse servono per acquistare qualsiasi tipo di prodotto o servizio nel mondo virtuale, con il vantaggio di operare su un registro decentralizzato, che garantisce quindi trasparenza, sicurezza e immutabilità delle transazioni.

2.2 Smart contracts

Abbiamo già citato come gli smart contracts esistano per automatizzare operazioni su blockchain e assicurare che le transazioni avvengano secondo regole e standard prestabiliti. Rispetto alle odierne applicazioni internet, la caratteristica più distintiva dello smart contract è l'irreversibilità della sua esecuzione, essendo archiviato sulla blockchain e dunque producendo un risultato immutabile e testimoniato dall'intera catena. Ciò rende gli smart contracts la scelta perfetta per l'implementazione di token crittografici: dietro ogni token c'è infatti uno smart

contract. Per la realizzazione di un Metaverso iperreale e per supportare attività simili al mondo fisico all'interno del mondo digitale, gli smart contracts svolgono quindi un ruolo fondamentale. Inoltre, lo sviluppo di smart contracts è utile per autorizzare il processo di creazione di funzionalità aggiuntive nel Metaverso senza sostanzialmente modificare la sua intera base di codice.

2.3 NFT

Se il Metaverso sarà il nuovo mondo, gli NFT saranno i mattoni. Infatti, un altro pilastro dei Blockchain Metaverse oltre alle criptovalute sono proprio i non-fungible token.
La differenza tra token fungibili e non fungibili è che i primi sono uguali l'uno all'altro, perciò per esempio tutte le criptovalute sono token fungibili poiché hanno l'obiettivo di funzionare come mezzo di scambio, mentre i token non fungibili sono smart contracts che rappresentano l'atto di proprietà e il certificato di autenticità scritto su blockchain di un bene unico (digitale o fisico); essi non sono quindi reciprocamente intercambiabili.
Tutto quello che conosciamo e facciamo può essere tramutato in NFT, ma in questo momento ci sono alcune categorie di NFT che vanno per la maggiore, ad esempio i collezionabili, l'arte e la fotografia, gli avatar, la musica, ecc. Gli appassionati fanno a gara tra loro nei siti di aste specializzate per mettere le mani su oggetti virtuali unici; basti pensare che l'opera NFT che al momento detiene il record assoluto di incassi è l'immagine digitale "The Last 5000 Days" dell'artista Beeple, venduta per la sorprendente cifra di 69 milioni di dollari (42.329 ETH). Il meccanismo alla base di questa ossessione non è diverso da quello del collezionismo tradizionale, se non per il fatto che l'acquirente poi non finisce per avere un oggetto fisico da poter esporre, ma l'unica ricompensa è il prestigio di poter dire di essere gli unici possessori al mondo dell'originale. Un NFT può però essere anche associato al diritto di usufruire di un servizio esclusivo, ad esempio l'ingresso ad un evento; gli utilizzi sono quindi moltissimi e in continua evoluzione.
All'interno dei Blockchain Metaverse l'utente si trova in una realtà digitale in cui tutte le risorse grafiche, a partire dall'avatar che impersonifica e il paesaggio che vede ed esplora, sono un non-fungible token. Si possono individuare tre tipologie di NFT principali presenti nei Metaversi, analizzate di seguito.

2.3.1 NFT di beni immobili/terreni

La risorsa principale di un Blockchain Metaverse è costituito dalla terra (detta land), una proprietà immobiliare sotto forma di NFT che consente di dare luogo e forma alle proprie attività virtuali. Proprio come nel mondo reale, il costo dei

terreni nel Metaverso varia in base alla posizione geografica, al prestigio del luogo in cui si trova la proprietà e alla grandezza dello spazio a disposizione, ed è ovviamente nella valuta specifica di quel mondo virtuale.
Al momento le piattaforme virtuali più famose del Metaverso dove è possibile acquistare terreni sono The Sandbox e Decentreland, in cui questi NFT sono venduti a cifre da capogiro: su The Sandbox, ad esempio, un utente ha pagato un equivalente di 450.000 dollari per un terreno vicino alla casa di Snoop Dogg. Entrambi i Metaversi, per ora, mettono a disposizione un numero limitato di aree di terreno, monitorando costantemente l'evoluzione della domanda e mantenendo il loro valore quanto più possibile entro determinati range prestabiliti.
Il mercato immobiliare del Metaverso, detto **Virtual Real Estate**, ha raggiunto nel 2021 un valore di 500 milioni di dollari ed è in forte crescita: si stima che a fine 2022 la cifra sarà addirittura raddoppiata.

2.3.2 NFT legati alla moda

Gli NFT legati alla moda sono semplicemente accessori digitalizzati che possono essere indossati dagli avatar digitali degli utenti per distinguersi da tutti gli altri. Per molte persone, soprattutto nelle convinzioni di molti brand, nel prossimo futuro invece di guardare nel proprio armadio per scegliere qualcosa da indossare per una videochiamata, si potrebbe spulciare il proprio guardaroba virtuale per scegliere un vestito digitale renderizzato in 3D da "indossare". Inoltre, sempre più produttori in ambito fashion scommettono che questi abiti virtuali potrebbero eventualmente essere indossati in tutto il Metaverso, nei giochi, sui social media e anche "visti" sul corpo nel mondo reale attraverso occhiali di realtà aumentata.
Gli NFT legati alla moda all'interno del Metaverso sono stati oggetto di collaborazione con molti marchi importanti, come Gucci e Louis Vuitton, che hanno lanciato articoli di moda in edizione limitata. Decentraland ha creato addirittura il "Luxury Fashion District", dove a Marzo si è tenuta la prima Metaverse Fashion Week, un insieme di eventi, presentazioni, after-party e sfilate completamente virtuali ma con la partecipazione di molti noti brand reali. Questo dimostra come la prossima grande vetrina dell'industria della moda potrebbe diventare interamente virtuale per mezzo del Metaverso e degli NFT.

2.3.3 NFT In Game

Il Metaverso, oggi, viene utilizzato soprattutto per il gaming. Le potenzialità degli NFT legate al mondo dei Metaversi sono talmente infinite che sempre più aziende appartenenti al mondo videoludico stanno investendo in questo campo. Secondo un rapporto rilasciato dalla Blockchain Gaming Alliance, il gaming su blockchain continua infatti a crescere e a dominare il settore degli NFT, con una quota di

mercato di circa il 22%.
Gli NFT In Game consistono in oggetti, personaggi o qualsiasi altra cosa utilizzabile all'interno del gioco e che sono parte delle sue dinamiche. Sono quindi qualcosa di astratto che può essere impiegato per combattere e avanzare. Possono inoltre essere scambiati con altri giocatori, ottenendo così un guadagno.
In questo contesto, un Metaverso importante è ad esempio Star Atlas, costruito sulla blockchain di Solana. Esso è forse uno dei Metaversi orientati al gaming più complessi, non tanto per la difficoltà di gioco, quanto per la varietà di scenari, possibilità e oggetti presenti al suo interno. É ambientato nello spazio in un futuro distopico, nell'anno 2060, in cui tre fazioni in guerra tra loro si combattono per avere il possesso sulle poche risorse rimaste. Ci sono momenti in cui bisogna sfidare gli avversari, altri in cui è più simile a un gioco di ruolo, si deve poi esplorare il mondo in cui ci si trova alla ricerca degli oggetti più vari, come vestiti, armi, risorse in genere, che possono essere scambiate non solo per avere la meglio sui nemici, ma anche per ottenere guadagni dalla loro vendita. Sono NFT quindi per esempio le navi con cui esplorare il mondo virtuale, le strutture come stazioni spaziali o centrali elettriche, oggetti da collezione come skin, poster o equipaggiamenti; sono NFT anche i nomi utente e molto altro ancora.

2.4 Play-to-Earn

L'ascesa della tecnologia blockchain ha portato a un cambiamento di paradigma nell'industria del gioco: se fino a poco tempo fa essa equivaleva a divertimento, oggi equivale a ritorni economici notevoli, come in parte si è già avuto modo di capire da quanto detto in precedenza.
I non-fungible tokens e le criptovalute consentono infatti una meccanica Play-to-Earn, che permette ai giocatori di guadagnare attraverso l'attività di gioco. Il premio viene elargito al giocatore sotto forma di token, con un valore direttamente proporzionale alla quantità di ore impiegate nel gioco, dunque vale il principio per cui chi gioca di più vince ricompense più consistenti. Partecipando o semplicemente passando il tempo a giocare quindi vi è la possibilità di creare profitto, tramite i token guadagnati.
Un Metaverso Play-to-Earn di successo è ad esempio Axie Infinity, gioco basato su Ethereum e ispirato a Pokémon, dove i giocatori possono collezionare, allevare e far combattere piccoli animaletti domestici detti Axies, rappresentati da NFT. Attraverso il completamento di sfide o battaglie con altri Axies, ovvero giocando, è possibile guadagnare token del Metaverso, in maniera proporzionale ai propri punti esperienza, cioè al tempo passato nel gioco.
Il Play-to-Earn è indispensabile per attirare nel Metaverso un numero di utenti

sempre più elevato, ai fini di renderlo sempre più interessante agli occhi degli sponsor intenzionati a entrare come proprietari o come semplici attori di marketing.

2.5 Branding & Marketing

I brand oltre a partecipare al Metaverso producendo degli NFT legati al loro marchio, possono anche decidere di investire nell'acquisto di proprietà, laddove dare forma ad attrattive e negozi virtuali. Nel Metaverso di The Sandbox, ad esempio, sono presenti importanti brand appartenenti ad ambiti di business anche molto diversi tra loro: ritroviamo un nome di culto nell'industria dell'entertainment come Atari, un fashion brand come Adidas, un rapper come Snoop Dogg o franchise come The Walking Dead o i Puffi. Questo perché usufruendo di Metaversi già consolidati è possibile raggiungere il pubblico in modo innovativo, raccontando i propri valori e pubblicizzando nuovi prodotti. In particolare, alcuni vantaggi del metaverse marketing sono:

- aumentare la visibilità del brand aggiungendo ai visitatori di negozi/mostre fisici un numero di partecipanti potenzialmente illimitato
- veicolare i valori dell'azienda rendendo il pubblico parte attiva del racconto
- rafforzare l'immagine del brand presso l'audience di riferimento, oltrepassando la logica del prodotto e ponendo l'enfasi sul fattore emozionale ed esperienziale
- consolidare il legame di fedeltà con il pubblico di clienti o semplici appassionati del brand attraverso la condivisione di un evento virtuale, fortificando il senso di appartenenza alla community.

Il Metaverso rappresenta quindi per aziende e brand un nuovo mercato emergente dove poter trovare visibilità, applicare nuove strategie per fare business e ampliare il proprio profitto.

2.6 Eventi virtuali

All'interno delle proprietà del Metaverso è possibile creare eventi, come concerti virtuali, oppure giochi, parchi tematici ed altre attività capaci di generare un flusso economico, sia per quanto concerne le risorse necessarie per crearle (i creatori producono gli NFT necessari all'evento e li vendono all'organizzatore), sia per il profitto generato dalla partecipazione all'esperienza degli altri abitanti del Metaverso, che dovranno acquistare biglietti sotto forma di NFT.
In un mondo virtuale in 3D dove è di fatto possibile creare qualsiasi cosa, gli event planner si possono quindi sbizzarrire, non dovendo obbedire alle leggi della fisica

o avere a che fare con problemi di sicurezza pubblica.
Il Metaverso dà inoltre la possibilità agli eventi di essere più inclusivi: potranno ospitare un numero molto maggiore di persone ed elimina le barriere delle distanze fisiche, per cui potranno ospitare un pubblico mondiale potenzialmente illimitato, rappresentando una vera rivoluzione in questo settore.

3 Blockchain

3.1 Raccolta dei dati

Il Metaverso sarà una realtà digitale che si affiancherà al mondo fisico. Man mano che sempre più persone si uniscono ai mondi digitali, grandi quantità di dati vengono creati e la capacità di archiviazione dei dati del mondo fisico verrà spinto al limite. Di conseguenza, l'archiviazione dei dati sarà un'importante sfida per la distribuzione di applicazioni come giochi, intrattenimento, immobili o assistenza sanitaria sul Metaverso.

L'acquisizione di dati autentici sarà semplificata per applicazioni come social networking con il passaggio alla tecnologia blockchain. La rete distribuita consentirà la convalida delle transazione e il tracciamento dei dati del Metaverso. Tutti i dati acquisiti sono sottoposti a una validazione tramite i protocolli di consenso che saranno specifici di ogni blockchain, di conseguenza l'acquisizione dei dati è resistente agli attacchi che mirano a corrompere i dati archiviati. Sebbene le tecnologie di archiviazione dei dati siano progredite, la mole di dati continuerà ad aumentare e riuscire a tenere il passo con la quantità e la velocità alla quale i dati vengono generati è un compito complicato. Inoltre, anche l'eterogeneità dei dati generati dalle applicazioni rappresenta una grande sfida.

