MODULO 2:

IL PROBLEMA DEI GENERALI BIZANTINI, ALGORITMI DI CONSENSO, TIPI DI ALGORITMI DI CONSENSO.

Il problema dei generali bizantini

La tecnologia blockchain, conosciuta anche come “contabilità distribuita” (o con le sue sigle inglesi DLT) o in spagnolo “catene di blocchi”, è un protocollo di operazioni di scambio tra pari che si verificano, gestiscono e verificano in modo decentralizzato, automatizzato, condiviso e sicuro. Affinché la tecnologia blockchain sia affidabile, alla base c'è il consenso.

Che cos’è il consenso? È semplicemente il fatto che tutti i membri di una rete siano d’accordo sul fatto che una transazione X sia avvenuta tra due membri della rete in un determinato momento.

Per raggiungere un accordo, evitando inganni e riducendo al minimo gli errori, è qui che entra in gioco la soluzione al problema dei generali bizantini, ovvero un vecchio gioco di logica: in un assedio c'è un numero indeterminato di generali che deve coordinarsi per la conquista. Solo uno (il comandante) invia l'ordine (che è binario, attaccare o ritirarsi), il resto sono generali. Può esserci uno o più traditori (comandante incluso), con l'obiettivo che l'ordine non venga eseguito.
Tutti insieme, ma controllandosi a vicenda.
Così, e semplificando molto, ogni tenente (membro della rete) riceve un ordine (transazione) e lo invia

agli altri. L'ordine contraddittorio del traditore rimarrebbe minoritario, anche se fosse quello del comandante (colui che ordina la transazione), e verrà considerato vero l'ordine maggioritario. I traditori maliziosi vengono così neutralizzati.

Esistono certe condizioni che le blockchain reali creano per rendere più resistente il consenso ottenuto attraverso questo sistema di prova del lavoro (Proof Of Work in inglese), come viene solitamente chiamato:

Tutti i generali comunicano con tutti gli altri.

Ogni generale sa chi gli invia l'ordine.

In assenza di un messaggio, c'è un ordine predefinito. Gli ordini sono scritti e firmati.

Gli errori casuali vengono controllati tramite codici di rilevamento degli errori.

La marcatura temporale affidabile impedisce la duplicazione degli ordini.

La risoluzione di questo dilemma, raggiunta nel 1982, è una delle basi fondamentali del funzionamento delle blockchain, nonché l'elemento che le rende un modo affidabile per effettuare transazioni tra nodi non necessariamente affidabili: tutti i nodi partecipano e registrano tutte le transazioni. Le fondamenta del futuro sono state gettate.

Algoritmi di consenso

Che cos'è un algoritmo di consenso blockchain?
Nel contesto delle criptovalute, gli algoritmi di consenso sono elementi cruciali di tutte le reti blockchain, poiché sono responsabili del mantenimento dell'integrità e della sicurezza di questi sistemi distribuiti. Il primo algoritmo di consenso creato per una criptovaluta è stato Proof of Work (PoW), progettato da Satoshi Nakamoto e implementato in Bitcoin come formula per superare i Bizantine Faults (Errori bizantini).

Algoritmo di consenso
Un algoritmo di consenso può essere definito come il meccanismo attraverso il quale una rete blockchain raggiunge il consenso. Le blockchain pubbliche (decentralizzate) sono sistemi distribuiti e, poiché non dipendono da un'autorità centrale, i loro nodi (anch'essi distribuiti) devono concordare sulla validità delle transazioni.
È qui che entrano in gioco gli algoritmi di consenso, incaricati di assicurare che le regole del protocollo siano rispettate e di garantire che tutte le transazioni avvengano in modo affidabile; ciò implica che le monete potranno essere spese una sola volta.

Prima di addentrarci nei diversi tipi di algoritmi di consenso, è importante comprendere le differenze tra un algoritmo e un protocollo.

Algoritmo di consenso contro protocollo

I termini algoritmo e protocollo sono spesso usati in modo intercambiabile, tuttavia non sono la stessa cosa. In termini semplici, possiamo definire un protocollo come le regole primarie di una blockchain; e l'algoritmo, come il meccanismo attraverso il quale tali regole saranno seguite.

Oltre ad essere ampiamente utilizzata nei sistemi finanziari, la tecnologia blockchain può essere applicata a un'ampia varietà di attività commerciali e risultare adatta a diversi casi d'uso. Tuttavia, indipendentemente dal contesto, una rete blockchain si baserà sempre su un protocollo che definirà il presunto funzionamento del sistema. Per questo motivo, tutti i suoi elementi, così come i partecipanti alla rete, dovranno rispettare le regole del protocollo sottostante.

