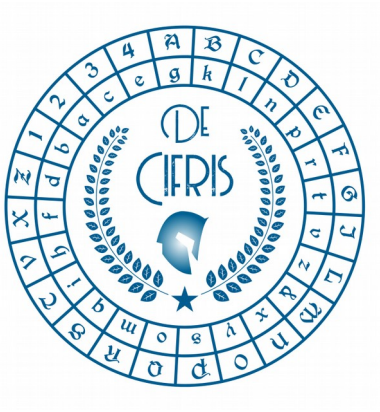


Distributed Consensus Algorithm
- a novel approach -

Fabio Fiori
fabio.fiori@quadrans.io

Introduzione

Nella tecnologie blockchain è di fondamentale importanza il metodo decisionale con cui i blocchi vengono validati e aggiunti alla chain.

Dato che non esiste un'organizzazione centralizzata che possa decidere se una transazione è da ritenersi valida, occorre predisporre un algoritmo che provveda ad effettuare le verifiche in modo deterministico.

Questa tipologia di algoritmi definisce la metodologia di Consensus che la blockchain utilizzerà per inserire nuovi blocchi all'interno della catena.

Il consensus in Blockchain

La blockchain può essere definita come un enorme database decentralizzato, pubblico e immutabile.

Uno dei problemi principali in questo è sicuramente ottenere il consensus in un ambiente dove i vari attori non si conoscono e non esiste un legame di trust tra di loro.

Inoltre, la metodologia scelta deve essere trasparente e equa per tutti i partecipanti.