L'abilità di sfruttare i dati nel Metaverso è ciò che li rende preziosi. La raccolta e organizzazione dei dati è essenziale per gli utenti, per questo è un settore che richiede un grande investimento di tempo e fatica. L'uso della tecnologia blockchain aiuterà nella raccolta di dati da fonti attendibili, riducendo così la quantità di dati errati. I proprietari dei dati avranno controllo totale sui propri dati, ed eventuali manipolazioni di dati da parte di terzi saranno limitate. Ciò garantisce che i dati che fluiscono nel Metaverso siano di un elevato standard di qualità. Inoltre, grazie alla natura decentralizzata della tecnologia blockchain, i *data scientist* potranno comunicare e collaborare all'ottimizzazione dei dati, che ridurrà notevolmente i tempi e le spese associate alla classificazione e alla creazione dei *data set* per applicazioni di analisi, nonché il rischio di contaminazione dei dati. Questo migliorerà la disponibilità di dati per gli stakeholder del Metaverso, permettendone uno sviluppo rapido ed efficace.

Alcuni dei problemi, come i modelli di consenso, il costo dei blocchi e la verifica delle transazioni, sono ancora lontani da una soluzione e di conseguenza, il processo per cambiare l'intero sistema sarà lungo e costoso. Questi problemi saranno risolti

in futuro, spianando la strada per una vasta gamma di nuove ed entusiasmanti opportunità.

3.2 Privacy

La tecnologia blockchain offre gli utenti del Metaverso la possibilità di controllare le proprie informazioni personali attraverso l'uso di chiavi private e pubbliche, concedendo di fatto titolarità dei propri dati. In questo modo gli intermediari di terze parti non possono abusare o guadagnare dati personali conservati nel Metaverso, ma saranno direttamente i proprietari a regolare quando e come una terza parte può accedere alle proprie informazioni.

Questo obiettivo è possibile grazie al fatto che sulla blockchain è implementabile un protocollo di *Zero-knowledge proof*, questo permette agli utenti di avere un comodo accesso ai dati essenziali del Metaverso, ma proteggendo la loro privacy e mantenendo la proprietà sui propri beni. La *Zero-knowledge proof* è un protocollo di blockchain con cui gli utenti possono persuadere le applicazioni che qualcosa su di loro c'è realmente senza rivelare le informazioni.

L'adozione della tecnologia blockchain può aiutare gli utenti a proteggere la privacy dei propri dati. Tuttavia, un singolo errore umano, come la perdita di una chiave privata, ha il potenziale per compromettere la sicurezza della tecnologia blockchain e la privacy dei dati nel Metaverso. Inoltre, gli aggressori possono facilmente prendere di mira le applicazioni di terze parti, poiché tendono ad avvalersi di meccanismi di sicurezza inadeguati, che portano alla compromissione delle informazioni personali. Quindi, c'è ancora molto potenziale per un'indagine su come la blockchain può garantire la privacy dei dati degli utenti nel Metaverso.

3.3 Interoperabilità dei dati

Il Metaverso sarà una piattaforma di interazione sociale e culturale; verrà creata attraverso la fusione di numerosi regni digitali e l'interoperabilità sarà la principale forza trainante. Verranno creati progressivamente dei ponti virtuali per consentire agli utenti di mantenere i loro *avatar* e beni mentre si trasferiscono tra diversi mondi virtuali. Un insieme diversificato di applicazioni come la finanza e sanità saranno in grado di comunicare e scambiare informazioni. Le tradizionali piattaforme digitali centralizzate attualmente disponibili sono disgiunte e disorganizzate. Gli individui devono configurare i propri account, *avatar*, hardware e metodi di pagamento per usare diverse applicazioni, e le opzioni a disposizione dell'utente per trasferire i propri beni digitali come NFT e *avatar* in un altro ambiente digitale sono limitate.

La possibilità di introdurre un'applicazione nel mondo virtuale dipenderà dall'interconnessione tra i mondi virtuali. Indipendentemente da dove si trovano o quale tecnologia adottano, le applicazioni del mondo digitale dovrebbero essere in grado di comunicare liberamente informazioni una con l'altra. L'interoperabilità del Metaverso dipende dalla capacità di gestire le interazioni tra mondi virtuali in un modo appropriato, che è una grave limitazione dell'approccio tradizionale. Per questo un protocollo a catena incrociata è una soluzione perfetta, in quanto consente lo scambio di possedimenti come *avatar*, NFT e pagamenti tra mondi virtuali. Questo protocollo fornirà le basi per l'adozione diffusa del Metaverso ed eliminerà la necessità di intermediari. La sola blockchain renderà semplice la connessione tra persone e l'uso di applicazioni.

Nonostante il potenziale della blockchain in aumento, per avere l'interoperabilità tra diversi mondi virtuali nel Metaverso sono necessarie ulteriori ricerche. La sfida principale del protocollo a catena incrociata è l'esistenza di diverse blockchain pubbliche in diversi mondi virtuali che non condividono un linguaggio comune. Esse, infatti, adottano diverse architetture nei blocchi, diversi protocolli di consenso e forniscono diversi gradi di *smart contracts*, rendendo difficile l'interoperabilità.

3.4 Blockchain per IoT nel Metaverso

Il Metaverso dovrà raccogliere dati da una varietà di dispositivi *Internet of Things* (IoT) per garantire che funzioni in modo efficiente in diverse sue applicazioni come medicina, istruzione e città intelligenti. I dispositivi IoT connetteranno il Metaverso attraverso l'uso di una gamma diversificata di hardware e controller. Il collegamento al Metaverso e la navigazione sia fisica che virtuale è resa possibile da dispositivi dotati di sensori specializzati. La capacità dei dispositivi IoT di eseguire operazioni nel Metaverso sarà fondamentale per permettere all'utente di operarvici.

I dati in un Metaverso devono essere privi di errori per poter essere analizzati. L'uso di una strategia centralizzata non è vantaggiosa quando si parla di memorizzare dati per mondi virtuali in quanto, se anche un singolo pezzo di dati è stato manomesso, danneggerà l'intero insieme di risultati prodotti. Per eliminare i conflitti e aumentare la fiducia tra gli utenti del Metaverso, ciascuna transazione è registrata e autenticata con la blockchain consentendo l'archiviazione dei dati in tempo reale. Così facendo tutte le parti interessate possono fare affidamento sui dati e agire prontamente ed efficientemente grazie alle transazioni immutabili. Inoltre, la blockchain consentirà ai dispositivi IoT di condividere e archiviare dati reali in modo sicuro su più mondi virtuali grazie all'interoperabilità.

La più grande sfida legata all'IoT nel Metaverso è legata all'enorme quantità

di sensori connessi. Con così tanti dispositivi connessi, l'archiviazione e la sicurezza sono una preoccupazione. Inoltre, è incredibilmente difficile analizzare dati IoT non strutturati in tempo reale; ricordando che la qualità dei dati può essere giudicata in base a quantità, accuratezza e velocità.

3.5 Blockchain per il digital-twin nel Metaverso

Le applicazioni del Metaverso non potranno funzionare correttamente a meno che non vi sia una forte connessione tra il mondo fisico e quello digitale. Ciò è reso possibile dai *digital-twins* che sono una rappresentazione digitale sofisticata della realtà nel Metaverso, dai beni semplici a prodotti complessi. Dunque, tutto ciò che è rilevante per le esigenze dell'utente potrebbe diventare una componente dell'ecosistema utilizzando i *digital-twins*.

Collaborazioni tra *digital-twins* in diversi mondi virtuali dovrebbero essere possibili, un *avatar* deve poter interagire e collegarsi ai *digital-twins* di servizi che vanno dall'assistenza sanitaria ai mercati finanziari. Inoltre, siccome i mondi virtuali sono in continua evoluzione, i *digital-twins* dovrebbero rilevare e rispondere a queste modifiche.

I dispositivi IoT consentono agli utenti di dare vita ai loro modelli preferiti mantenendoli sincronizzati con il mondo reale. Ogni azione del *digital-twins* nel Metaverso sarà registrata come una transazione sulla blockchain, che è immutabile e richiede consenso al cambiamento. Inoltre, unendo blockchain con AI, sarà possibile tracciare i dati dei sensori e produrre gemelli digitali di alta qualità. Infine, le proprietà crittografiche della blockchain e la trasparenza dei dati storici permettono ai *digital-twins* di resistente ad attacchi e condividere i dati in modo sicuro su diversi mondi virtuali.

I *digital-twins* dovrebbero essere in grado di identificare e correggere gli errori, il che si traduce in una comunicazione più accurata e coerente. Tuttavia, quando una varietà di dispositivi e sensori viene riunita per sviluppare questi modelli in tempo reale, è difficile mantenere i dati al sicuro da attachi *malware*. Inoltre, l'accuratezza del modello è influenzata dalla qualità dei dati utilizzato per creare il modello. In altre parole, i dati forniti dal la fonte deve essere genuina e conforme agli standard in termini di qualità.

4 The Sandbox

4.1 Che cos'é

"The Sandbox is a virtual metaverse where players can build, own, and monetize their gaming experiences on the Ethereum blockchain using the platform's utility token SAND. Players can create digital assets in the form of Non-Fungible Tokens (NFTs), upload them to the marketplace, and integrate them into games with Game Maker".

The sandbox é una delle realtá più concrete e promettenti nel mondo dei metaversi con blockchain. Si tratta di un progetto che nasce da due videogiochi per Android chiamati the sandbox (2011) e the sandbox revolution (2019), in cui i videogiocatori potevano costruire un mondo 2D in pixel art in completa libertà. Il progetto oggi parte da questa idea di poter costruire liberamente qualsiasi cosa, ma ampliandola tramite la possibilità di attribuire agli utenti la proprietà delle opere create come NFT e premiandoli per la partecipazione all'ecosistema. L'obiettivo dell'azienda è di creare quindi un ecosistema di gioco "community-driven", ossia un luogo nel quale i creator possano realizzare e monetizzare oggetti e giochi, usando la blockchain. É un progetto di Metaverso decentralizzato: ciò significa che non è la software house a decidere il valore dei beni sul mercato, bensì gli utenti che ne popolano la mappa. Questo metaverso, come molti altri permette ai videogiocatori di navigare all'interno di questo mondo virtuale tramite il proprio avatar, acquistare e vendere terreni , creare videogiochi all'interno di questi land e addirittura creare qualsiasi tipo di oggetto, sempre restando all'interno del mondo di gioco.

4.2 Il SAND

Il SAND è la cryptomoneta o token su cui si basa l'economia The Sandbox. Si tratta di un token ERC-20 disponibile dall'agosto 2020 e utilizzato per qualsiasi transazione interna all'ecosistema del videogioco. Giocatori, sviluppatori e publisher utilizzano SAND come valuta di The Sandbox, trasferibile un numero illimitato di volte per transazioni P2P, come l'acquisto o la vendita di LAND o ASSET, o anche l'accesso a GAMES. Caratteristica chiave del token è la potenziale crescita nel valore a causa della sua limitata disponibilità: si contano, infatti, 3 miliardi di SAND per gli utenti. Qualsiasi transazione in SAND prevede una tassa di transazione del 5%, di cui il 50% va allo Staking Pool e la parte restante alla

Foundation. La Foundation è costituita dai fondatori stessi di The Sandbox e tali entrate permettono di supportare l'ecosistema di The Sandbox offrendo continuamente esperienze di gioco e contenuti aggiuntivi di alta qualità. Lo Staking Pool, invece, è una porzione di SAND progettata come fondo per pagare gli interessi di staking degli utenti.

4.3 Gli asset

Uno dei concetti più importanti di questo Metaverso è quello di **asset**, ovvero qualsiasi costruzione 3D all'interno del mondo di gioco che può essere creata da qualsiasi utente . Essi sono NFT registrati con standard ERC-1155 su Ethereum. L'ASSET verrà caricato in una rete IPFS (InterPlanetary File System), un protocollo su rete peer-to-peer per archiviare e condividere dati identificandoli con un codice univoco, su piattaforma decentralizzata. Verrà poi registrato sulla blockchain per dimostrare la sua proprietà da parte del creatore e, in caso di acquisto, dell'acquirente. Oltre agli ASSET, l'utente potrà creare modalità di gioco in maniera completamente gratuita grazie al Game Maker sviluppato appositamente per il Metaverso di The Sandbox. Chiunque avrà modo di accedere a tale strumento, il quale non richiede alcuna abilità di programmazione e include guide e utility per l'apprendimento rapido e semplificato. Esattamente come gli ASSET, anche i giochi possono essere monetizzati richiedendo ai giocatori una tassa per parteciparvi. Per praticità, si identificano i giochi come GAMES, anch'essi registrati come Smart Contract sulla blockchain Ethereum con standard ERC-1155.

4.4 I land

ASSET e GAMES, a loro volta, si collocano in appezzamenti di terreno dalla dimensione pari a 96x96x128 metri detti **LAND** (o terre). La LAND è un pezzo di proprietà digitale nel metaverso di The Sandbox che i giocatori possono acquistare per costruire esperienze. Una volta che un giocatore possiede un pezzo di LAND, sarà in grado di popolarlo con giochi e assets. Più TERRE possono anche essere combinate per formare un estate. Il Metaverso di The Sandbox è formato esattamente da 166.464 LAND contenuti in una mappa unica. Una volta in possesso di un riquadro, anche questo registrato come NFT ma su ERC-721, gli utenti potranno eseguire le seguenti azioni.