Mentre il protocollo determina quali sono le regole, l'algoritmo indica al sistema quali passaggi seguire per rispettarle e produrre i risultati desiderati.

Ad esempio, l'algoritmo di consenso di una blockchain è ciò che determina la validità delle transazioni e dei blocchi. Pertanto, Bitcoin ed Ethereum sono protocolli, mentre Proof of Work e Proof of Stake sono i loro algoritmi di consenso.

Per illustrare meglio la questione, occorre tenere presente che il protocollo Bitcoin definisce come devono interagire i nodi, come devono trasmettere i dati, nonché quali sono i requisiti affinché una convalida di blocco sia effettiva. D'altra parte, l'algoritmo di consenso è responsabile di verificare i saldi e le firme, confermare le transazioni ed eseguire la convalida dei blocchi. E tutto questo dipende da un consenso di rete.

Diversi tipi di algoritmi di consenso

Esistono diversi tipi di algoritmi di consenso. Le implementazioni più comuni sono PoW e PoS. Ognuno presenta vantaggi e svantaggi per quanto riguarda l'equilibrio tra sicurezza, da un lato, e funzionalità e scalabilità dall'altro.

Proof of Work (PoW)

Il PoW è stato il primo algoritmo di consenso creato. È utilizzato da Bitcoin e da molte altre criptovalute. L'algoritmo Proof of Work è una parte essenziale del processo di mining.

Il mining in PoW comporta numerosi "tentativi di hashing", quindi una maggiore potenza di calcolo significa più tentativi al secondo. In altre parole, i miner con un'elevata velocità di hash hanno maggiori possibilità di trovare una soluzione valida per il blocco successivo (chiamato anche hash block). L'algoritmo di consenso PoW garantisce che i miner

siano in grado di convalidare un nuovo blocco di transazioni e aggiungerlo alla blockchain solo se i nodi distribuiti della rete raggiungono il consenso e accettano l'hash block fornito dal miner come prova di lavoro valida.

Proof of Stake (PoS)

L'algoritmo di consenso PoS è stato sviluppato nel 2011 come alternativa al PoW. Sebbene sia il PoS che il PoW condividano obiettivi simili, presentano anche alcune differenze e particolarità fondamentali. Soprattutto per quanto riguarda la convalida dei nuovi blocchi.

In poche parole, l'algoritmo di consenso Proof of Stake sostituisce il mining PoW con un meccanismo in cui i blocchi vengono convalidati in base allo “stake” (quantità di monete accumulate e bloccate) dei partecipanti. Il validatore di ogni blocco, chiamato anche forger (forgiatore) o minter (coniatore), è determinato dall'investimento nella criptovaluta stessa e non dalla quantità di potenza di calcolo destinata. Ogni sistema PoS può implementare l'algoritmo in modi diversi, ma in generale la blockchain sarà protetta da un processo di selezione pseudo-casuale che tiene conto del capitale del nodo e dell'età delle monete (il tempo in cui sono rimaste immobili, depositate o “staked”), insieme a un fattore di casualità.

La blockchain di Ethereum si basò inizialmente su un algoritmo PoW, ma nel 2022, con il Merge, il protocollo Casper fece passare la rete da PoW a PoS, con l'obiettivo di aumentarne la scalabilità.

Perché gli algoritmi di consenso sono importanti per le criptovalute?

Come ho già accennato, gli algoritmi di consenso sono fondamentali per garantire l'integrità e la sicurezza di una rete di criptovalute. Sono incaricati di fornire gli strumenti affinché i nodi distribuiti raggiungano un consenso su quale versione della blockchain sia quella autentica. Raggiungere un accordo sullo "stato" attuale della blockchain è essenziale affinché un sistema economico digitale funzioni correttamente.

L'algoritmo di consenso Proof of Work è considerato una delle migliori soluzioni al Problema dei Generali Bizantini, che ha permesso la creazione di Bitcoin come "Sistema Tollerante ai Guasti Bizantini" (Byzantine Fault Tolerant System). Ciò significa che la blockchain di Bitcoin è altamente resistente a un tipo di minacce denominate "attacchi del 51%" o "attacchi maggioritari", non solo perché la rete è decentralizzata, ma anche grazie all'algoritmo PoW. Gli alti costi coinvolti nel processo di mining rendono molto difficile e improbabile che i miner investano così grandi risorse per danneggiare la rete.