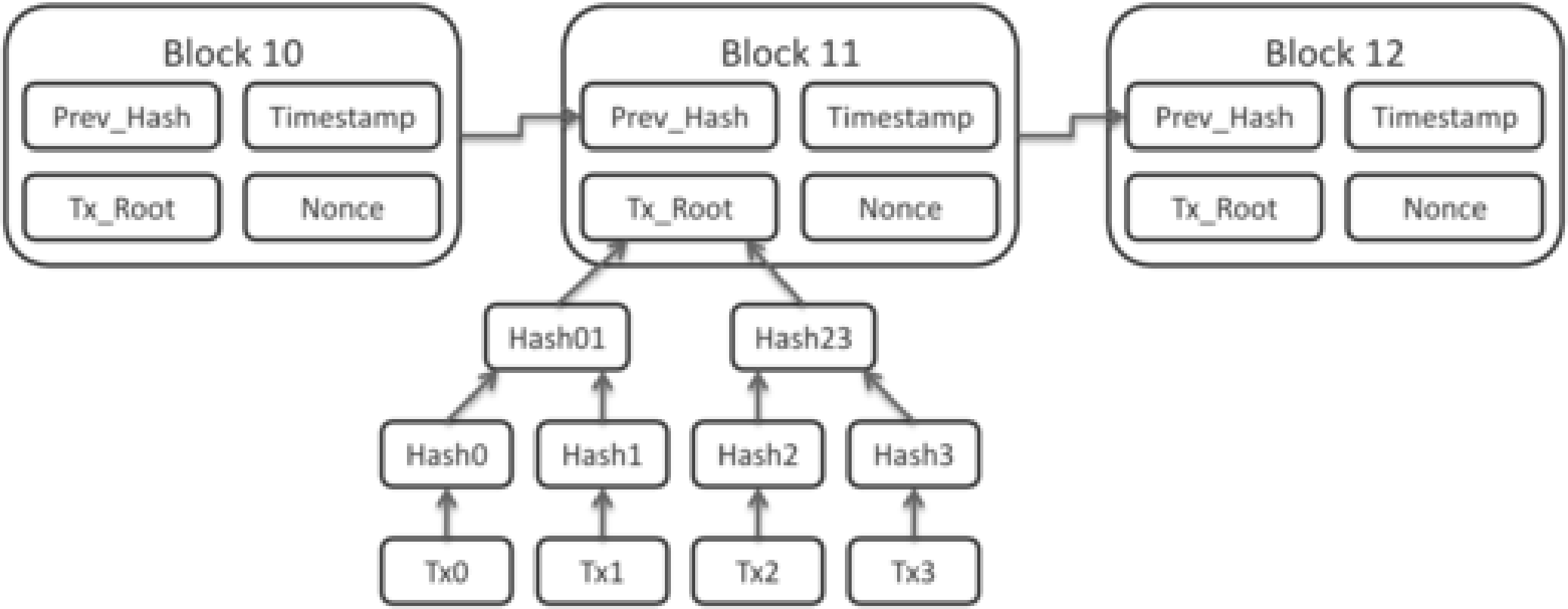
Aggiungere un blocco

Un blocco è composto da diverse informazioni, come l'hash del blocco precedente, una lista di transazioni, il timestamp corrente e altre informazioni utili a determinare la correttezza del blocco stesso.

Per aggiungere un blocco alla blockchain, e quindi allungare la catena, è necessario produrre una "prova" che attesti la buona fede del blocco prodotto.

L'operazione di aggiunta di un blocco alla blockchain viene definita *mining* o *minting*.

Aggiungere un blocco



Un primo problema!

In un ambiente distribuito, chiunque può proporre un nuovo blocco da aggiungere alla blockchain.

Può quindi accadere che due persone propongano due blocchi diversi nello stesso momento, oppure che un malintenzionato proponga una sua soluzione.

In questi casi si crea una fork all'interno della blockchain, creando quindi due chain che hanno lo stesso storico di blocchi, ma futuro differente.

Una prima soluzione!

Esistono diversi approcci a questo problema. Non si tratta di vere e proprie soluzioni, ma di metodi per scoraggiare questo tipo di attacchi.

- **Vince la fork più vecchia**
  Secondo questa regola, un miner in presenza di una fork aggiungerà i nuovi blocchi solo alla fork che avrà il blocco minato più vecchio. Questa soluzione è facilmente attaccabile in quanto basata solamente sul timestamp, che può essere facilmente attaccato.

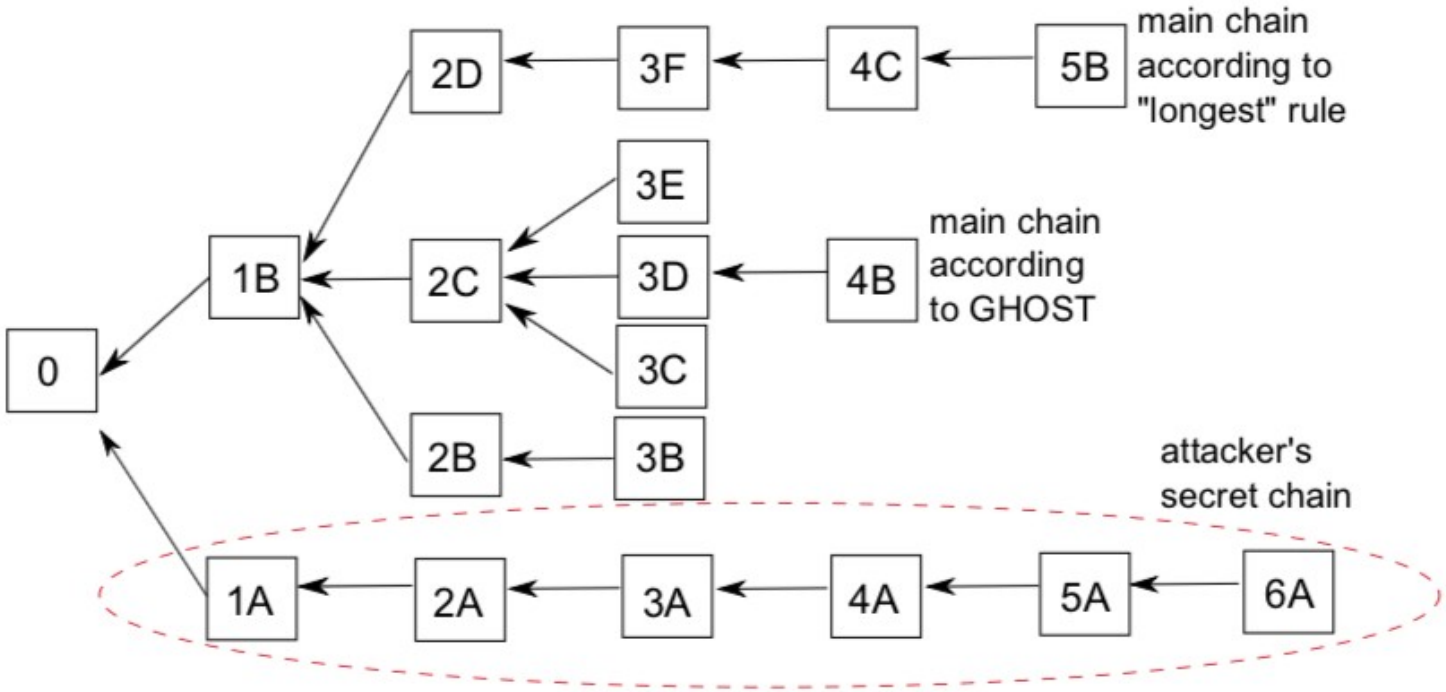
Una prima soluzione!