- Giocare e creare giochi: all'interno di un LAND è possibile dare vita allo spazio sociale che si desidera, a partire da un ambiente per chattare con altri utenti fino a un mondo fantastico dove combattere con draghi e mostri.

- Guadagnare token: un utente può decidere se limitare l'accesso al LAND facendo pagare il biglietto in SAND, oppure affittarlo ai creatori di GAMES, rendendo gli appezzamenti una fonte di entrate passive. Allo stesso modo, i proprietari di GAMES potranno monetizzarli per pagare l'affitto e trarne profitto.
- Partecipare alla governance del Metaverso: possedere un appezzamento LAND permette di prendere parte al processo decisionale di The Sandbox che, da piattaforma nata per mano della community, riceve novità e cambiamenti a seconda del volere della comunità stessa.
- Ospitare concorsi ed eventi: l'utente può preparare attività personalizzate grazie alle quali ottenere ricompense speciali.

Bibliografia

[1] Francesco La Trofa. *Metaverso e blockchain: dai mondi virtuali 3D una nuova grande opportunità per l'universo crypto.* https://tech4future.info/metaverso-blockchain-virtuale-3d-crypto/, 2021.

[2] PixelPlex Team. *Decentralized Economy — the Role of Blockchain in the Metaverse.* https://pixelplex.io/blog/importance-of-blockchain-in-metaverse/, 2022.

[3] Biagio Campagna. *Metaverso e Blockchain: nascita di una nuova economia di internet?* https://www.dirittodelrisparmio.it/2022/01/14/metaverso-e-blockchain-nascita-di-una-nuova-economia-di-internet/, 2022.

[4] Alberto Maiorana. *Se il Metaverso sarà il nuovo mondo, gli Nft saranno i mattoni.* https://www.huffingtonpost.it/blog/2022/02/16/news/gli_nft_sono_i_mattoni_del_metaverso-8760143/, 2022.

[5] David Edwards. *How Cryptocurrency will be used in the Metaverse.* https://roboticsandautomationnews.com/2022/03/09/how-cryptocurrency-will-be-used-in-the-metaverse/49752/#:~:text=A%20key%20role%20of%20cryptocurrency,purchase%20any%20products%20or%20services, 2022.

[6] Nicola Donda. *Metaverso, Blockchain, criptovalute, NFT e altre buzzword del web 3.0.* https://www.aipem.it/blog/metaverso-blockchain-criptovalute-nft-e-altre-buzzword-del-web-3-0/, 2022.

[7] Thippa Reddy Gadekallu, Thien Huynh-The, Weizheng Wang, Gokul Yenduri, Pasika Ranaweera, Quoc-Viet Pham, Daniel Benevides da Costa, and Madhusanka Liyanage. *Blockchain for the Metaverse: A Review.* rXiv:2203.09738, 2022.

NFT E LO STANDARD ERC721

Riccardo Bertolo, Davide Fioriti, Manco Davide, Linda Terzi

Capitolo 1

Introduzione

1.1 Contenuti

Il termine "Blockchain 2.0" si riferisce ad un nuovo modo d'impiego della blockchain, in particolare estende la blockchain a settori diversi da quello finanziario attraverso l'utilizzo di Smart Contract e non-fungible token (NFT). sit [c]

Il concetto di NFT deriva originariamente da uno standard di token di Ethereum, con l'obiettivo di distinguere ogni token con segni distinguibili. Questo tipo di token può essere associato a proprietà virtuali/digitali come loro identificazioni univoche. Con gli NFT, tutte le proprietà contrassegnate possono essere liberamente scambiate con valori personalizzati in base alla loro età, rarità, liquidità, ecc. Tuttavia, lo sviluppo dell'ecosistema NFT è ancora in corso e le tecnologie degli NFT sono premature. Wang et al. [2021]

Nel presente elaborato si vuole approfondire lo standard ERC721 e i non-fungible token. In particolare dopo una breve introduzione agli strumenti della blockchain 2.0, dapprima si descrive lo standard ERC721 per poi studiare gli NFT attraverso una breve analisi di mercato e le loro applicazioni attuali e future.

1.2 Tecnologia Blockchain 2.0

1.2.1 Smart Contract

Il primo esempio di Smart Contract si è avuto con le macchine dispensatrici di bevande e merendine: in corrispondenza di un pagamento monetario automaticamente viene elargito un bene di consumo. sit [a]

Gli Smart Contract, originariamente introdotti da Szabo, hanno l'obiettivo di accelerare, verificare o eseguire la negoziazione digitale. La loro applicazione include molti ambiti tra cui quello assicurativo e immobiliare.

Ethereum ha ulteriormente sviluppato la tecnologia Smart Contract nel sistema blockchain. Wang et al. [2021]

Gli Smart Contract consentono a parti sconosciute e partecipanti decentralizzati di condurre scambi equi senza una terza parte fidata e proporre inoltre un metodo unificato per creare applicazioni in una vasta gamma di settori. Le applicazioni che operano su Smart Contract si basano su meccanismi di transizione statale. Gli stati, che contengono istruzioni e parametri, sono condivisi da tutti i partecipanti, garantendo così trasparenza nell'esecuzione delle presenti istruzioni. Wang et al. [2021]

Gli Smart Contract sono un tipo di account Ethereum, ovvero hanno un saldo e possono inviare transazioni in rete ma non sono controllati da un utente, bensì sono distribuiti in rete ed eseguiti come programmato. Essi sono veri e propri programmi che consentono di definire dei comportamenti ben definiti a fronte del verificarsi di alcuni eventi.

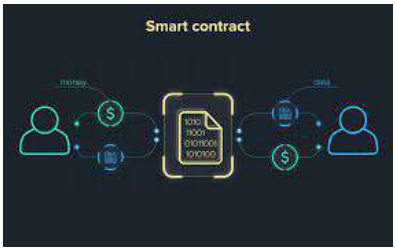


Figura 1.1. Immagine tratta da https://www.arlawpractice.com .

Gli account degli utenti possono interagire con uno Smart Contract inviando transazioni che eseguono una funzione definita sul contratto. Gli Smart Contract possono definire regole, come un normale contratto, e imporle automaticamente tramite codice; inoltre non sono eliminabili di default e le interazioni con essi sono irreversibili.sit [b]

La maggior parte delle soluzioni NFT si basano su piattaforme blockchain basate su Smart Contract per garantire esecuzioni sensibili agli ordini.Wang et al. [2021]

Scrittura

Uno Smart Contract è un contratto sotto forma di codice che rimanda l'esecuzione di alcune o tutte le sue clausole a un software. Il concetto di Smart Contract si compone delle seguenti tre parti:

- il codice di un programma che diventa l'espressione di una logica contrattuale (l'auto funziona solo in caso di pagamento delle rate);
- i messaggi inviati al programma stesso che rappresentano gli eventi che devono far attivare il contratto (il mancato pagamento della rata);
- un meccanismo che ponga in essere gli effetti previsti dalla logica (all'auto viene inibita la messa in moto). sit [c]

Basati sulla blockchain gli Smart Contract adottano linguaggi di scripting di Turing completi per ottenere funzionalità complicate ed eseguire una replica completa della transizione dello stato su algoritmi di consenso in modo da ottenere la coerenza finale.Wang et al. [2021]

Uno Smart Contract è una raccolta di codice (le funzioni) e dati (lo stato) che risiede a un indirizzo specifico sulla blockchain di Ethereum.sit [b]

Tutti possono scrivere uno Smart Contract e distribuirlo nella rete. Per distribuire un contratto, è sufficiente sapere programmare in un linguaggio per Smart Contract e avere abbastanza ETH.

Distribuire uno Smart Contract è tecnicamente una transazione, quindi occorre pagare così come avviene per un semplice trasferimento di ETH, con la differenza che i costi per la distribuzione di un contratto sono molto più elevati. Affinché la macchina virtuale Ethereum possa interpretare e memorizzare uno Smart Contract, questo deve però essere compilato prima di poter essere distribuito.

Sono stati messi a punto specifici linguaggi di programmazione, su tutti Solidity, per l'implementazione degli Smart Contract. In particolare Ethereum prevede i linguaggi:

- Solidity,
- Vyper. sit [b]

Il codice di uno Smart Contract si attiva ogni volta che l'account riceve un messaggio, consentendone la lettura e di scrivere nella memoria interna e inviare messaggi di follow-up o creare contratti successivi. Tutti i messaggi inviati e ricevuti come parte dell'esecuzione del codice hanno diversi campi.

Quelli standard per le criptovalute includono il destinatario, la firma del mittente e l'importo da trasferire. de Figueiredo Novo

Infine si sottolinea che gli Smart Contract sono pubblici su Ethereum e possono essere considerati come API aperte, è quindi possibile chiamare altri Smart Contract nel proprio contratto in modo da ampliare enormemente quello che è possibile fare con uno Smart Contract. Inoltre i contratti possono distribuire altri contratti.sit [b]

Limiti

Gli Smart Contract da soli non possono ottenere informazioni sugli eventi del mondo reale perché non possono inviare richieste HTTP; infatti basarsi su informazioni esterne potrebbe pregiudicare il consenso, importante per la sicurezza e la decentralizzazione, per questo si utilizzano gli oracoli.

Un altro limite degli Smart Contract è la dimensione massima del contratto. Uno Smart Contract può avere una dimensione massima di 24KB. sit [b]

1.2.2 Standard ERC-20 e standard ERC-721

ERC sta per Ethereum Request for Comments e sono standard tecnici basati su Ethereum token, disponibili online come EIP - Ethereum Improvement Proposals.

Gli EIP includono ciò che sono note come specifiche del protocollo di base, che comprendono quelle che sono state implementate e rilasciate, o quelli che dovrebbero esserlo, insieme alle API client e agli standard contrattuali.

Gli ERC comprendono standard e convenzioni a livello di applicazione per Ethereum inclusi, ma non limitati a Smart Contract e standard di token. Mentre ERC-20 specifica

l'interfaccia token standard, fornendo un'implementazione del modello per un'API token Smart Contract, ERC-721 lo fa per token non fungibili.

Esistono quindi due standard principali per i token: ERC-20 per i token fungibili (FT) e ERC-721 per token non fungibili (NFT). de Figueiredo Novo

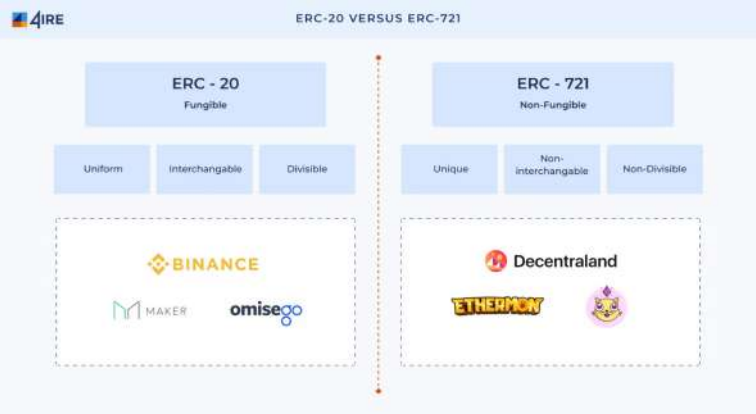


Figura 1.2. Confronto standard ERC-20 ed ERC-721. Immagine tratta da https://4irelabs.com/ .

Lo standard **ERC-20** presenta sei parametri obbligatori per ogni Smart Contract:

1. *totalSupply* massimo numero di token che possono essere creati;
2. *balance0f* assegna un numero iniziale di token a qualsiasi indirizzo specificato, solitamente i creatori del token;
3. *transfer* trasferisce i token a chi li acquista;
4. *transferFrom* invia token da una persona all'altra;
5. *approve* verifica che uno Smart Contract possa distribuire token, in base alla fornitura restante (verifica necessaria per eseguire 3);
6. *allowance* verifica che un indirizzo abbia un saldo sufficiente per inviare token ad un altro indirizzo (verifica necessaria per eseguire 4).

ERC-721 (Ethereum Request for Comments 721), proposto da William Entriken, Dieter Shirley, Jacob Evans e Nastassia Sachs nel gennaio 2018, è uno standard token non fungibile che implementa un'API per token all'interno di Smart Contract. sit [b]

Lo standard ERC-721 fornisce funzionalità di base per il tracciamento e il trasferimento di NFT. de Figueiredo Novo

Ad esempio per il trasferimento di token da un account a un altro, la richiesta del saldo corrente di token di un account, del proprietario di un token specifico e anche la quantità totale di token disponibili sulla rete. Oltre a questo ha anche altre funzionalità, come la

possibilità di approvare che una quantità di token di un account possa essere spostata da un account terzo.