Tipi di algoritmi di consenso

Esistono molti algoritmi per raggiungere il consenso in una blockchain, ma ad oggi il Proof of Work di Bitcoin rimane quello dominante tra le piattaforme blockchain attuali.

Quanti algoritmi di consenso esistono per le blockchain?

Un algoritmo di consenso può essere definito come il meccanismo attraverso il quale una rete blockchain raggiunge un consenso. Come è noto, le blockchain devono raggiungere un consenso tra i nodi che le mantengono, per garantire la sicurezza della rete in generale, convalidando più volte le transazioni che vi avvengono e definendo quali sono legittime da aggiungere alla catena principale.

Bitcoin è stata la prima criptovaluta a introdurre il termine algoritmo di consenso, poiché, come ben sappiamo, utilizza l'algoritmo Proof of Work (PoW), oggi oggetto di accese discussioni a causa del suo eccessivo consumo energetico. A seguito del boom delle criptovalute, sono state ideate molte varianti che hanno dato vita a una serie di opportunità, il cui obiettivo principale rimane lo stesso: raggiungere il consenso in una rete blockchain.

Ecco perché vi propongo una sintesi degli algoritmi di consenso più comuni e meno pubblicizzati attualmente presenti nel mercato delle criptovalute.

Proof-of-Work (PoW)

Come accennato in precedenza, è il primo algoritmo di consenso blockchain ed è stato utilizzato per la prima volta da Bitcoin, la criptovaluta attualmente leader di mercato. Nel mining PoW, i miner risolvono complessi enigmi matematici che richiedono molta potenza di calcolo. Il primo a risolvere il puzzle crea un blocco e riceve una ricompensa per questo. Il modo per risolverlo è fondamentalmente un “indovinello”, poiché non esiste alcun metodo alternativo se non quello di prova ed errore.

L'algoritmo PoW garantisce che i miner possano convalidare un nuovo blocco di transazioni e aggiungerlo alla catena solo se i nodi distribuiti della rete raggiungono il consenso e accettano l'hash trovato dal miner come valido.

Criptovalute che lo utilizzano:

Secondo il sito cryptoslate, un totale di 105 monete tra gli oltre 38 milioni attualmente esistenti nell'ecosistema utilizzano il PoW come meccanismo di consenso, anche con alcune derivazioni e/o miglioramenti come nel caso della Komodo Platform che genera il proprio consenso con lo schema di base del PoW, ma replicato, chiamato dPoW. Nonostante attualmente il settore PoW rappresenti una quantità minima di meccanismi di consenso, capitalizza circa il 60% del totale del mercato.

Bitcoin utilizza l'algoritmo SHA 256 per firmare le proprie transazioni, per cui monete come Bitcoin Cash, Bitcoin SV e Syscoin implementano essenzialmente la stessa metodologia di Bitcoin, ma con un miglioramento delle dimensioni del blocco che consente di aumentare i tempi di generazione e convalida.

In generale, Bitcoin (BTC), Litecoin, Monero, Dash, Bitcoin Cash, Bitcoin SV, Ethereum Classic, Zcash, tra le altre, utilizzano l'algoritmo Proof of Work.

Queste piattaforme, per la loro analogia con la valuta leader, sono chiamate piattaforme blockchain di prima generazione e la stragrande maggioranza si colloca tra le prime 20 più importanti del mercato delle criptovalute, in termini di capitalizzazione di mercato, con una quota del 55-60% del mercato, pari a circa 1500 miliardi di dollari (1,5 bilioni)

Proof-of-Stake (PoS)

Questo algoritmo di consenso nasce come alternativa al PoW e mira a raggiungere un consenso distribuito. È stato utilizzato per la prima volta da Peercoin ed è stato creato nel 2011, dopo essere stato discusso in un forum su Bitcointalk nello stesso anno.

Il suo funzionamento differisce notevolmente dall'algoritmo precedente. Invece di far dimostrare ai miner che ogni singola transazione è legittima, il

Proof of Stake, o Prova di Partecipazione o di Posta in Gioco, richiede che una persona metta in gioco, mantenga o blocchi le monete e ne convalidi la proprietà. In poche parole, questo algoritmo sostituisce il mining intensivo del PoW con un meccanismo in cui i blocchi vengono convalidati in base alla “partecipazione” delle parti coinvolte.