- **Vince la fork più lunga**
  Questo approccio, che fu proposto nella prima versione di Bitcoin, considera la chain più lunga come quella valida a cui agganciare nuovi blocchi. Tuttavia, esistono casi in cui, se la fork avviene rapidamente, la catena più lunga potrebbe essere quella non corretta, in quanto la potenza di calcolo si distribuirebbe sulle varie fork.

Una prima soluzione!

- **GHOST**
  Questo approccio, considerato il più sicuro al momento, valuta tutte le diramazioni della rete per determinare quella che è stata generata utilizzando la maggior potenza computazionale. In questo modo per portare a termine con successo un attacco è necessaria (teoricamente) più della metà della potenza di calcolo sulla rete.

Una prima soluzione!



Il problema dei gen. bizantini

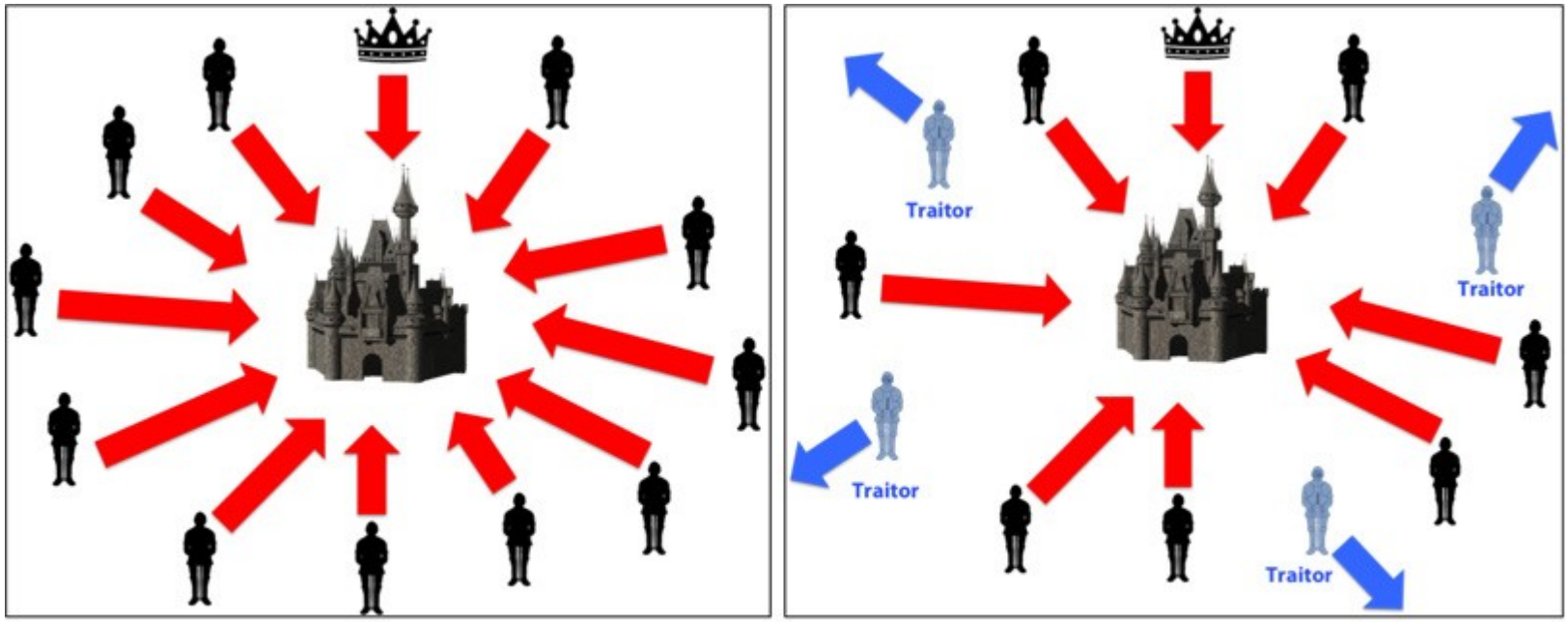
Il problema dei generali bizantini è un problema ai fini del raggiungimento del consensus in un ambiente distribuito.

