Politecnico di Torino

Politecnico di Torino

Corso di Laurea in Ingegneria Informatica

Blockchain: un'analisi comparativa dei diversi protocolli

Tesi di Laurea Magistrale

Relatore:
Prof. Danilo Bazzanella

Candidato:
Federico Raimondi

Correlatore:
Dott. Jacopo Romagnoli

Anno Accademico 2021 – 2022

Sommario

Negli ultimi anni, grazie agli enormi investimenti nel settore, la tecnologia blockchain è evoluta a livello esponenziale in molteplici aspetti, portando sia all'innovazione dei protocolli esistenti che alla creazione di nuove soluzioni. La prima applicazione reale della blockchain avviene nel 2008, con la nascita di Bitcoin, un progetto volto alla decentralizzazione dei pagamenti peer-to-peer. Con l'aumento dell'adozione da parte di privati e aziende, sono stati sviluppati sempre più progetti blockchain, facendola diventare virale anche in altri ambiti e soluzioni, come ha fatto Ethereum che ha introdotto una piattaforma completamente decentralizzata di smart contract ed applicazioni. La presenza di centinaia di blockchain ha reso la scelta di un protocollo abbastanza complessa, serve chiarezza sullo scopo d'utilizzo ma allo stesso tempo bisogna trovare il giusto compromesso tra le varie proprietà. Definito da Vitalik Buterin, co-fondatore della rete Ethereum, il trilemma blockchain afferma infatti che non è possibile ottenere contemporaneamente le proprietà di scalabilità, decentralizzazione e sicurezza, senza sacrificare una di esse. La loro classificazione è complessa, in quanto ogni caratteristica include a sua volta vari aspetti che possono influire in modo significativo. Ad esempio, nella scalabilità, che indica la capacità della rete di evolversi all'aumentare delle risorse, sono fondamentali parametri come la latenza, il throughput o le commissioni delle transazioni. Allo stesso tempo, essa può dipendere dal protocollo di consenso utilizzato che influisce però direttamente anche sulle proprietà di decentralizzazione e sicurezza.

In particolare, in questa tesi, nella prima fase è stata analizzata la blockchain sotto ogni punto di vista, a partire dalla sua storia per poi entrare nello specifico delle sue componenti e funzionalità. Successivamente, è stato approfondito il protocollo Bitcoin, con una particolare attenzione alle sue potenzialità e limitazioni, che sono state utilizzate come metrica per il confronto con altri protocolli.

La seconda fase si è incentrata sul trilemma blockchain, con l'introduzione di alcune soluzioni per i protocolli già esistenti, e sull'analisi di Ethereum, Algorand e Solana. Essi sono stati classificati in base alle loro proprietà attuali, con un'attenzione anche dal punto di vista della sostenibilità ambientale.

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione

La blockchain è una delle tecnologie di maggiore successo in questi ultimi anni, con investimenti crescenti e opportunità di innovazione sempre più chiare in tutto il mondo. L'Harvard Business Review nel maggio 2016 aveva reso noto un articolo in cui si attribuiva proprio alla blockchain la maggior probabilità di introduzione di un cambiamento tecnologico. A fine 2018 inoltre, Forbes ha pubblicato un articolo intitolato "The Fourth Industrial Revolution Built On Blockchain And Advanced With AI", dove si ipotizzava come la blockchain poteva migliorare le inefficienze della tecnologia moderna, e come poteva guidare la quarta rivoluzione industriale se accoppiata all'intelligenza artificiale [1].

Questi sono stati evidenziati con il passare degli anni, grazie anche al supporto di grandi aziende che hanno delineato concretamente il futuro della blockchain con i loro investimenti.

Rispetto all'anno 2020, in cui la spesa totale dedicata allo sviluppo di questa tecnologia era di circa 500 milioni di dollari, tra settembre 2021 e metà giugno 2022 tale cifra è stata superata solamente dal singolo investimento di Alphabet con la cifra di 1,5 miliardi di dollari. Tra i principali investitori, nello stesso periodo, si distinguono inoltre BlackRock (1,17 miliardi), Morgan Stanley (1,11 miliardi), Samsung (979 milioni) e Goldman Sachs (698 milioni) [2].