Sebbene esistano diversi modi per selezionare il nuovo creatore di blocchi al fine di evitare la centralizzazione dovuta alla quantità di monete che possono essere bloccate o “puntate”, in generale la blockchain è garantita da un processo di selezione pseudo-casuale che considera la ricchezza del nodo e l'anzianità delle monete insieme a un fattore di casualità.

Esistono molte derivazioni di questo algoritmo; tra le più rilevanti abbiamo:

Proof of Anonymous Stake (PoSA): Cloakcoin, Spectrocoin Proof of Importance (PoI): NEM

Proof of Storage: Storj

Proof of Stake Time (PoST): Vericoin

Prova di Velocità di Staking (PoSV): Reddcoin

Esistono molte monete che utilizzano questo algoritmo in tutte le sue derivazioni; tra le più rilevanti figurano Binance Coin, Stellar, Dash, Neo, Cosmos, Ontology e altre. Complessivamente, questo settore rappresenta circa 365 miliardi di dollari, pari al 15% del mercato generale.

Prova di partecipazione delegata (DPOS)

La Prova di partecipazione delegata (DPOS) è un meccanismo di consenso molto veloce, meglio conosciuto per la sua implementazione in EOS e spesso definito come democrazia digitale, grazie al suo sistema di voto ponderato in base alla quota.
Il suo funzionamento prevede che gli utenti votino dei "delegati" ai quali viene conferito il potere di ottenere profitti gestendo un nodo completo. Il peso del loro voto dipende dalla loro partecipazione o dal numero di monete bloccate. Poiché i delegati desiderano ricevere il maggior numero possibile di voti, sono costantemente incentivati a creare valore per la comunità, in quanto è probabile che ricevano voti aggiuntivi per averlo fatto.
Si suppone che questo metodo sia più efficiente e protegga gli utenti da interferenze normative indesiderate. Tuttavia, il suo massimo esponente, EOS, è stato oggetto di una massiccia fuga di sviluppatori iniziali che accusano il sistema di essere centralizzato e insicuro.
Tra i più importanti abbiamo ovviamente EOS, Tron, Cardano, Tezos, Lisk, Bitshares, Steem, tra gli altri. Il numero di progetti coinvolti è abastanza limitato (sono solo 23), rappresentando, in termini di capitalizzazione di mercato, il 3,3% del totale del

mercato, con una capitalizzazione totale vicina ai 79 miliardi.
Questo algoritmo è diventato popolare tra gli sviluppatori di applicazioni decentralizzate (dApp), che tra EOS e Tron dominano il sottosettore in termini di milioni di dollari, secondo il sito Dappreview.

Delegated Byzantine Fault Tolerance (dBFT)

La Delegated Byzantine Fault Tolerance è un nome elegante e geniale per una soluzione volta a raggiungere un consenso finale in determinate condizioni. La condizione è davvero semplice: purché meno di 1/3 dei nodi contabili siano attori MALVAGI, si può arrivare a un consenso finale e tutti saranno felici.
Il dBFT non garantisce il consenso nel senso che è possibile che la rete di messaggistica sia interrotta e che le persone semplicemente non possano comunicare tra loro. Tuttavia, offre garanzie di protezione: se raggiunge un consenso, non potrà raggiungere un altro consenso diverso in seguito. Finché gli attori malintenzionati sono meno di 1/3 dei nodi contabili, allora va tutto bene. Sebbene non sia ancora di uso comune, rappresenta un'alternativa più semplice alla proof-of-stake, alla proof-of-importance e alla proof-of-work. La tolleranza delegata ai guasti

bizantini utilizza una regola dei due terzi e altri elementi per garantire che si raggiunga il consenso anche in presenza di molte incognite.

L'algoritmo è stato proposto da NEO, che da allora sviluppa le proprie applicazioni decentralizzate sotto questo meccanismo.

Prova di attività (PoA)

Il concetto è stato introdotto per la prima volta nel 2012 come alternativa alla Prova di partecipazione (PoS). La Prova di attività è essenzialmente una struttura alternativa per Bitcoin e rappresenta una combinazione di due dei meccanismi di consenso più diffusi: la Prova di lavoro e la Prova di partecipazione. La Proof of Activity è stata introdotta per placare i timori sulla fine del mining di Bitcoin una volta esauriti i 21 milioni di monete disponibili e integra la Proof of Work per aiutare a prevenire un attacco del 51%.