Questo problema viene spesso esemplificato nella situazione in cui 3 o più generali debbano decidere se attaccare o ritirarsi una volta ricevuto un ordine da un comandante superiore. Uno più generali potrebbe essere un traditore, quindi potrebbe fornire agli altri generali informazioni discordanti oppure effettuare un'azione in disaccordo con quella impartita.

Il problema dei gen. bizantini

Definizione formale:
Dato un numero N di processi, si richiede che al termine dell'algoritmo tutti i processi corretti impostino la variabile di decisione sullo stesso valore. Questo valore deve essere quello fornito dal processo comandante nel caso in cui questo sia corretto. I processi non corretti possono non inviare messaggi oppure inviarne con contenuto arbitrario. I messaggi non sono firmati.

Il problema dei gen. bizantini



Coordinated Attack Leading to Victory

Uncoordinated Attack Leading to Defeat

La soluzione

Nella versione originale, è dimostrato che non esiste soluzione a questo problema se il numero di processi non corretti è maggiore o uguale ad un terzo del numero totale dei progetti.

La soluzione proposta da Satoshi Nakamoto per ovviare a questo problema all'interno della rete Bitcoin è la Proof-of-Work.

Questa soluzione non è perfetta, ma consente al Bitcoin di avere una buona protezione da questo tipo di attacchi e di raggiungere una visione coerente e globale del sistema distribuito.

La soluzione

Altre blockchain utilizzano altri tipi di protezione, come ad esempio la pBFT (Pratical Byzantine Fault Tolerance), utilizzano altre metodologie di consensus oppure rendendo la rete permissioned.

Questo tipo di soluzione è suscettibile ad altri tipi di attacchi, come il Sybil attack o il 50%+1 attack.

Metodologie di consensus

Queste tipologie di algoritmi si possono dividere in alcune famiglie, in base alla loro tipologia:

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Proof of Authority (PoA)
- Proof of Burn (PoB)
- Proof of Location (PoL)
- Proof of Space (PoSpace)
- e molti altri…

Durante questo seminario, ci si concentrerà prevalentemente sulla prima e sulla seconda categoria.

Proof of Work (PoW)

La Proof of Work consiste nel creare un dato che sia difficile da calcolare, che rispetti determinate condizioni e che sia facile da verificare per gli altri attori all'interno del sistema.

Dato che tutti i miner agganciati alla rete devono eseguire lo stesso calcolo per concorrere alla generazione del nuovo blocco, questa metodologia è decisamente costosa, in termini di energia e di tempo.

La metodologia di PoW più comunemente utilizzata è Hashcash.