Se uno Smart Contract implementa i seguenti metodi ed eventi può essere chiamato contratto token non fungibile ERC-721 e, una volta distribuito, sarà responsabile di tenere traccia dei token creati su Ethereum.sit [b]

Standard ERC-1155

Per completezza si cita anche un terzo standard, più recente e generale dei primi due descritti: ERC-1155.

Una criticità di ERC-721 è che prevede la scrittura di uno Smart Contract per ogni token, rappresentando quindi una soluzione semplice, ma non molto funzionale. Un ulteriore passo avanti è stato lo standard ERC-1155 che rappresenta una generalizzazione e semplificazione dello stardard ERC-721.

ERC-1155 prevede invece un solo Smart Contract che contiene i dati di configurazione di tutti i token, andando così a semplificare e ridurre il numero di transazioni necessarie per scambiarli tra diversi utenti. Con questo standard è possibile creare sia FT che NFT.

1.2.3 Token

Un token (gettone) rappresenta un valore o un diritto ed è nella sostanza come una moneta virtuale con un utilizzo specifico. La parola token viene usata per significati diversi:

- Utility token: danno diritto all'utilizzo di alcune features su una piattaforma,oppure a benefici o servizi premium;
- Security token: danno diritto di partecipazione al profitto della piattaforma che li ha emessi;
- Payment token (coin): criptomonete.

I tokend fungibili (FT) rappresentano diverse quantità di identiche (fungibili) risorse e sono spesso impiegati per l'implementazione di criptovalute su Ethereum. I token non fungibili (NFT) a loro volta possono rappresentare la proprietà di diversi tipi di beni distinti, ad esempio la proprietà fisica come case o opere d'arte uniche, o oggetti da collezione come animali domestici virtuali o carte da gioco. de Figueiredo Novo

Fungible token

Token significa letteralmente "gettone" e, in ambito blockchain, il termine era strettamente legato al concetto di ICO (Initial Coin Offering), sistema di raccolta fondi non regolamentato per nuove criptovalute, assimilabile all'OPA (Offerta Pubblica di Acquisto) che è invece regolamentata. La prima ICO per il lancio della criptovaluta Mastercoin è del 2013.

Nel 2014 si utilizzò il sistema per raccogliere fondi per Ethereum. Tuttavia, come la blockchain è una tecnologia che si è andata sempre più allontanando dalle criptovalute, anche il significato di token è nel corso del tempo mutato. Oggi definisce un insieme di

informazioni digitali che conferiscono un diritto di proprietà a un soggetto all'interno di una blockchain. Il token può contenere altri diritti e il loro insieme viene governato da Smart Contract.

Esistono oggi diverse tipologie di token in base al diverso approccio tecnologico o all'utilizzo cui sono destinati e non ne esiste attualmente una classificazione standard condivisa. Il team di Untitled INC (network nato nel 2001 che riunisce vari esperti di blockchain) ha presentato nel gennaio 2018 un'ipotesi di classificazione. sit [c]

Non-fungible token

Il non-fungible token (NFT) è un tipo di criptovaluta derivato da Smart Contract di Ethereum. Esso è utilizzato per identificare inequivocabilmente qualcosa o qualcuno. sit [b]

Figura 1.3. Icona NFT tratta da Wikipedia.com .

In generale, sono beni fungibili quelli che possono essere replicati e quindi sostituiti con altri di pari valore. Per esempio una banconota (due banconote da 10 Euro hanno identico valore), una lattina di una bevanda commerciale o uno smartphone nuovo ecc.. Sono beni infungibili quelli che non possono essere replicati in quanto unici. Per esempio un appartamento, un terreno o un'opera d'arte. Gli NFT cercano di replicare nel mondo del digitale ciò che sono i beni infungibili nel mondo reale. sit [a] Questo tipo di token trova la sua utilità su piattaforme che offrono oggetti collezionabili, chiavi di accesso, biglietti della lotteria, posti numerati per concerti o eventi sportivi ecc. sit [b]

Gli NFT si differenziano dagli Smart Contract perché questi ultimi sono dei veri e propri programmi che implementano un contratto mentre gli NFT sono dei token (cioè dei gettoni) di cui si può attestare l'unicità e la proprietà.

La differenza non è quindi nell'unicità ma nella natura dell'oggetto. Gli NFT si possono applicare alle opere artistiche di natura digitale, attestandone l'autenticità e la proprietà. sit [a]

NFT è unico e non può essere scambiato come per simile (equivalentemente, non fungibile), rendendolo adatto per identificare qualcosa o qualcuno in un modo unico.

Utilizzando NFT su Smart Contract (in Ethereum) un creatore può facilmente dimostrarne l'esistenza e la proprietà di risorse digitali sotto forma di video, immagini, arti, eventi biglietti, ecc. Inoltre, il creatore può anche guadagnare royalties ogni volta di un commercio di successo su qualsiasi mercato NFT o tramite scambio peer-to-peer.

Storia completa, commerciabilità, ampia liquidità e comoda interpretabilità consentono a NFT di diventare una promettente soluzione di protezione della proprietà intellettuale (IP). Sebbene essenzialmente gli NFT rappresentano poco più di un codice, essi proteggono bene i prezzi di vendita di questi prodotti relativi alla PI.

Capitolo 2

Standard ERC-721

ERC-721 introduce uno standard per NFT, questo tipo di token è unico e può avere un valore diverso rispetto ad un altro token dello stesso Smart Contract, dovuto all'età, alla rarità o ad altro.

2.1 Codice ERC-721

ERC-721 (Ethereum Request for Comments 721), proposto da William Entriken, Dieter Shirley, Jacob Evans e Nastassia Sachs nel gennaio 2018, è uno standard token non fungibile che implementa un'API per token all'interno di Smart Contract.

Fornisce funzionalità per il trasferimento di token da un account a un altro, la richiesta del saldo corrente di token account, del proprietario di un token specifico e anche la quantità totale di token disponibili sulla rete. Oltre a queste ha la possibilità di approvare che una quantità di token di un account possa essere spostata da un account terzo.

Se uno Smart Contract implementa i precedenti metodi ed eventi può essere chiamato contratto token non fungibile ERC-721 e, una volta distribuito, sarà responsabile di tenere traccia dei token creati su Ethereum. eth

Un'interfaccia standard consente alle applicazioni di wallet/broker/asta di funzionare con qualsiasi NFT su Ethereum. Questo standard si ispira allo standard dei token ERC-20 e si basa su due anni di esperienza dalla creazione di EIP-20.

L'EIP-20 non è sufficiente per tracciare gli NFT perché ogni asset è distinto (non fungibile) mentre ciascuno di una quantità di token è identico (fungibile).

2.1.1 Analisi del codice

Per procedere con l'analisi del codice è opportuno introdurre l'NFT identifier. Ogni NFT è identificato da un ID uint256 univoco all'interno dello Smart Contract ERC-721, tale numero identificativo non deve variare per la durata del contratto. La coppia (indirizzo del contratto, uint256 tokenId) è un identificatore globale unico e completo per un asset

specifico su una catena Ethereum. Mentre alcuni Smart Contract ERC-721 possono trovare conveniente iniziare con ID 0 e semplicemente incrementarli di uno per ogni nuovo NFT, i chiamanti non devono presumere che i numeri ID abbiano uno schema specifico per loro e devono trattare l'ID come un elemento sconosciuto.

Inoltre gli NFT possono diventare non validi (ovvero distrutti).

Presentazione del codice di EIP-721: eip

- `balanceOf(proprietario indirizzo) → uint256 balance {`

  ```
  require(_owner != address(0), ZERO_ADDRESS);
  return _getOwnerNFTCount(_owner);
  }
  ```

  Restituisce il numero di NFT nell'account del proprietario.

- `ownerOf(uint256 tokenId) {`

  ```
  _owner = idToOwner[_tokenId];
  require(_owner != address(0), NOT_VALID_NFT);
  }
  ```

  Restituisce il proprietario dell'NFT specificato da tokenId.

- `safeTransferFrom(address from, address to, uint256 tokenId){`

  ```
  require(_isApprovedOrOwner(_msgSender(), tokenId))
  _safeTransfer(from, to, tokenId, _data);
  }
  ```

  Trasferisce uno specifico NFT (tokenId) da un account a un altro. 'from' e 'to' non possono essere zero. tokenId deve essere di proprietà del chiamante. Se il chiamante è diverso da 'from', deve essere stato autorizzato a spostare questo NFT dalla funzione approve o setApprovalForAll.

- `transferFrom(address from, address to, uint256 tokenId) {`

  ```
  address tokenOwner = idToOwner[_tokenId];
  require(tokenOwner == _from, NOT_OWNER);
  require(_to != address(0), ZERO_ADDRESS);
  _transfer(_to, _tokenId);
  }
  ```

  Trasferisce uno specifico NFT (tokenId) da un account a un altro. Se il chiamante è diverso da 'from', deve essere stato autorizzato a spostare questo NFT dalla funzione approve o setApprovalForAll.

- `approve(address to, uint256 tokenId) {`

  ```
  address tokenOwner =  idToOwner[_tokenId];
  require(_approved != tokenOwner, IS_OWNER);
  idToApproval[_tokenId] = _approved;
  emit Approval(tokenOwner, _approved, _tokenId);
  }
  ```

Questo evento viene attivato quando un utente approva un altro utente ad assumere la proprietà del token, ovvero viene attivato ogni volta che viene eseguita la funzione di approvazione. Emette le informazioni su quale account possiede attualmente il token, quale account è autorizzato ad assumere la proprietà del token in futuro e quale token (per ID) è autorizzato a trasferire la sua proprietà.

- ```
  getApproved(uint256 tokenId) → address operator {
   return idToApproval[_tokenId];
  }
  ```

  Restituisce l'indirizzo approvato per un ID token o zero se non è impostato alcun indirizzo.

- ```
  setApprovalForAll(address operator, bool approved) {
   ownerToOperators[msg.sender][_operator] = _approved;
   emit ApprovalForAll(msg.sender, _operator, _approved);
  }
  ```

  Attiva o disattiva l'approvazione di un determinato operatore. Un operatore può trasferire tutti i token del mittente per suo conto.

- ```
  isApprovedForAll(address owner, address operator) → returns (bool){
   return ownerToOperators[_owner][_operator];
  }
  ```

  Indica se un operatore è approvato da un determinato proprietario. I parametri sono _owner overo l'indirizzo che possiede gli NFT ed _operator l'indirizzo che agisce per conto del proprietario.

- ```
  safeTransferFrom(address from, address to, uint256 tokenId, by-
  tes data) {
   address tokenOwner = idToOwner[_tokenId];
   require(tokenOwner == _from, NOT_OWNER);
   require(_to != address(0), ZERO_ADDRESS);
   _transfer(_to, _tokenId);
   if (_to.isContract()) {
    bytes4 retval = ERC721TokenReceiver(_to).onERC721Received(msg.sender,
  _from, _tokenId, _data);
    require(retval == MAGIC_ON_ERC721_RECEIVED, NOT_ABLE_TO_RECEIVE_NFT);
   }
  }
  ```

  Trasferisce in modo sicuro la proprietà di un determinato token ID a un altro indirizzo Se l'indirizzo di destinazione è un contratto, deve implementare IERC721Receiver; in caso contrario, il trasferimento viene annullato. Richiede che msg.sender sia il proprietario, o che abbia l'approvazione.

- ```
  Transfer(address from, address to, uint256 tokenId) {
   address from = idToOwner[_tokenId];
  ```
  ```