Questo meccanismo funziona partendo da un approccio di Proof of Work in cui i miner risolvono essenzialmente un puzzle crittografico e reclamano la loro ricompensa in caso di successo. La differenza sta nel fatto che i blocchi minati contengono solo intestazioni e indirizzi di ricompensa di mining invece di contenere transazioni.

La Proof of Activity, in sintesi, seleziona una coppia casuale dalla rete per firmare un nuovo blocco.

Questo metodo richiede uno scambio continuo di dati. Per ridurre il traffico, il “modello” del blocco non include l'elenco delle transazioni e, al suo posto, lo aggiunge l'ultimo firmatario. Come punto a sfavore, eredita lo svantaggio sia della Proof of Work che della Proof of Stake in termini di elevate risorse utilizzate e validatori malintenzionati. Tra le monete più popolari che lo utilizzano troviamo Decred (DCR) ed Espers (ESP).

Proof of Burn (PoB)

Il Proof of Burn è parallelo al concetto secondo cui è impossibile per qualcuno eliminare dati da una blockchain. Quindi, l'idea da sviluppare era quella di “bruciare” le monete. Consiste nel fornire prove che alcune monete sono state bruciate nel processo di invio di una transazione a un indirizzo che non può essere utilizzato. Questo metodo funziona solo con monete estratte da criptovalute Proof of Work. Gli utenti cercheranno di bruciare il maggior numero possibile di monete per poter “vincere” la ricompensa del blocco. Il più delle volte la Proof of Burn è stata introdotta per diffondere altre monete distruggendo il valore di una.
Si dice che il processo di selezione sia casuale, ma allo stesso tempo, si dice anche che più monete brucia l'utente, maggiori saranno le sue possibilità di

essere selezionato per estrarre il blocco successivo. Questo è simile al processo di Bitcoin, dove l'investimento risiede nella potenza di calcolo che deve essere migliorata per ottenere migliori hashrate.
Slimcoin (SLM) è il principale esponente di questo algoritmo. Anche TGCoin o Third Generation Coin, utilizzano l'algoritmo. Tuttavia, la moneta ausiliaria per Counterparty, un'estensione del software Bitcoin con funzionalità di monete colorate, è stata distribuita attraverso un processo di Proof of Burn. I partecipanti hanno dovuto inviare Bitcoin a un indirizzo non affidabile e hanno ricevuto in cambio token Counterparty.

Prova di capacità (POC)

La Prova di capacità è un meccanismo di consenso che utilizza un processo chiamato tracciamento. Con la Prova di lavoro, i miner utilizzano la potenza di calcolo per indovinare la soluzione corretta; tuttavia, con la Prova di capacità, le soluzioni vengono pre-memorizzate in archivi digitali (come i dischi rigidi). Questo processo è chiamato tracciamento. Dopo che un archivio è stato tracciato (il che significa che è stato riempito di soluzioni), è possibile partecipare al processo di creazione dei blocchi.
Chiunque abbia la soluzione più veloce per il puzzle di un (nuovo) blocco, può creare il nuovo blocco.

Maggiore è la capacità di archiviazione, più soluzioni si potranno memorizzare e maggiori saranno le probabilità di creare un blocco.
La prova di capacità comprende due parti distinte: il tracciamento (o la creazione dell'archivio dei plot) e l'estrazione effettiva dei blocchi. La dimensione del tuo disco rigido è il fattore che determina il tempo necessario per sviluppare gli archivi di tracciamento. Questo varia da alcuni giorni a un paio di settimane. Burstcoin è stato il primo a introdurre questo concetto. Altri esempi sono Chia, SpaceMint.

Prova del tempo trascorso (POET)

POET è un algoritmo di meccanismo di consenso spesso utilizzato nelle reti blockchain autorizzate per decidere i diritti di mining o i vincitori dei blocchi nella rete. Le reti blockchain autorizzate sono quelle che richiedono a ogni potenziale partecipante di identificarsi prima di potersi unire. Basato sul principio di un sistema di lotteria equo in cui ogni nodo ha la stessa probabilità di essere un vincitore, il meccanismo POET si basa sulla distribuzione equa delle possibilità di vincita tra il maggior numero possibile di partecipanti alla rete.
Questo meccanismo di consenso può funzionare solo se esiste un sistema per verificare che nessuno possa gestire più nodi contemporaneamente e che il tempo di attesa assegnato sia effettivamente

casuale. Senza un sistema di questo tipo, il meccanismo di consenso presenta gravi difetti. Essenzialmente, il flusso di lavoro è simile al meccanismo di consenso seguito dall'algoritmo Proof of Work (PoW) di Bitcoin, ma senza il suo elevato consumo energetico. Il caso più esemplare è Hyperledger Sawtooth, una piattaforma blockchain modulare, autorizzata e di livello aziendale.