Nonostante questo grande e crescente interesse degli ultimi anni, la nascita della blockchain risale a molto tempo fa, ed è riconducibile ai primi anni '90. Infatti, la prima volta che è stata descritta questa tecnologia è nel 1991 dai ricercatori Stuart Haber e W. Scott Stornetta, i quali avevano descritto una soluzione pratica per la marcatura temporale di documenti digitali, per fare in modo che non potessero essere retrodatati o alterati. Questo tramite una catena di blocchi protetta dalla crittografia. Un anno dopo, nel 1992 hanno aggiornato il sistema introducendo la struttura dati "Merkle tree" rendendo questa tecnologia più efficiente grazie alla possibilità di raccogliere diversi documenti in un unico blocco. Tuttavia, questa tecnologia è rimasta inutilizzata, e il brevetto è scaduto nel 2004 [3]. Quattro anni dopo però, nel 2008, la storia della blockchain inizia a guadagnare rilevanza, grazie alla creazione del Bitcoin.

Capitolo 2

La Blockchain

2.1 Definizione

La blockchain è un registro condiviso e distribuito che semplifica il processo di registrazione delle informazioni e il monitoraggio delle risorse di una rete, ad esempio, aziendale. In altre parole, si può immaginare come un database che, invece di memorizzare tutte le voci su un computer, memorizza i record e le transazioni, su diversi nodi [4].

L'idea di base della tecnologia blockchain, quindi, è di costruire una rete che non necessita di un'autorità centrale di controllo, ma che permetta di effettuare transazioni che siano sicure e non modificabili. Questo concetto ha stravolto un problema che coinvolge la società ogni singolo giorno, ossia riuscire a creare uno scambio tra persone che non si conoscono e non hanno motivo di fidarsi l'uno dell'altro, in modo totalmente autonomo e affidabile.

Le informazioni al suo interno possono essere facilmente consultate in qualsiasi momento, avendo la certezza di ottenere sempre dei dati aggiornati e non contraffatti. Le risorse possono essere sia immateriali come, ad esempio, proprietà intellettuali, brevetti e diritti d'autore che beni tangibili come una casa, un'automobile, soldi contanti, terreni e tanto altro. Praticamente qualsiasi cosa che possiede del valore intrinseco può essere tracciata e scambiata su una rete blockchain, riducendo i costi per tutti i soggetti coinvolti grazie alla mancanza di intermediari.

Ogni volta che avviene una transazione, essa viene archiviata sotto forma di un blocco di dati, che è condiviso tra più computer e non può essere modificato senza un accordo (consenso) dell'intera rete. I vari blocchi creati sono concatenati in ordine cronologico per formare una vera e propria catena, e da qui nasce il nome "blockchain", catena di blocchi. Per creare la catena viene utilizzata una funzione di hash. Lo scopo di questa funzione, in generale, è trasformare una stringa di lunghezza arbitraria in una sequenza di bit con lunghezza predefinita. Essa è veloce e facile da calcolare ma allo stesso tempo è irreversibile, deterministica e una piccola variazione dell'input, produce un notevole cambiamento dell'output. Inoltre, non può accadere che a dati differenti venga attribuito lo stesso valore di hash, e

questo permette di verificare se un dato è stato modificato, in quanto la funzione di hash calcolerà un valore completamente diverso da quello originale; quindi, per queste proprietà è utilizzata per verificare l'immutabilità di una informazione. Più precisamente, nella blockchain, ogni blocco include l'hash del blocco che lo precede creando così un collegamento che garantisce l'integrità del blocco precedente, via via fino al blocco "genesi", ossia il primo della catena.

2.2 Caratteristiche

Le opportunità che la tecnologia blockchain offre sono molteplici, ma nonostante questo è alquanto strabiliante la semplicità delle operazioni che si possono effettuare su di essa. L'attività fondamentale è quella di creare nuovi blocchi, che si traduce e semplifica nell'inserimento di nuove informazioni e nel recupero dei dati di cui si necessita. Non è assolutamente possibile modificare nessun dato, né tanto meno cancellarlo. Questo può essere fatto solamente aggiungendo un nuovo blocco con le informazioni aggiornate, ma che non elimina o nasconde la storia passata delle stesse.
La blockchain ha diverse proprietà, ma le principali su cui si basa possono essere riassunte in decentralizzazione, scalabilità e sicurezza.