```
 _clearApproval(_tokenId);
 _removeNFToken(from, _tokenId);
 _addNFToken(_to, _tokenId);
 emit Transfer(from, _to, _tokenId);
}
```

Questo evento viene attivato quando la proprietà del token cambia da un individuo all'altro. Emette le informazioni su quale account ha trasferito il token, quale account ha ricevuto il token e quale token (per ID) è stato trasferito.

- `Approval(address owner, address approved, uint256 tokenId)`
  Viene emesso quando viene modificato l'indirizzo approvato per un NFT.
- `ApprovalForAll(address owner, address operator, bool approved)`
  Viene emesso quando un operatore è abilitato o disabilitato per un proprietario. L'operatore può gestire tutte le NFT del proprietario.

In Solidity gli eventi sono segnali inviati che possono essere attivati dagli Smart Contract. Le dApp, o altri elementi connessi all'API JSON-RPC di Ethereum, possono attendere questi eventi e agire di conseguenza. Gli eventi sono anche indicizzabili, in modo che la cronologia dell'evento sia ricercabile in seguito.

2.2 ERC-1155

ERC-1155 è uno standard di token nella blockchain di Ethereum che facilita la creazione di tipi di token sia fungibili che non fungibili. L'obiettivo è creare un'interfaccia di Smart Contract che possa rappresentare entrambi i tipi, infatti è chiamato standard multi-token. Lo standard ERC-1155 ha le stesse funzionalità di un token ERC-721 e ERC-20, ma ne migliora la funzionalità ed in generale risulta più efficiente. Le transazioni che utilizzano lo standard ERC-1155 possono essere raggruppate per aiutare a ridurre il costo del trading di token, questo rappresenta uno dei vantaggi del nuovo modello.

ERC-1155 presenta i seguenti vantaggi:

- Trasferimento effettivo: Lo standard ERC-1155 consente agli utenti di effettuare massicci trasferimenti di token in modo nativo su uno Smart Contract. In uno Smart Contract con una serie di token fungibili o non fungibili, uno sviluppatore può scegliere di trasferire più token nella stessa operazione. Questo non solo riduce i costi di transazione, ma riduce anche l'impatto sulla rete.
- Più token in un unico contratto: ogni token ERC-1155 descrive l'esistenza e il funzionamento di tipi di token fungibili e non fungibili. Ad esempio, mentre un ERC-1155 può creare uno o più NFT, può anche descrivere token fungibili, tutti all'interno dello stesso contratto.
- Trasferimento sicuro del token: il modello di token ERC-1155 include una funzione che controlla se una transazione è valida o meno. Se una transazione non viene completata, questa funzione restituisce il token all'emittente. Questo è di rilievo

quando gli utenti commettono accidentalmente un errore nella trascrizione o inviano token all'indirizzo sbagliato. Il codice può invertire automaticamente la transazione.

2.2.1 ERC-721 vs ERC-1155: la differenza

Lo standard ERC-721 produce esclusivamente NFT e costringe gli sviluppatori a creare uno Smart Contract per ogni nuovo token. D'altra parte, l'ERC-1155 consente di sviluppare un singolo Smart Contract che può essere utilizzato per coniare token fungibili o NFT.

Poiché ERC-721 consente una singola operazione per ogni transazione, è costoso sia a livello computazionale che temporale; inoltre riduce l'efficacia della rete blockchain con codice ridondante.

ERC-1155, invece, consente più operazioni in una singola transazione che risulta più economica ed efficiente. Inoltre ERC-1155 utilizza meno spazio di archiviazione su una rete blockchain.

Capitolo 3

Processo di creazione di un NFT

La coniazione di ogni Non-Fungible Token richiede il pagamento di una tassa per le emissioni di gas generate, per pagare le spese energetiche sostenute dalla Blockchain; questo rende la creazione di NFT non accessibile a tutti.

Tuttavia, esistono piattaforme in grado di facilitare il processo.

3.1 Operazione di mint

Quando si parla di 'mint' di un NFT ci si riferisce al processo di creazione, quindi al suo inserimento all'interno di una determinata Blockchain.

Durante questo processo si converte un file digitale, che può essere un'immagine, un file musicale o un qualsiasi altro file, in un non-fungible token (NFT) che vive su una Blockchain e quindi è protetto e immutabile.

Per *mintare* un NFT è necessario collegare il proprio wallet, ed assicurarsi che detenga il corrispettivo di criptovalute necessarie all'operazione di minting, poiché il processo richiede della computazione da parte dei nodi della rete Blockchain, e ciò ha un costo, le gas fees.

Questo costo dipende da quanto è impegnata la rete di Miner che devono "scrivere" le operazioni sul registro della Blockchain. In alcuni momenti di grande attività, questa commissione potrebbe essere anche molto elevata, quindi, se è possibile, è meglio aspettare quando la rete sarà meno congestionata.

Quando si *minta* un proprio NFT è opportuno specificare le royalties, ovvero la percentuale sul prezzo di vendita che si percepirà ogni volta che l'NFT verrà rivenduto (tutte le vendite successive alla prima), al contrario se si *minta* un NFT di un progetto creato da terzi, si avrà la proprietà del bene e si potrà beneficiare di tutte le utilities del progetto, ma le royalties delle vendite successive andranno ai creatori del progetto.

Ogni progetto può avere utilities differenti, che possono essere nella vita reale, nel Metaverso, nel mondo del gaming o è semplicemente un pezzo da collezione; in ogni caso gli utenti possono decidere di vendere nuovamente gli NFT *mintati* su marketplace secondari come Opensea ad un prezzo maggiore rispetto a quello pagato in fase di mint.

La Blockchain più famosa per gli NFT è sicuramente Ethereum, dove le gas fees sono relativamente alte, mentre su altre Blockchain, come Polygon o Solana abbiamo gas fees molto minori, in alcuni casi quasi inesistenti.

3.1.1 Buy e mint a confronto

L'acquisto di un NFT è molto più comune del mint, poiché risulta essere un'operazione più semplice in quanto basta procedere alla transazione dell'acquisto su uno dei Marketplaces dove l'NFT è listato (messo in vendita a un prezzo fisso o ad un'asta). Una volta terminato l'acquisto, l'NFT verrà trasferito e si potrà vedere all'interno del wallet dell'acquirente.

Successivamente si potrebbe vendere l'NFT ad altri potenziali utenti in profitto o in perdita.

Quando si sceglie di acquistare un NFT come investimento, è opportuno stimare il potenziale rischio a cui ci si espone.

L'acquisto di un NFT dà maggiori garanzie, in quanto si può valutare se acquistare o meno in base alla tendenza di mercato del momento e al prezzo di resell successivo. Al contrario, il mint di un NFT creerà un situazione più rischiosa, in alcuni casi, in quanto non si può fare una scelta analizzando il mercato del progetto, in quanto è appena agli inizi.

Un altro aspetto da considerare, però, è che il prezzo di mint, nel caso in cui il progetto successivamente aumenti di valore, è sicuramente più economico di un eventuale acquisto al mercato secondario, dopo che ha già subito un aumento di prezzo.

3.2 Come creare un NFT su OpenSea

Il primo passaggio, per poter creare un NFT all'interno del marketplace OpenSea, è collegarsi a quest'ultimo utilizzando un browser che abbia l'estensione di MetaMask installata.

Successivamente è sufficiente collegare il proprio account MetaMask al dominio di OpenSea.

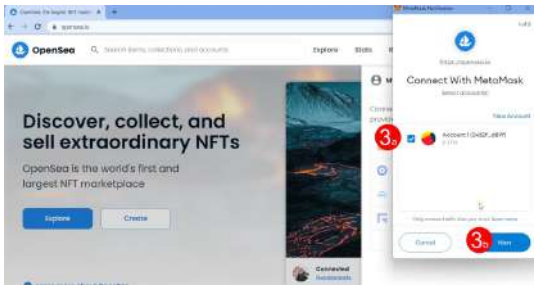


Figura 3.1. Collegamento di Metamask ad OpenSea.

Una volta fatto ciò, OpenSea genererà in automatico un account sulla piattaforma collegato all'Address del wallet MetaMask. Ora si ha il necessario per creare il proprio NFT nei seguenti passi:

1. Caricare un file per creare l'NFT (la dimensione massima su OpenSea è 100 MB)

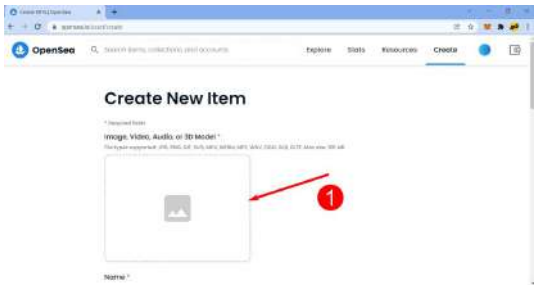


Figura 3.2. Schermata per il caricamento del file.

2. Scrivere il nome del NFT, ovvero il titolo dell'opera, è possibile referenziare quest'ultima con un link a una pagina esterna (per esempio al dettaglio dell'opera in un sito esterno). Opzionalmente è possibile aggiungere dei campi descrittivi dell'opera.

3. È possibile scegliere la collezione di cui l'NFT fa parte, se la si è creata il precedenza, nel caso l'utenza sia alla prima creazione, invece, la scelta della collezione non sarà disponibile.

4. È inoltre possibile inserire del contenuto sbloccabile. Sostanzialmente un contenuto che può essere visualizzato solo da chi possiede l'opera.

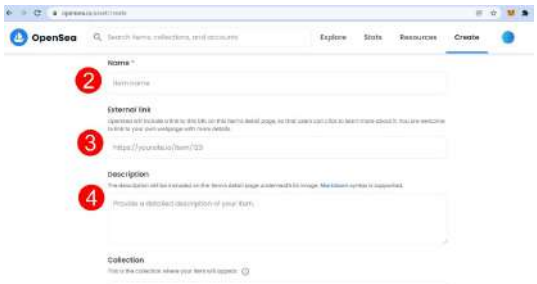


Figura 3.3. Schermata degli attributi dell'NFT.

5. Nella sezione Properties è possibile inserire i metadata dell'NFT che si sta generando, quindi gli attributi che permetteranno in seguito di definire la rarità del pezzo all'interno dell'intera collezione. Un NFT che possiede un attributo poco comune all'interno della totalità dei pezzi di una collezione, sarà sicuramente molto più raro di altri che hanno solo attributi comuni.

Figura 3.4. Bored Ape Yacht Club #1459. Tratta da https://opensea.io/.

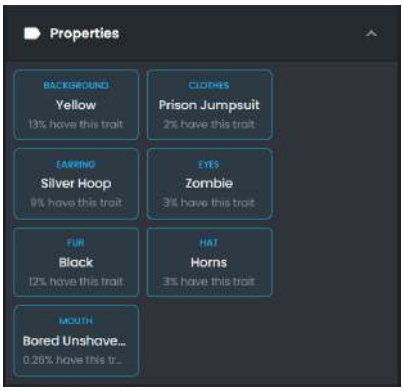


Figura 3.5. Properties Bored Ape Yacht Club #1459. Tratta da https://opensea.io/.

6. Scegliere la blockchain nella quale si desidera generare l'NFT, è possibile scegliere tra Ethereum e Polygon (Matic), questa scelta influirà sui costi futuri, poiché per mettere in vendita un NFT su rete Ethereum si pagano delle gas fees, mentre la rete Polygon Matic prevede commissioni quasi nulle. (Fig.3.6)

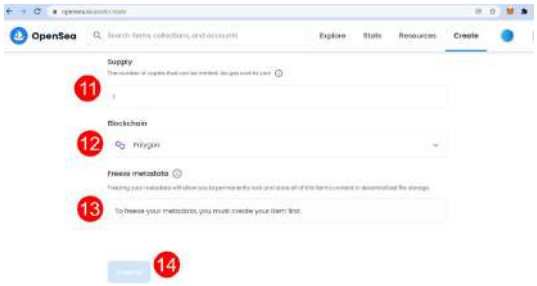


Figura 3.6. Scelta della blockchain.

7. Una volta fatto ciò, il pulsante "Create" genererà l'NFT. (Fig.3.7)

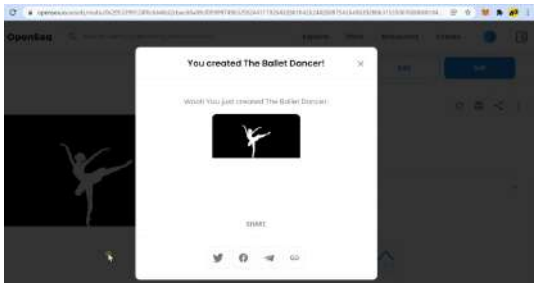


Figura 3.7. Creazione dell'NFT.

Capitolo 4

Analisi di mercato

4.1 Marketplace

I Marketplace per NFT sono piattaforme nate con lo scopo di facilitarne l'acquisto e la vendita.

Ad ogni NFT viene attribuito un valore dal creatore, in fase di Mint e successivamente dai futuri proprietari, che possono decidere di venderlo a prezzo fisso, con la possibilità di accettare offerte a ribasso, o tramite un'asta virtuale.

Solitamente Marketplace diversi si concentrano su categorie di NFT differenti: Sit [e]

- **Arte Generativa.**
- **PFP (Profile-picture projects) o Avatar.**
- **Arte 1/1.**
- **Gaming.**
- **Fotografia.**
- **Collezionabili.**
- **Musica.**
- **Wearable digitali e Asset virtuali.**

Tra i Marketplace più importanti possiamo trovare Rarible, SuperRare, Foundation, Mintable e OpenSea, il Marketplace più utilizzato a livello globale con più di 80 milioni di NFT nella sua vetrina. Sit [c]

In queste piattaforme non ci sono delle entità centrali o intermediari per far avvenire le transazioni, consentendo agli utenti di concludere compere e vendite mettendosi d'accordo in modo diretto; l'unica cosa di cui hanno bisogno è un wallet Ethereum, ad esempio MetaMask.