Hashcash

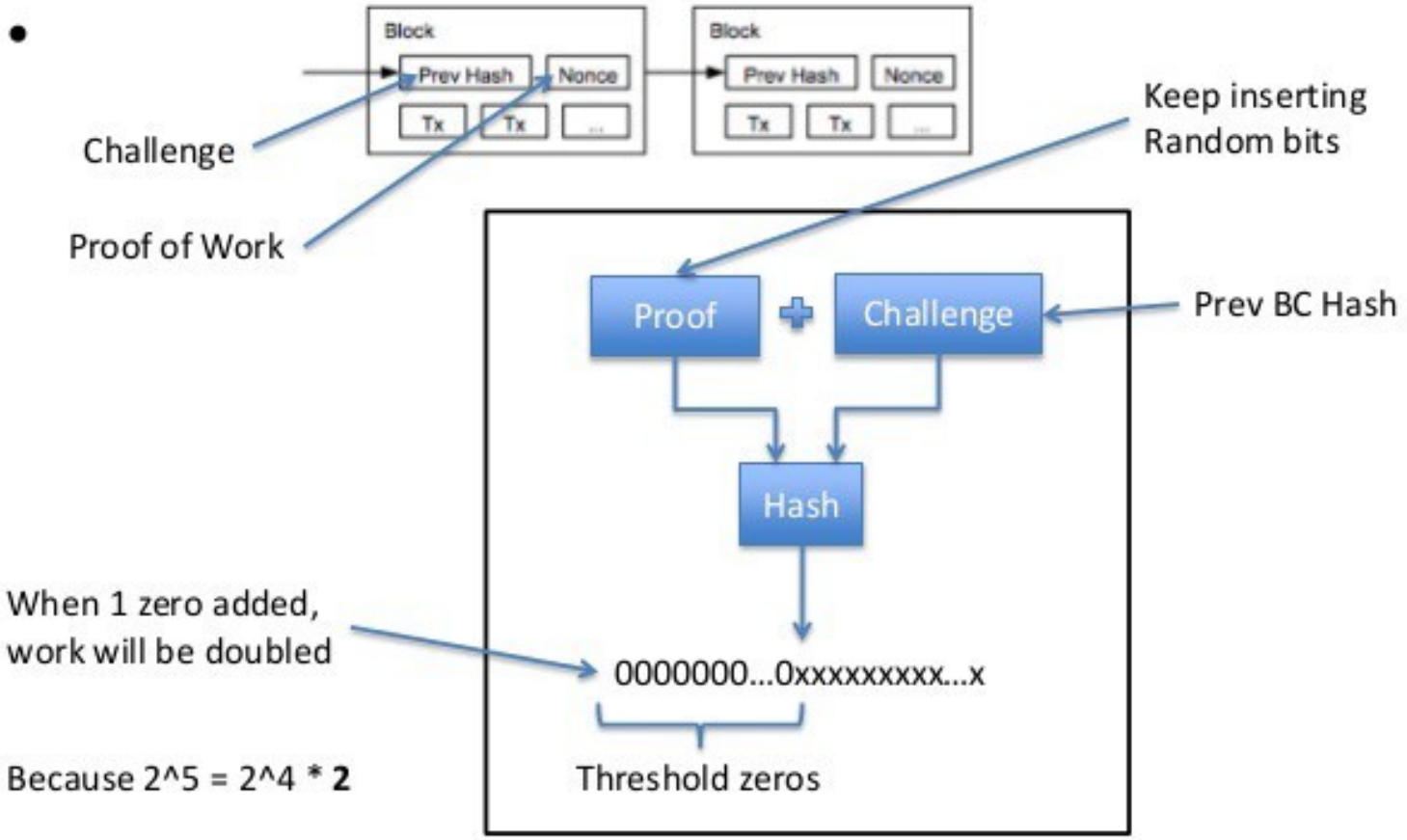
Hashcash è sicuramente la classe di algoritmi PoW più diffusa. È basata sulle funzioni di hash, che sono funzioni deterministiche che mappano dati di una dimensione arbitraria in un dato di lunghezza fissa.

Queste funzioni devono essere difficilmente invertibili, resistenti alle collisioni e uniformi.

La struttura generale di questo metodo consiste nel cercare un certo numero di bit, chiamato *Nonce*, che aggiunto ai dati originali produce un hash con un determinato numero di zeri all'inizio.

Hashcash PoW

Proof of Work



SHA-256

SHA-256 è la funzione utilizzata come PoW da Bitcoin. Fa parte della famiglia delle funzioni Secure Hash Algorithms.

La lunghezza dell'output è di 256 bit, e la difficoltà, intesa come numero di zeri da ottenere all'inizio del risultato è modificata periodicamente in modo da mantenere stabile la rete al variare della potenza di calcolo.

Al momento attuale l'hash rate dell'intera rete Bitcoin è di circa 50.000 PH/s.

Scrypt

Scrypt è la funzione utilizzata come PoW da Litecoin e Dogecoin.