2.2.1 Decentralizzazione

Come precedentemente discusso, è possibile identificare la blockchain come una base di dati distribuita, una DLT (Distributed Ledger Technology). In particolare, tutti gli utenti sono collegati tra di loro in una rete peer-to-peer, sono in possesso dell'intera catena di blocchi e quindi, il dato è ridondante su tutti i nodi. Ma il significato di "decentralizzazione" in questo contesto è legato al controllo e al processo decisionale, che viene trasferito da un'unica entità centralizzata a una rete distribuita composta da diversi nodi. Tutto questo è possibile grazie anche alla trasparenza, infatti tutti i partecipanti vedono le stesse informazioni, allo stesso tempo e possono visualizzare le intere operazioni svolte sulla blockchain, come ad esempio il trasferimento di moneta tra diversi utenti. Questa caratteristica rende possibile la definizione di una rete senza fiducia, che non indica la poca sicurezza ma piuttosto che gli utenti non hanno bisogno di fidarsi degli altri partecipanti per evitare frodi. Per poter funzionare, questo sistema necessità però di alcune regole. Esse sono descritte dal

protocollo di consenso, permettono di sincronizzare i vari nodi e creare una modalità di concordato condiviso per l'inserimento di nuove informazioni, di un nuovo blocco nella catena.
Infatti, è possibile registrare nuove transazioni soltanto quando il numero di approvazioni supera la maggioranza dei partecipanti alla rete, per evitare che un singolo utente prenda decisioni in autonomia introducendo informazioni potenzialmente dannose.

2.2.2 Scalabilità

Una caratteristica importante per le blockchain è la scalabilità, ossia la capacità del sistema di gestire un numero sempre maggiore di partecipanti mantenendo almeno costanti le prestazioni.
Se un protocollo è poco scalabile rischia di creare una congestione della rete, in quanto la crescita del numero dei nodi aumenta di conseguenza le richieste di esecuzione delle transazioni, che non riescono ad essere eseguite. Questo causa un rallentamento nelle tempistiche di conferma delle transazioni e un aumento significativo delle commissioni da pagare per farle eseguire, quindi riduce le prestazioni del sistema. Infatti, spesso questa proprietà viene confusa con le prestazioni del sistema, che vengono però misurate attraverso metriche quali il numero di transazioni al secondo o il tempo medio di conferma di una transazione. È importante distinguere i due termini in quanto molti approcci per il miglioramento delle prestazioni non intaccano affatto la scalabilità, in quanto non cambia la capacità del sistema di ottimizzare la sua esecuzione con l'aggiunta di altre risorse. La scalabilità richiede intrinsecamente lo sfruttamento del parallelismo.

2.2.3 Sicurezza

La sicurezza solitamente è proporzionale alla decentralizzazione del sistema e dal numero di partecipanti al network. Infatti, la blockchain è, per costruzione, sostanzialmente inattaccabile essendo impossibile compromettere contemporaneamente migliaia o magari milioni di utenti senza lasciare nessuna traccia, anche se ogni singolo utente non utilizza sistemi di protezione raffinati. Nella blockchain, nessun partecipante può manomettere una transazione una volta che qualcuno l'ha registrata nella catena. Se un blocco include un errore, è necessario aggiungere una nuova transazione per modificarlo, ed entrambe le transazioni sono e saranno visibili alla rete. Inoltre, ogni nuovo blocco si collega a tutti i blocchi precedenti in una catena crittografica irreversibile. Ogni blocco aggiuntivo

rafforza la verifica del blocco precedente e quindi dell'intera blockchain. In particolare, i blocchi contengono le transazioni e i dati del blocco precedente, questo significa che se voglio falsificare il blocco *t*-5 ad esempio, devo andare a modificare anche tutti quelli dopo. Questo perché il blocco *t*-4 punterebbe ancora al vecchio blocco e invaliderebbe tutta la catena. La conclusione è che più un blocco riceve a sua volta blocchi in coda, più diventa sicuro. Ma questo argomento differisce in base al tipo di blockchain che si prende in considerazione.

2.3 Tipologie di blockchain

Le blockchain possono differire sotto diversi aspetti e questo rende possibile la loro applicazione in ambiti molto diversi tra loro. In particolare, è importante, quando si parla di una rete di questo tipo, distinguere chi può partecipare e chi ha accesso ai dati. Queste differenze giocano il ruolo di discriminante per la classificazione delle tipologie di blockchain, che è possibile identificare in quattro diverse voci: pubblica, privata, ibrida, di consorzio.

2.3.1 Reti blockchain pubbliche

In questa rete chiunque possieda un computer può potenzialmente diventare un "nodo", cioè accedere alla rete, eseguire delle transazioni o partecipare alla verifica e creazione di un nuovo blocco. Per questo motivo questa tipologia viene definita anche "permissionless", senza permesso.
Le informazioni non sono archiviate in un registro unico ma distribuite su una rete peer-to-peer, rendendo il funzionamento della rete completamente trasparente e aperto. Nessun utente ha privilegi sugli altri né facoltà di alterare i dati salvati sulla catena, mantenendo uno dei cardini principali di questa tecnologia, l'immutabilità. Di fondamentale importanza diventa il protocollo di consenso, che valida il funzionamento corretto di tutto il sistema. Un esempio di applicazione di blockchain pubblica conosciuta è il Bitcoin.