Una proprietà molto importante da considerare, e che i Marketplace mostrano direttamente nella pagina di ogni NFT, è il resoconto totale delle attività di quel singolo NFT,

dalla data di mint. In questo modo si possono rivedere tutti i proprietari passati, eventuali trasferimenti, le offerte che ci sono state e i prezzi ai quali è stato venduto.

Queste informazioni direttamente sulla pagina del Marketplace riducono notevolmente gli sforzi per verificare se un NFT è originale o un duplicato e consentono di analizzare il totale andamento del prezzo nel tempo. De-Rong Kong [2021]

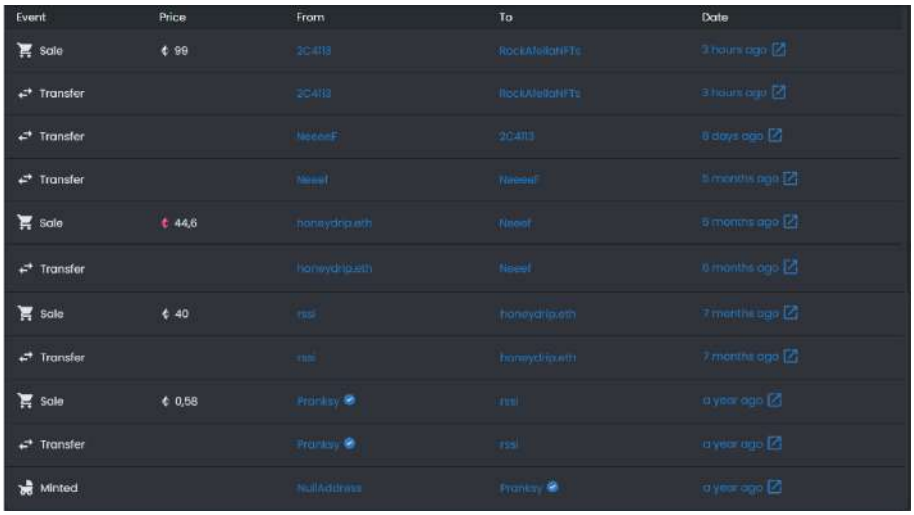


Figura 4.1. Attività Bored Ape Yacht Club #5884. Tratta da https://opensea.io/.

In Figura 4.1 si può vedere l'intera attività per l'NFT #5884 della collezione "Bored Ape Yacht Club", dalla data di mint, un anno fa, ad oggi.

Si nota una prima vendita a 0.58 ETH poco dopo il mint e poi 2 vendite nei mesi successivi, rispettivamente a 40 ETH e a 44.6 ETH, ed oggi (14/05/2022), a distanza di un anno, una vendita a 99 ETH.

Gli eventuali trasferimenti non legati ad una vendita potrebbero essere motivati come spostamenti dell'NFT da un "hot-wallet" ad un "cold-wallet" per aumentarne la sicurezza.

4.2 Performance di mercato

4.2.1 Paesi interessati

L'interesse per gli NFT è esploso negli ultimi anni a livello globale, dando l'opportunità al mercato finanziario di espandersi verso il mondo digitale attraverso la nuova tecnologia BlockChain 2.0.

Secondo una ricerca sul numero di ricerche per il termine "NFT" su Google, i Paesi che manifestano maggior interesse a questa innovazione sono quelli orientali, cosa non sorprendente, in quanto sono anche ai primi posti per quanto riguarda altri argomenti correlati, ad esempio criptovalute, BlockChain e Bitcoin. Sit [d]

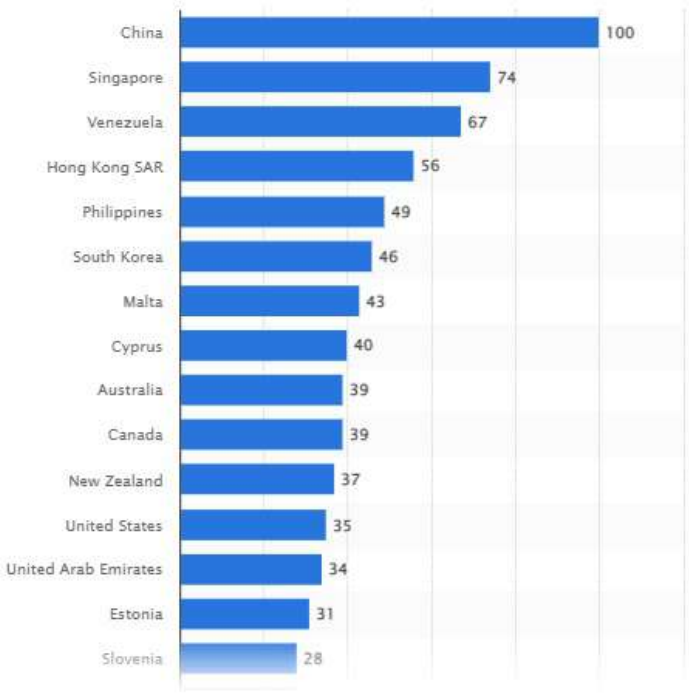


Figura 4.2. Classifica Paesi. Tratta da https://findstack.com/nft-statistics/ .

4.2.2 Andamento recente

Secondo i dati riportarti da NonFungible.com Sit [a], si possono analizzare alcuni parametri relativi all'andamento degli NFT negli ultimi anni in Figura 4.3.

In generale dal 2019 al 2021 il mercato è aumentato considerevolmente: da 1,6 milioni di vendite registrate nel 2019, è passato a circa 27 milioni nel 2021.

Il prezzo medio di vendita è passato da 15 dollari a circa 800 dollari generando un incremento del volume di dollari scambiati, da 24 milioni nel 2019 a circa 17,5 miliardi nel 2021.

	2019	2020	2021
Volume of dollars traded	$24,532,783	$82,492,916 +236%	$17,694,851,721 +21,350%
Volume of sales	1,619,516	1,415,638 -13%	27,414,477 +1,836%
Buyers	44,324	75,144 +70%	2,301,544 +2,962%
Sellers	25,036	31,774 +27%	1,197,796 +3,669%
Total active wallets	55,330	89,061 +61%	2,574,302 +1,822%
Total profit (when reselling)	$2,890,230	$12,074,654 +317.77%	$5,407,158,315 +44,681%
Total losses (when reselling)	$1,372,663	$1,990,198 +44.99%	$667,191,955 +33,423%
Average number of transactions	2.0	1.9 -5%	1.8 -5.26%
Average length of ownership	84	156 +85.71%	48 -69.23%
Market capitalisation	$123,999,573	$372,203,300 +200%	$16,898,362,987 +4,440%
Number of active Smart Contracts	988	2,001 +103%	10,017 +401%
Average price	$15.17	$49.18 +224%	$807.52 +1,542%

Figura 4.3. Andamento del mercato NFT dal 2019 al 2021. Tratta da Sit [a] .

Già nel 2020 si riscontra un leggero aumento, ma è nella fine del 2021 che il mercato è in pieno "boom", supportato anche dall'ingresso di alcuni clienti, come Nike, Louis Vuitton e Samsung.

Il numero di Smart Contract attivi, corrispondente al numero di progetti attivi, è aumentato, ma più modestamente rispetto all'incremento di compratori e wallet e questo ha comportato un forte aumento dei prezzi.

Altri dati interessanti sono il numero di profitti e il numero di perdite.

I profitti nella tabella sono da intendere come il volume totale cumulativo che gli utenti hanno guadagnato rivendendo i beni acquistati al mercato secondario (quindi differenza tra il prezzo di acquisto e il prezzo di rivendita).

Si può notare però che l'aumento dei profitti è accompagnato da un aumento delle perdite, in quanto essendoci molti nuovi progetti ogni giorno, molti di essi si rivelano dei progetti "scam" o semplicemente non riescono a "partire" al meglio nel breve periodo e quindi gli investitori che hanno comprato a mercato primario, rivendono a mercato

secondario a un prezzo inferiore, cercando di recuperare almeno in parte la cifra investita, andando a generare una perdita. Sit [a]

4.2.3 Mercato Primario e Secondario

Per apprendere l'andamento del mercato degli NFT in questi ultimi mesi si può far un confronto tra mercato primario, dove si acquista al momento dell'emissione e mercato secondario, dove si acquista da un rivenditore, con un eventuale aumento di prezzo.

In Figura 4.4 e 4.5 si può vedere rispettivamente il volume in dollari e vendite in confronto tra il mercato primario e secondario, considerando come lasso temporale l'ultimo quadrimestre del 2021 e il primo trimestre del 2022. Sit [b]

Figura 4.4. Volume di dollari scambiati in confronto tra mercato primario e secondario. Tratta da Sit [b].

Figura 4.5. Volume di vendite in confronto tra mercato primario e secondario. Tratta da Sit [b].

Si può notare che il valore in dollari in circolazione e il volume di vendite del mercato secondario sono nettamente superiori a quelli del mercato primario.

La grande produzione durante tutto il 2021, però, ha rallentamento in questo primo trimestre del 2022, che si può considerare come una fase di post-saturazione del mercato.

4.2.4 Relazione NFT e Criptovalute

I Marketplace NFT al loro interno utilizzano criptovalute, solitamente Ether (ETH) come mezzo di pagamento, evidenziando una stretta relazione tra il mercato delle criptovalute e quello degli NFT, in quanto un utente per acquistare un NFT deve prima acquistare delle criptovalute.

Il mercato delle criptovalute, quindi ha un impatto notevole sul mercato dei NFT.

A questo proposito si può fare un confronto sull'andamento dei prezzi di Bitcoin (ETH) e Ether (ETH) rispetto al numero di wallets attivi che posseggono NFT e alle loro vendite, dal 2018 alla prima metà del 2021 (Fig.4.6).

Sulla Blockchain di Bitcoin non esistono gli NFT, ma è giusto considerarlo nell'analisi, in quanto essendo il leader nel campo delle criptovalute, il suo andamento influenza l'andamento di tutte le altre criptovalute.

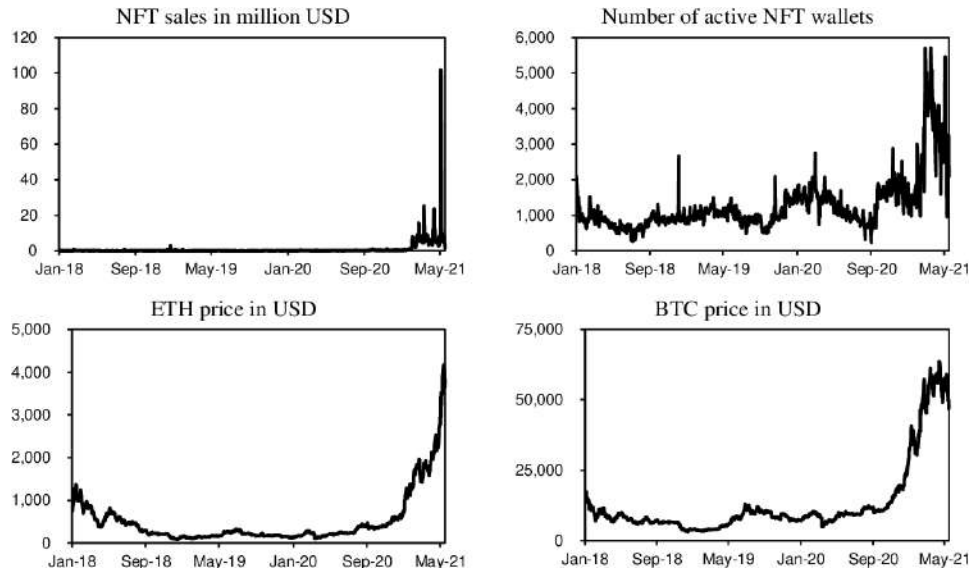


Figura 4.6. Immagine tratta da Ante [2021] .

Quindi dalla Fig.4.6 si può notare che i prezzi di BTC ed ETH influiscono sul mercato NFT, mentre il mercato NFT non sembra influenzare in modo significativo il prezzo delle criptovalute.

Questo risultato era il più atteso, in quanto le criptovalute servono per l'acquisto e il trading di NFT e quindi un abbassamento del valore generale delle criptovalute significa un potere d'acquisto più basso, che rischia di deprimere il mercato NFT.

Caso opposto, invece, si ha quando il valore delle criptovalute tende a salire, in quanto gli investitori cercano investimenti alternativi, andando a favorire anche il mercato NFT.

Un altro fattore però, è da tenere in considerazione, in quanto un utente, che possiede un NFT, può scambiarlo o venderlo a se stesso in modo trasparente ma totalmente anonimo, in quando qualunque transazione è fatta tramite indirizzi pubblici, ma non riconducibili al medesimo individuo, della blockchain sulla quale vive l'NFT.

In questo modo, la domanda e il prezzo di vendita possono essere simulati e gonfiati con l'obiettivo di attirare futuri acquirenti. La legalità di comportamenti di questo genere, però, non è attualmente chiara.

Capitolo 5

Applicazioni e opportunità

Negli ultimi tempi, sta crescendo sempre più l'interesse e la curiosità sul tema NFT e si sta indagando sulle possibili applicazioni degli stessi in campi che vadano oltre il semplice collezionismo. In questo capitolo si descrivono le applicazioni di maggiore rilievo e le opportunità che tale mondo ha da offrire.Wang et al. [2021]

5.1 Crypto Art

Per Crypto Art si intende una qualsiasi forma d'arte che permetta di essere digitalizzata, sia essa un'opera fisica (un quadro, una canzone, una poesia, ecc.) o un oggetto già digitale di per sé. Massimo Franceschet [2019]

A ciascuna opera si associa il proprio NFT che è contenuto in una specifica Blockchain: ciò consente di avere un set di informazioni associate all'opera, tali da garantirne l'autenticità e il diritto di proprietà per chi la acquisterà. Nella Blockchain, quindi, non è contenuto il file vero e proprio dell'opera, ma la sua orma, rappresentata dal NFT, il quale possiede al suo interno i metadata del file prodotto dall'artista.

Il primo NFT ad essere elencato in una delle principali case d'asta di Christie's è stato quello relativo all'opera "Everydays: the First 5000 Days" (Figura 5.1), dell'artista noto come Beeple. Nel 2021 tale opera è stata venduta per 69.3 milioni di dollari partendo da una base d'asta di 100 dollari ed è un collage delle prime 5000 opere della serie "Everydays" prodotta dall'artista stesso. Soldavini [2021]

Nel sito di Christie's ancora oggi si può vedere come fu proposta l'opera:

Beeple (b. 1981)
EVERYDAYS: THE FIRST 5000 DAYS
token ID: 40913
wallet address: 0xc6b0562605D35eE710138402B878ffe6F2E23807
smart contract address: 0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756
non-fungible token (jpg)
21,069 x 21,069 pixels (319,168,313 bytes)
Minted on 16 February 2021. This work is unique.

Si possono osservare due hash: uno relativo all'indirizzo del wallet che ha creato (mintato/coniato) l'opera e l'altro corrispondente allo smart contract sul quale è stato creato il NFT, seguendo le norme stabilite dallo smart contract stesso.

Ovviamente tale opera non è il primo NFT di sempre, tuttavia può essere considerato il primo di successo.

L'aspetto principale che mise in luce tale evento fu quello della vendita dell'autentica opera digitale e quindi del passaggio della stessa dal proprietario all'acquirente. L'opera è disponibile per tutti online, ma esiste un proprietario che è colui che ha "l'originale", ovvero l'unico che possiede il NFT associato all'immagine. Egli da una parte può dimostrare a tutti di possedere effettivamente l'opera, dall'altra può essere certo lui stesso di possederne l'originale.

Figura 5.1. Everydays: the First 5000 Days - Beeple, 2021.

5.1.1 Crypto Art come movimento artistico