È un algoritmo che si basa sulla derivazione di chiavi basata su password, e necessita di molta più memoria rispetto ad altre PoW.

È stata proposta come alternativa alla PoW basata su SHA in quanto si pensava non potesse essere risolta utilizzando ASIC proprio per questa sua caratteristica legata al consumo di memoria.

Ethash

Ethash è la funzione studiata per il mining sulla blockchain di Ethereum.

Combina l'algoritmo di hash SHA-3 (Kekkak) con una variante dell'algoritmo di Dagger-Hashimoto.

Dopo l'annuncio di ASIC in grado di risolvere questo tipo di PoW, gli sviluppatori hanno deciso di scrivere un nuovo algoritmo di hash chiamato ProgPoW, in attesa del passaggio a Ethereum 2.0, che avrà un consensus basato su Proof of Stake.

Ethash

L’algoritmo può essere descritto nel seguente modo:

- Viene calcolato un seed per ogni blocco, basato sui dati al suo interno e sulla storia dei blocchi precedenti
- Da questo seed, viene calcolato una cache pseudocasuale da 16MB
- Sulla base di questa cache, viene generato un dataset da 1GB. La larghezza cresce linearmente col tempo
- L’operazione di mining consiste nel prendere porzioni casuali di questo dataset ed effettuarne l’hash.

Hashcash – Alternative

Esistono alternative ad Hashcash, che utilizzano un diverso concetto di lavoro per effettuare la verifica.

Alcune di queste alternative considerano come lavoro la messa a disposizione di spazio su disco, altre invece si basano sulla posizione geografica o sul “bruciare” i propri coin.

Ci sono stati diversi tentativi anche di utilizzare la potenza di calcolo della PoW per risolvere problemi scientifici o di ricerca.

Proof of Stake (PoS)

La Proof of Stake è un protocollo diverso rispetto alla PoW, in quanto non è basato su una competizione relativa al lavoro, ma richiede che ogni utente che partecipa al consensus dimostri il possesso di un certo quantitativo di coin.

È stata utilizzata inizialmente da Peercoin, e implementata successivamente da altre criptovalute come per esempio Cardano.

Esistono varianti rispetto all'implementazione originale come per esempio la Delegated Proof of Stake (DPoS)

Proof of Stake (PoS)

Mentre nella PoW tutti eseguono contemporaneamente lo stesso lavoro, nella PoS solo uno creerà il blocco successivo.

Ad ogni blocco viene scelto in maniera deterministica chi si dovrà occupare di forgiare il blocco successivo.

La selezione può avvenire in modo casuale, in base alla velocità, al voto oppure in base all'anzianità.

Proof of Stake (PoS)

- **Selezione casuale**
  Questo permette di selezionare in modo pseudocasuale chi genererà il prossimo blocco, ed è basata su dati presenti all'interno della blockchain e quindi risulta facile predire chi si dovrà occupare di produrre il nuovo blocco.

- **Selezione sull'anzianità**
  Questa metodologia si basa sull'intervallo di tempo in cui lo stake viene bloccato e sull'importo che viene bloccato. Chi avrà lo stake più grande e bloccato da più giorni sarà il creatore del blocco successivo.

Proof of Stake (PoS)

- **Selezione a votazione**
  Questa è una variante in cui ogni stakeholder effettua una votazione per eleggere un insieme ridotto di nodi che si occuperanno di forgiare i blocchi.

- **Selezione sulla velocità**
  Questa implementazione predilige la movimentazione della moneta invece che l'immobilizzazione. Quindi il prossimo che potrà forgiare il nuovo blocco sarà quello che avrà effettuato il numero maggiore di transazioni.

Altre metodologie

Proof of Burn (PoB)
Il funzionamento della PoB è molto semplice, infatti consiste nel “bruciare” coin per manifestare la propria “buona fede” nella blockchain.

Proof of Location (PoL)
La PoL funziona in maniera analoga alla PoA, ma il discriminante per essere o meno eletti come authority è la propria posizione geografica.

Proof of Space (PoSpace)
La PoSpace consiste nell’allocare un certo ammontare di spazio di storage per risolvere una sfida e poter aggiungere un nuovo blocco alla blockchain.