Algoritmo di consenso Obelisk

Obelisk è un promettente algoritmo di consenso che mira a eliminare le carenze degli algoritmi Proof of Work (PoW) e Proof of Stake (PoS) e rende possibile mantenere lo stato della blockchain nella rete distribuita con una potenza di calcolo minima e senza necessità di partecipazione. Riduce la necessità di mining, migliora significativamente la velocità delle transazioni e offre una sicurezza potenziata.

Obelisk cerca di aggirare i problemi di PoW e PoS distribuendo l'influenza nella rete secondo un concetto chiamato “rete di fiducia”, in cui la densità della rete di sottoscrittori di un nodo determina la sua influenza sulla catena.

Il caso più esemplare di questo algoritmo di consenso lo troviamo nel progetto chiamato SkyCoin.

Proof of Assignment (PoA)

Si tratta di un meccanismo di consenso di nuova generazione che richiede meno potenza e può essere eseguito su hardware di fascia relativamente bassa. Il meccanismo di funzionamento del PoA consente alle applicazioni quotidiane dell'Internet delle cose (IoT) di essere utilizzate per funzioni di mining di base a capacità limitata. Grazie alla loro potenza di elaborazione integrata, i dispositivi compatibili con l'IoT possono essere utilizzati per il mining di criptovalute.

Tuttavia, dato che la memoria disponibile e la potenza di elaborazione su questi dispositivi sono limitate, il loro contributo al mining rimane modesto. Il meccanismo di funzionamento dell'algoritmo PoA facilita questo tipo di mining “leggero”.

L'esempio più degno di nota si trova nella blockchain IOTW, o su quella di IOTA.

Proof of Checkpoint (PoC)

Proof of Checkpoint è un sistema ibrido che combina un sistema Proof of Stake con un sistema Proof of Work. L'idea alla base di questo concetto è quella di mitigare gli attacchi al sistema Proof of Stake. Tuttavia, è ancora soggetto ad attacchi a un nodo che è rimasto disconnesso per un periodo di tempo prolungato e, a sua volta, può essere utilizzato per fornire informazioni false sulla blockchain.

Ogni x numero di blocchi nel sistema Proof of Stake richiede l'estrazione di un blocco Proof of Work. Ogni blocco Proof of Work non contiene transazioni ed è direttamente collegato sia alla rete Proof of Work che alla rete Proof of Stake.

Proof of Formulation (PoF)

Si tratta di un algoritmo di consenso proposto dalla piattaforma sudcoreana FLETA, denominato Proof of Formulation (PoF), cerca di risolvere le carenze di PoW (consumo energetico), PoS (vulnerabilità di sicurezza) e dPoS (centralizzazione) combinando il meglio di ciascuno in un unico meccanismo di consenso.

Nella Proof of Formulation (PoF), il mining e la generazione di blocchi avvengono in modo diverso rispetto alle piattaforme blockchain esistenti. I formulatori fungono da generatori di blocchi sulla piattaforma FLETA. Gli osservatori consentono la conferma in tempo reale dei blocchi generati ed evitano la doppia spesa (double spending).

I formulatori costituiscono la spina dorsale dell'algoritmo PoF. L'algoritmo PoF differisce dal PoW in quanto non richiede un'enorme potenza di calcolo e differisce anche dal DPoS, dove solo i delegati eletti possono partecipare al mining.

Grazie al breve tempo di blocco di soli 0,5 secondi, il mining è ad alta velocità, con soli quattro secondi per

blocco. Inoltre, nell'ecosistema di mining di FLETA, i blocchi vengono confermati istantaneamente tramite i Nodi Osservatori. Tra i cinque nodi di osservazione, tre di essi devono convalidare i blocchi immediatamente dopo la loro generazione, consentendo una rapida diffusione dei blocchi.

Grazie alla sua elevata scalabilità ottenuta tramite l'uso della tecnologia di frammentazione parallela e una struttura multi-chain indipendente,la piattaforma FLETA promette di essere un ambiente eccellente per lo sviluppo illimitato di Dapp separando le prestazioni della catena principale dal dominio dei dati: ció consente a ciascuna Dapp di operare in modo indipendente, riducendo i costi eccessivi di sviluppo ed esecuzione delle applicazioni decentralizzate.