Prima della messa all'asta dell'opera di Beeple, la Crypto Art aveva già avuto modo di esprimersi e di affermarsi come un vero e proprio movimento artistico. La sua data di nascita può essere considerata il 13 gennaio 2018, quando a New York si svolse la prima mostra "Rare Digital Art Festival", dove ovviamente per acquistare una data opera

era necessario comprarne il NFT. Come ogni movimento artistico gran parte delle opere hanno caratteristiche comuni, seppure ovviamente ci sia estrema libertà nella creazione. In particolare Jason Bailey, nel suo articolo "What is Crypto Art?" (Bailey [2018]), redatto in seguito alla visita alla Rare Digital Art Festival, fornisce dei tratti che ricorrevano nei primi NFT proposti.

Tra i tanti descritti da Bailey spiccano i seguenti:

- Ha come soggetti spesso i cosiddetti 'meme', le famose immagini con scritte in evidenza, note per essere molto impiegate nei social e per la loro viralità. Questo fattore ha certamente inciso nel successo iniziale della Crypto Art e la famosa rana Pepe ne è un esempio (Figura 5.2).
- Molti artisti nella Crypto Art desiderano rimanere anonimi. Dal momento che i NFT vengono venduti su Blockchain, un'artista può decidere di rimanere anonimo e nascondersi dietro all' indirizzo pubblico.
- Chiunque può proporre la propria opera d'arte a prescindere da abilità, formazione, classe, genere, razza, età, credo, etc.

Figura 5.2. PEPEPOPE - Pepeboost, 2016. Di tale NFT ne esistono 48 esemplari, ciascuno con il proprio numero di serie in modo tale da garantirne l'unicità. Il valore medio attuale per NFT associato a tale opera è l'equivalente di circa 12 BTC.

5.1.2 Violazioni di copyright

Come è stato sottolineato, l'opera associata ad un NFT non è replicabile, cioè non è possibile copiarne il NFT. Tuttavia è ancora possibile in qualche modo proporre sul mercato un'opera simile ad un'altra, associata ad un diverso NFT. Attualmente, nei principali

marketplace per NFTs (come Opensea o Coinbase), non esiste un modo completamente automatizzato per controllare la violazione di copyright da parte di un NFT. Basti pensare al gran numero di cloni creati a partire da una delle prime collezioni di NFT come CryptoPunks.

Figura 5.3. Schermata di Opensea relativa a CryptoPunks

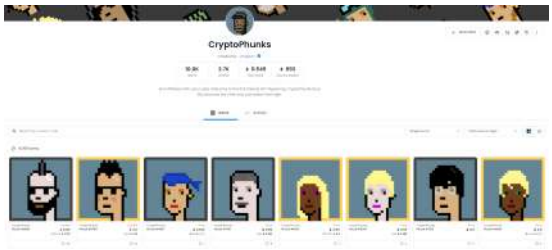


Figura 5.4. Schermata di Opensea relativa a CryptoPhunks

CryptoPhunks, CryptoPhunk, PolygonPunks, sono solo alcuni dei progetti che hanno in qualche modo copiato in parte l'originario progetto CryptoPunks. La prima di queste in particolare copia sostanzialmente tutta la collezione di Cryptopunks: l'unico suo contributo è quello di specchiarne le immagini. Tuttavia, su Opensea, tutte queste collezioni sono attualmente disponibili.

Risulta naturale domandarsi fino a che punto è lecito copiare un progetto. In effetti non esiste una risposta in generale. Per tal motivo i marketplaces si affidano ad un proprio team di sicurezza che controlla regolarmente che non vengano violate le proprie politiche. In caso contrario le piattaforme si riservano la possibilità di rimuovere il NFT in questione. Ad esempio Opensea introduce il termine *fair use*, che gli utenti devono conoscere prima di creare un NFT (ope). In generale, per fair use si intende utilizzare un'opera protetta da copyright (come un libro, un film o un personaggio) in modo trasformativo per usi come commenti, critiche, istruzione o parodia.

Opensea in particolare suggerisce le seguenti domande, che il creator deve porsi in fase di creazione del NFT:

- Possiedi i diritti originali per tutti gli elementi del tuo lavoro?
- In caso negativo, l'utilizzo dell'opera protetta da copyright aggiunge una nuova espressione, un nuovo significato o un nuovo messaggio all'opera originale?
- L'utilizzo dell'opera protetta da copyright influisce negativamente sul valore o sui proprietari dell'opera originale?
- Hai l'autorizzazione scritta dal creatore originale per creare un NFT?
- Se stai modificando un NFT esistente (come CryptoPunks o BAYC), possiedi l'NFT originale nel tuo account?

Per quanto riguarda CryptoPhunks, il creator ha rispettato tutte queste condizioni e per tale motivo la sua collezione è ancora online.

5.2 Crypto Games

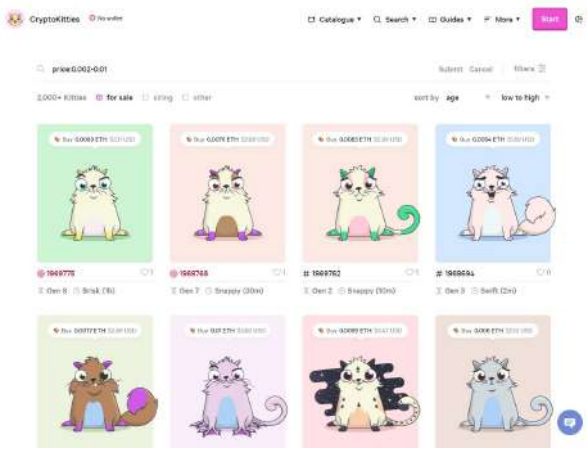


Figura 5.5. Sezione del sito di CryptoKitties relativa alla compravendita dei kitties.

I NFT offrono grandi possibilità anche all'industria relativa ai videogame. Negli ultimi anni hanno preso sempre più spazio giochi per cellulare, pc e console gratuiti ma con alcune feature a pagamento, i cosiddetti videogiochi *breeding* ('allevamento'). In essi i giocatori possono prendersi cura di animali virtuali, gestire aziende fittizie o altro, vivendo in un mondo dove anche altri utenti svolgono le stesse mansioni.

L'esempio più famoso nel mondo NFT è CryptoKitties, appartenente alla categoria dei *crypto game*, ovvero dei giochi che includono elementi appartenenti alla tecnologia Blockchain. In esso è possibile crescere il proprio gattino (associato ad un NFT), acquistato in fase di iscrizione, ma anche venderlo e comprarne di nuovi da altri utenti (Cry).

L'obiettivo del gioco quindi non è unicamente la crescita del proprio gattino, ma anche e soprattutto il trading sugli NFT relativi. D'altra parte si hanno anche altre possibilità permesse dalla Blockchain su cui si fonda il generico crypto game; un esempio può essere il fatto che ogni utente possieda la storia dei detentori dell'item acquistato. Ciò garantisce benefici sia ai creatori del gioco sia agli utenti: i primi infatti guadagnano royalties ogni volta che l'item da loro creato viene rivenduto da un utente all'altro, dall'altra l'utente entra in possesso di qualcosa di unico e quindi spesso soggetto a crescite di valore a causa della sua rarità. In tal modo entrambe le parti possono trarre profitto dal market secondario sulle NFT.

Inoltre, ad esempio relativamente a CryptoKitties, dal momento che il gioco si trova sulla Blockchain, ed è quindi decentralizzato, nulla potrà mai togliere ad un compratore di gattini, il proprio gattino. Infatti, seppure il sito ufficiale del gioco può essere chiuso o rompersi, il token relativo al gattino è salvato nel wallet del possessore su Ethereum e quindi non può essere rimosso.

5.2.1 Play-to-Earn game

Una particolare categoria di Crypto Game sono i cosiddetti *Play-to-Earn game*. Nei giochi blockchain meno recenti, i giocatori si affidano al caso per ottenere profitti: in CryptoKitties, ad esempio, il valore del gattino dipende dalla sua generazione, dagli attributi che possiede, dalla "bellezza" che altri utenti gli attestano, più in generale da fattori che non sono migliorabili attraverso un lavoro vero e proprio compiuto dall'utente. Il play-to-earn, invece, ha creato economie di gioco e modelli commerciali in cui i giocatori possono lavorare nel gioco per ottenere un reddito. Axie Infinity su Ethereum ne è un famoso esempio. Axie Infinity è una piattaforma che ospita NFT Axie, costruita sulla blockhain di Ethereum, e che può essere considerata una via di mezzo tra Pokèmon e Cryptokitties (Axi).

I token AXS possono essere scambiati, comprati o guadagnati all'interno del gioco. Per giocare, hai bisogno di 3 Axies (personaggi del gioco) per formare una squadra, il che potrebbe essere un ostacolo per alcuni utenti a causa del prezzo, poiché l'Axie più economico costa 0,03 ETH. Ovviamente ogni Axie è unico ed è associato ad un NFT che il giocatore possiede nel proprio wallet su Ethereum. Ciò che distingue tale gioco da CryptoKitties sono le sfide tra giocatori. Infatti in esse, il giocatore più abile a creare una squadra ben combinata, e quindi a battere l'avversario, può vincere token SLP (Smooth Love Potion), che sono token fungibili, il cui valore è ovviamente variabile.

Il collezionamento dei SLP, può avvenire anche all'infuori delle battaglie tra giocatori. Infatti nel gioco è possibile affrontare una modalità avventura e svolgere delle tasks quotidiane, grazie alle quali si possono guadagnare i suddetti token. In alternativa, si può guadagnare denaro allevando i propri NFT Axies e vendendoli sul mercato, proprio come descritto in precedenza.

Figura 5.6. Esempio di schermata di gioco di Axie Infinity

5.3 Crypto Tickets

Una delle opportunità offerte dalla Blockchain è la possibilità di raccogliere soldi in modo anonimo per un preciso scopo. Tuttavia, i NFT estendono enormemente tali confini della Blockcahin, imposti dalla natura fungibile delle criptomonete. I NFT permettono di

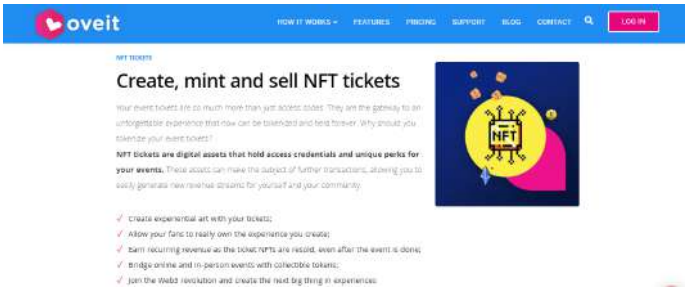


Figura 5.7. Screenshot preso da www.oveit.com.

collegare un preciso indirizzo ad un preciso evento come nella vita reale, ma sfruttando le garanzie assicurate dalla Blockchain.

Un esempio può essere la compravendita di biglietti per degli eventi. In generale, quando si acquistano tradizionalmente biglietti per un qualsiasi evento, a meno che non si acquisti direttamente da chi propone l'evento, è necessario che i clienti si fidino di terze parti. Tuttavia, da sempre è presente il rischio di essere truffati, comprando biglietti contraffatti, scaduti o cancellati. Inoltre un biglietto potrebbe essere venduto più volte, ad esempio estraendo il codice dello stesso da una foto postata online da parte di un incauto cliente.

I biglietti basati su NFT consentono di superare questi problemi. Infatti un biglietto è unico e non può avvenire il "double selling", ovvero non può essere venduto lo stesso biglietto a due utenti distinti. Inoltre si garantisce l'anonimicità dell'acquirente, che in generale potrebbe non essere concessa da una generica piattaforma. Non solo: oltre alla trasparenza tra cliente e venditore, chiunque compri il *crypto ticket* potrebbe eventualmente rivenderlo sulla Blockchain senza alcun problema di passaggio, dal momento che l'identità del possessore del biglietto viene sempre omessa.

Tra le più famose piattaforme basate su NFT Tickets spiccano Oveit e SeatlabNFT. Ad un primo sguardo superficiale potrebbe sembrare che queste società svolgano il ruolo delle "terze parti" prima citate, ovvero intermediari che si fanno garanti dell'integrità del biglietto. In realtà il loro ruolo è unicamente quello di gestire la produzione dei biglietti NFT e la messa in vendita su Blockchain, in modo tale da rendere il tutto più vicino ad utenti che non conoscono tale mondo e desiderano proporre sul mercato i biglietti per un evento da loro organizzato.

5.4 NFT e Metaverso

Con il termine Metaverso si denota la futura generazione di internet, uno spazio in cui gli utenti possono interagire tra di loro attraverso degli avatar e possono utilizzare applicazioni in uno spazio virtuale tridimensionale.