Altre metodologie

Proof of Authority (PoA)
La PoA viene presentata per la prima volta nell'EIP-255 come proposta alternativa alla PoW per la rete di test Rinkeby. La prerogativa è quella di creare un'oligarchia di nodi che possano effettuare il sealing del blocco ed eleggere (o rimuovere) nuove authority. Le authority procederanno a turno, ed è necessario che almeno il 50% + 1 delle authority resti attiva o il processo si ferma.

Un approccio nuovo

Quello che è viene proposto è una metodologia di consensus Proof of Work basata sulla risoluzione di un problema matematico, il problema del logaritmo discreto su una curva ellittica (ECDLP).

La soluzione di questo problema verrà utilizzata come validazione del blocco da aggiungere alla blockchain.

Le curve ellittiche utilizzate in questo approccio sono unicamente quelle su campi di numeri primi.

Struttura della blockchain

La blockchain proposta conterrà al suo interno due tipologie di blocchi:

- **Un Epoch Block**
  Questo blocco conterrà la lista delle transazioni e l'header come tutti gli altri blocchi, ma conterrà anche un numero primo *p*, una curva ellittica *E* e un punto base *P* su *E*. Inoltre conterrà come PoW un numero intero *N* tale per cui *NP* sia un punto di *E*.

  Questo tipo di blocco si ripresenterà periodicamente all'interno della blockchain.

Struttura della blockchain

- **Uno Standard Block**
  Questo blocco è una versione ridotta del blocco precedente, in quanto eredita i parametri della curva *E* dall'Epoch Block precedente.

  Questa tipologia di blocchi rappresenta numericamente la maggioranza dei blocchi all'interno della blockchain.

In pratica, l'Epoch Block definisce i parametri della PoW validi per i seguenti Standard Block e fino alla creazione di un nuovo Epoch Block.

Standard Block

Per la creazione di uno standard block, verrà creato l'header del blocco contenente il Merkle root *M* delle transazioni, l'hash del blocco precedente, il timestamp e un intero *N*, risultato della PoW, che risolva il seguente problema:

$$\text{P\_Gen}(H(h_{prev} \,||M), E) = N \cdot P$$

Dove la funzione P_Gen costruisce un punto sulla curva ellittica in base ai parametri forniti.

Epoch Block

La creazione di un Epoch Block è più complessa rispetto a quella dello Standard Block, in quanto, oltre a generare i parametri dello Standard Block, dovrà:

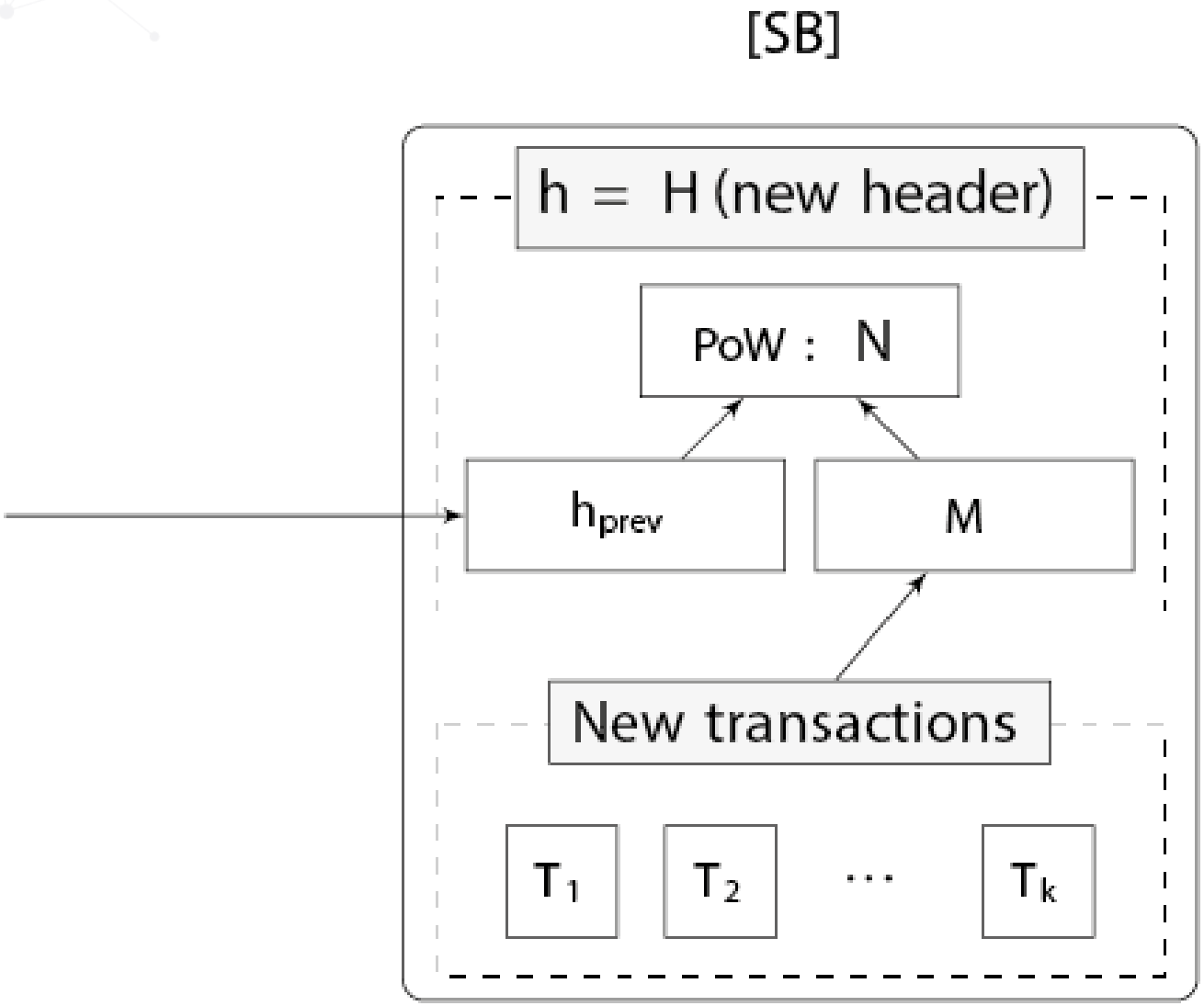
- **Generare *p***
  Questo numero primo, la cui lunghezza determina la difficoltà della PoW, e deve essere generato in maniera deterministica, utilizzando come base l'hash del blocco precedente.

Epoch Block

- **Generare *E***
  E è la curva ellittica sul campo finito F_p, sulla quale verranno presi i punti per la Proof of Work.

- **Generare *P***
  P è il punto base della curva, sulla quale verrà effettuata la Proof of Work.

Struttura del blocco



Conclusioni

La ricerca scientifica è stata realizzata in collaborazione con il CryptoLab dell'Università degli Studi di Trento.

Il nostro lavoro in questo momento è concetrato sull'implementazione di un Proof of Concept di questa nuova metodologia di consensus, in modo da poter valutare le sue prestazioni in casistiche prese dal mondo reale e valutare la robustezza agli attacchi di questa tipologia di algoritmi.

Inoltre, stiamo per entrare nell'epoca dei Quantum computer...

quadrans FOUNDATION

Grazie

Bibliografia

1. Nakamoto S., Bitcoin: A Peer-to-Peer Electronic Cash System, (2008), URL: https://bitcoin.org/bitcoin.pdf.
2. Ethereum team, Ethash, (2018), ethereum/wiki/wiki/Ethash
3. Sompolinsky Y., Zohar A., Secure High-Rate Transaction Processing inBitcoin, https://eprint.iacr.org/2013/881.pdf
4. Lamport L., Shostak R., Pease M., The Byzantine Generals Problem, in ACM Transactions on Programming Languages and Systems, vol. 4, nº 3, luglio 1982
5. Bitcoin.org
6. Castro, M., Liskov, B. (2002). "Practical Byzantine Fault Tolerance and Proactive Recovery". ACM Transactions on Computer Systems.
7. Computing for Good - Ripple's Contribution to Science, http://www.devtome.com/doku.php?id=computing_for_good
8. Meneghetti A., Sala M., Sogiorno D., Taufer D., A survey on PoW-based consensus with a new ECDLP-based PoW proposal
9. King S., Nadal S.: PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, (2012), URL: https://peercoin.net/whitepapers/peercoin-paper.pdf