2.3.2 Reti blockchain private

Dal punto di vista del funzionamento di base il sistema è identico, cioè si basa sempre su connessioni decentralizzate peer-to-peer, ma non è possibile per chiunque diventare un nodo e partecipare alla rete senza alcuna autorizzazione, quindi, sono decentralizzate solo parzialmente. Infatti, sono definite anche "permissioned" o "gestite", in quanto c'è la presenza di un'entità centrale che determina chi possa accedervi. Oltre a definire chi è autorizzato a far parte della rete, tale autorità definisce quali sono i ruoli che un utente può ricoprire all'interno della stessa. Solitamente queste reti operano in ambito ristretto, ad esempio quello aziendale, quindi, sono di dimensioni più piccole. Per questo motivo possono essere considerate le più veloci e le più economiche in quanto le transazioni sono verificate da un numero limitato di nodi.

2.3.3 Reti blockchain ibride

Come si può intuire dal nome, la blockchain ibrida è una fusione tra quella pubblica e quella privata. Su questa catena di blocchi coesistono un sistema pubblico in cui chiunque può avere accesso parziale alla rete ed una parte privata con accesso ristretto e limitato. Nello specifico, l'accesso a dati specifici o talvolta in generale la visione del registro delle transazioni non è pubblico, ma è regolamentato da una politica di autorizzazioni. Le applicazioni sono molteplici, per esempio, le aziende che effettuano la vendita al dettaglio possono decidere di mostrare al pubblico solo alcune delle informazioni del prodotto riguardante la filiera di produzione.

2.3.4 Reti blockchain di consorzio

Anche in questo caso si è di fronte ad una piattaforma che conserva elementi pubblici e privati, ma che a differenza delle blockchain ibride la parte "privata" non è nelle mani di una singola entità centrale, ma di più organizzazioni che condividono la responsabilità della gestione di una blockchain. Queste organizzazioni preselezionate stabiliranno chi può inoltrare transazioni o accedere ai dati.
Una blockchain di questo tipo è la soluzione ideale per un business aziendale in quanto tutti i partecipanti devono essere autorizzati e hanno una responsabilità condivisa.

2.4 Protocolli di consenso

Il protocollo di consenso è uno dei punti più delicati e più oggetto di attacchi di tutta la blockchain. Grazie alla sua struttura a catena, con ogni blocco che contiene l'hash del blocco precedente, e al fatto che l'intera catena è distribuita, la blockchain tende ad essere molto difficile da modificare fraudolentemente. Il punto più a rischio della struttura è l'inserimento di nuovi blocchi. Tutte le blockchain hanno necessità di un protocollo di consenso, cioè un algoritmo che permetta a tante persone che non si conoscono di accordarsi su cos'è un blocco valido da inserire nella rete, considerando il fatto che un certo numero di utenti potrebbero essere malevolo.
Esistono tanti protocolli di consenso, di seguito sono analizzati i principali.

2.4.1 Proof of work

Il primo dei sistemi ideato come creare un protocollo di consenso è la proof-of-work (PoW). Essa è una dimostrazione che l'utente ha svolto un determinato lavoro, attestando quindi il suo impegno e in un certo senso anche la sua affidabilità, diminuendo l'appetibilità ad attacchi che abusano del servizio, come ad esempio Denial of Service[1] (DOS). Essi sono comunque fattibili, ma i risultati sarebbero deludenti e i costi estremamente elevati.
Una caratteristica di questa tipologia di protocollo è la sua asimmetria, in quanto il lavoro deve essere moderatamente complesso per il richiedente del servizio ma veloce e facile da verificare per il fornitore per evitare rallentamenti. Esistono varie tipologie di PoW ma la forma più semplice è realizzata tramite la risoluzione di un problema crittografico e si può descrivere, semplicisticamente, nel seguente modo:

1. Dato un testo qualsiasi, si aggiungono dei caratteri casuali e si calcola la funzione di hash.
2. Se il risultato ottenuto è minore di un certo valore (target), la PoW termina e l'hash calcolato può essere usato come prova del lavoro svolto.
3. Se invece il risultato della hash è maggiore del target si riprende dal punto 1.

[1] Attacco mirato a sospendere/bloccare il servizio offerto dalla piattaforma esaurendo le risorse necessarie per il suo normale funzionamento.