Un esempio è *Decentraland*, il primo mondo virtuale completamente decentralizzato, dove gli utenti propongono e votano le modifiche delle politiche o dei contratti NFT consentiti all'interno del mondo, ad esempio. In un mondo virtuale come questo, destinato ad essere estremamente utilizzato in futuro, risulta necessario un certificato di proprietà di un dato oggetto virtuale, che garantisca la non replicabilità e la sua autenticità. In questo senso gli NFT sono la soluzione migliore, a partire dai semplici item associati al proprio avatar (come abiti, cappelli, scarpe), per poi passare a beni più importanti (palazzi, isole, mezzi di trasporto).

Un progetto interessante è quello di *Cryptokicks* proposto da Nike dopo aver acquisito RTFKT, una piccola società che già aveva prodotto in passato le cosiddette scarpe digitali. In effetti tale progetto punta a vendere NFT di scarpe digitali che gli utenti possano far indossare ai loro avatar nel mondo virtuale (Figura 5.8). Tale progetto è stato sin da subito di successo: propone circa 11.000 esemplari, alcuni più comuni, il cui valore si aggirava attorno ai 7.000 euro, e altri più rari, che valevano invece sui 130.000 dollari. Attualmente il *floor price* (il prezzo più basso a cui è possibile comprare un NFT di questa collezione su Opensea) si aggira attorno a 1,39 ETH. Essendo questi pezzi in versione limitata, si crede che in futuro acquisiranno ancora più valore, e quindi la Nike potrà avere delle importanti entrate dalle royalties frutto delle rivendite delle stesse scarpe da parte degli attuali possessori.

Attualmente ci si limita soltanto al collezionismo per quanto riguarda le Cryptokicks, poiché non è chiaro come Nike garantirà agli acquirenti di indossare gli NFT nel Metaverso. Tuttavia è chiaro che l'azienda voglia investire in questa nuova tecnologia: nel Novembre del 2021, tramite la piattaforma Roblox, Nike ha creato *Nikeland*, la sua città immaginaria (Nik). L'obiettivo dell'azienda è lanciare prototipi di scarpe e farle provare agli utenti nel mondo virtuale, prima di avviare una produzione di massa in quello reale. Una sorta di laboratorio dove si possono analizzare gli interessi degli utenti. D'altra parte, l'impegno impiegato nella produzione dei NFT da parte della Nike fa pensare che in futuro sarà anche possbile far indossare al proprio avatar nel mondo virtuale le "scarpe animate" come quelle di CryptoKicks che nella realtà non possono essere riprodotte.

5.5 Opportunità

Essendo il mondo dei NFT ancora agli inizi, sono molte le opportunità e le proposte che si possono avanzare nella società attuale. In questa sezione si riportano da una parte alcuni esempi di progetti da poco sviluppati e dall'altra idee non ancora implementate.

- **Settore automobilistico.** [Alf] Anche nel mondo automotive la tecnologia NFT può dare un suo contributo. Una prova è la casa automobilistica di Alfa Romeo la quale ha recentemente proposto sul mercato un nuovo modello, la Alfa Tonale, disponibile nelle concessionarie a partire dal 4 giugno 2022, collegata ad un certificato digitale NFT. L'obiettivo è quello di non permettere la manomissione dei dati dell'auto per scopi fraudolenti. Infatti, con il consenso del cliente, il sistema NFT registrerà i dati del veicolo nei tempi successivi all'acquisto, come garanzia della

Figura 5.8. NFT "RTFKT x Nike Dunk Genesis ANGL CRYPTOKICKS", presa da www.opensea.com.

giusta manutenzione dell'auto, con un impatto positivo sul suo valore di mercato. Il certificato digitale permetterà la completa tracciabilità del ciclo di vita della vettura: chilometri percorsi, incidenti, interventi di manutenzione, tutto ciò che serve sapere per certificare lo stato del veicolo. Fungerà così da garanzia per la futura vendita dell'usato. Sul mercato delle auto usate, infatti, la certificazione NFT rappresenta un'ulteriore fonte di credibilità su cui contare per proprietari o concessionari e ciò quindi farebbe fronte al drastico calo di valore che affligge una qualsiasi autovettura immediatamente dopo l'acquisto.

- **Turismo.** [Ife] In occasione dell'EXPO Dubai 2020, l'ente sloveno per il Turismo, in collaborazione con il Ministero dello Sviluppo Economico del Paese, lancia *I Feel Nft*, la prima azione di promozione turistica in Italia legata agli NFT. Il progetto lanciato all'Expo è il primo del genere al mondo. Come viene riportato nel sito relativo al progetto, l'idea è quella di creare dei souvenir digitali che i turisti possano portare a casa dopo un viaggio in Slovenia. Per entrare in possesso di tali NFT è necessario prima di tutto creare un wallet su Tolar Hashnet, la blockchain sulla quale è basato il progetto. Quindi è necessario collegare tale wallet alla applicazione appositamente creata e quindi inserire il codice promozionale ricevuto in fase di visita del paese (nel caso dell'EXPO 2020 il codice veniva consegnato quando qualcuno si presentava allo stand). Passo successivo alla presentazione del progetto a Expo Dubai, l'avvio ufficiale di I Feel NFT in Italia con un sito web dedicato e la Nft Card, prevista per il lancio in 1000 unità [For]. La Card garantisce di acquisire nel proprio wallet un NFT corrispondente a un souvenir certificato, ad esempio, scelto dalla raccolta presente sulla piattaforma dedicata che garantisce l'accesso ad una serie di servizi

esclusivi (musei, mostre, esperienze), a contenuti digitali esclusivi e ad attrazioni proposte dall'offerta turistica slovena. I cimeli digitali e le esperienze presenti sulla piattaforma in formato NFT mostrano i luoghi unici e le peculiarità del territorio sloveno. Tra le categorie proposte: paesaggio, attrazioni, cultura, video, fotografia, immagini a 360 e modelli 3D.

- **Certificazione competenze.** Uno dei punti di forza della blockchain è la sua immutabilità. Ciò permette in generale di avere la certezza che tutto ciò che viene inserito su di essa sia immutabile, verificato e validato. Per tale motivo potrebbe essere utile associare i NFT ad ogni titolo di studio, diploma, certificato, attestato, in modo tale che ogniqualvolta una azienda voglia assumere nuovo personale, possa osservare con facilità ciò che davvero il candidato possiede. Spesso verificare ciò può diventare un processo inutilmente lungo e faticoso. Con la creazione di una *educational blockchain* nazionale (o internazionale) sarebbe possibile validare i titoli di studio, associarli agli indirizzi tramite NFT nel momento in cui essi vengano conseguiti. Il momento del minting del NFT sarebbe l'unico istante in cui viene effettivamente controllato il possesso dello stesso titolo: da lì in poi i datori di lavoro si fideranno della blockchain che farà da garante dell'effettivo conseguimento del titolo. Ciò permetterebbe di avere un luogo condiviso a livello nazionale (o internazionale) in cui inserire sostanzialmente i curricula vitae certificati e approvati da tutti.

  Qualcosa di simile è stato proposto da Fiduxa, un'azienda progettata per facilitare la certificazione delle competenze in modo semplice, rapido, sicuro e con la possibilità da parte della persona proprietaria dei dati di scegliere quali dati rendere visibili e di ottenere per questo remunerazione in token. "Un curriculum certificato con Fiduxa – spiega la società – aiuterà le persone che cercano lavoro a presentare ai recruiter le proprie capacità in modo più efficace, senza l'ostacolo di dover progettare e disegnare il documento", facilitando per i propri utenti il cambio di lavoro anche in Paesi diversi dal proprio. Il profilo dell'utente che Fiduxa creerà, consentirà a chi assume di valutare i candidati più adatti alle loro richieste, senza dover passare in rassegna centinaia di curriculum, eliminando l'incombenza di farsi carico delle verifiche sui Cv (Ist).

Bibliografia

Alfa romeo tonale: "la metamorfosi". URL https://www.alfaromeo.it/alfa-news/2022/tonale.

Guida ad axie infinity: Come giocare e guadagnare. URL https://www.finder.com/it/axie-infinity.

Cryptokitties: Getting started. URL https://guide.cryptokitties.co/guide/getting-started.

Tecnologia blockchain e nft card per promuovere il turismo in slovenia. URL https://forbes.it/2022/04/14/tecnologia-blockchain-e-nft-card-per-promuovere-il-turismo-in-slovenia/.

I feel nft. URL https://ifeelnft.si/.

La blockchain per il curriculum: Fiduxa lancia l'ico. URL https://www.blockchain4innovation.it/ico/la-blockchain-per-il-curriculum-fiduxa-lancia-lico/.

Nike ha creato una città virtuale nel metaverso all'interno della piattaforma roblox. URL https://forbes.it/2021/11/25/perche-nike-sbarca-su-roblox-aprendo-una-citta-nel-metaverso/.

Yearly nft market, report 2021, a. URL https://nonfungible.com/reports/2021/en/yearly-nft-market-report.

Nft market, quarterly report, q1 2022, b. URL https://nonfungible.com/reports/2022/en/q1-quarterly-nft-market-report.

Migliori nft marketplace: Guida completa alle piattaforme più sicure, c. URL https://www.finaria.it/criptovalute/nft/migliori-nft-marketplace/#Che_cosa_sono_i_migliori_NFT_Marketplace.

The ultimate list of nft statistics (2022), d. URL https://findstack.com/nft-statistics/.

Luigi zanni: Quanti tipi di nft ci sono al mondo?, e. URL https://luigizanni.com/quanti-tipi-di-nft-ci-sono/.

URL https://eips.ethereum.org/EIPS/eip-721.

URL https://ethereum.org/it/developers/docs/standards/tokens/erc-721/.

Le raccolte spin-off, omaggio o remix sono consentite su opensea? URL https://support.opensea.io/hc/en-us/articles/1500010882082-Are-spin-off-homage-or-remix-collections-allowed-on-OpenSea-.

05. evoluzioni: smart contract e nft, a. URL https://www.7ecnologie.it/15-blockchain-e-bitcoin/05-evoluzioni-smart-contract-e-nft.

Documentazione sullo sviluppo di ethereum, b. URL https://ethereum.org/it/developers/docs/standards/tokens/erc-721/.

Blockchain: cos'è, come funziona e come cambierà il business, c. URL https://www.zerounoweb.it/cio-innovation/blockchain-cose-come-utilizzarla-e-come-cambiera-il-business/.

Lennart Ante. The non-fungible token (nft) market and its relationship with bitcoin and ethereum. 2021.

Jason Bailey. What is cryptoart? 2018.

Isac Daniel de Figueiredo Novo. Property-based testing of erc-721 ethereum smart contracts.

Tse-Chun Lin De-Rong Kong. Alternative investments in the fintech era: The risk and return of non-fungible token (nft). 2021.

T'ai Smith Blake Finucane Martin Lukas Ostachowski Sergio Scalet Jonathan Perkins James Morgan Sebastian Hernandez Massimo Franceschet, Giovanni Colavizza. Crypto art: A decentralized view. 2019.

Pierangelo Soldavini. I token non fungibili - christie's debutta nelle criptovalute: con 69,3 milioni di dollari è record per l'arte digitale. 2021.

Qin Wang, Rujia Li, Qi Wang, and Shiping Chen. Non-fungible token (nft): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447*, 2021.