Nella blockchain, il calcolo dell'hash viene effettuato sull'intero blocco. All'interno di esso è presente un campo denominato "nonce", che contiene un numero di quattro byte che viene fatto variare con lo scopo di ottenere output diversi dall'esecuzione della funzione di hash. L'unico modo per ottenere un output con le caratteristiche desiderate, quindi minore del target, è continuare a provarci in quanto per la natura stessa delle funzioni di hash non è possibile forzare il risultato in nessun modo. La PoW quindi, si basa solamente sulla potenza di calcolo, chi può fare più tentativi ha molte più probabilità di risolvere il problema.
La scelta del target è fondamentale in tal senso, perché si può modificare la probabilità di successo, e quindi si può rendere la PoW più o meno impegnativa. La difficoltà maggiore, infatti, è trovare l'equilibrio in quanto un problema troppo complesso richiederebbe molto tempo, le transazioni non verrebbero elaborate e il flusso si fermerebbe; ma allo stesso tempo un problema troppo semplice renderebbe la rete vulnerabile ad attacchi esterni.
I nodi sono denominati "miner", paragonati ai cercatori di oro che in passato andavano a caccia di pepite, che competono tra di loro sperando di essere i primi a risolvere il quesito in modo tale da ottenere il diritto di aggiungere il prossimo blocco alla blockchain e quindi, ricevere una ricompensa in criptovalute. Il problema principale della prova di lavoro sono i costi elevati. Il processo di mining richiede macchine altamente specializzate, capaci di risolvere in tempi brevi algoritmi estremamente complessi. Questi dispositivi non sono solo molto costosi, ma consumano enormi quantità di energia elettrica. Si tratta inoltre di una pericolosa minaccia alla decentralizzazione del sistema, in quanto solo una piccola fetta dell'utenza può permettersi questo genere di investimenti.

2.4.2 Proof of stake

Un altro tra i sistemi più utilizzati come protocollo di consenso è la proof-of-stake. Essa tiene in considerazione la quantità posseduta di una determinata criptovaluta, solitamente i token nativi della blockchain stessa, con l'idea di base che il nodo che detiene grandi somme di denaro ha tutto l'interesse a far funzionare il sistema. Più precisamente, gli utenti che partecipano devono bloccare una certa quantità di monete sulla rete, mettendole in staking[2].

[2] Congelamento di criptovalute in un wallet dedicato.

Ovviamente non si può usare semplicemente questa metrica per selezionare il validator[3] per l'inserimento del blocco, altrimenti tutti i blocchi sarebbero inseriti sempre dalla stessa persona. Sono stati creati quindi diversi metodi di selezione:

- Random: utilizza una funzione casuale, dove la maggior quantità di valuta in stake fa aumentare la possibilità di diventare il validator.
- Anzianità: si basa sul prodotto tra la quantità di monete possedute e il numero di giorni in cui tale somma è stata detenuta. In particolare, solo le monete che non sono state spese per almeno 30 giorni competono per la creazione del blocco successivo. Inoltre, l'ammontare utilizzato come scelta per la firma di un blocco ricomincia con anzianità pari a zero, come se fosse appena stato acquistato. Questa anzianità può anche decadere se il tempo del possesso diventa troppo grande, per evitare che somme consistenti e molto "anziane" possano dominare la blockchain.
- Velocità: per incoraggiare l'utilizzo della moneta, viene tenuta in considerazione maggiormente quanto essa viene spostata piuttosto che la quantità in possesso.

Quando un nodo viene scelto per creare il blocco successivo, verificherà se le transazioni nel blocco sono valide. Poi lo firma e lo aggiunge alla blockchain, ricevendo come ricompensa le commissioni di transazione del blocco stesso.

Proof-of-stake introduce molti vantaggi evidenti a discapito della PoW, dalla migliore efficienza energetica alla maggior decentralizzazione, sicurezza a scalabilità. Infatti, la PoS è incredibilmente più rispettosa per l'ambiente perché consuma molta meno energia grazie all'eliminazione dell'utilizzo della potenza di calcolo per il funzionamento del proceso. Questo depenna la necessità di acquisto di macchine fisiche, rendendo l'aggiunta di nuovi validator alla rete più economico, semplice, accessibile riducendo quindi drasticamente la latenza per approvare transazioni e produrre nuovi blocchi.

Rimane difficoltoso per i piccoli nodi assumere il ruolo di validator, perché gli slot dedicati a questo ruolo sono limitati e quindi è complicato avere una quantità di moneta in staking sufficiente ad essere competitivo nella selezione. Esiste un'alternativa a questa problematica che è la delega, dove è

[3] Nodo che si occupa della validazione dei blocchi.

possibile affidare la propria “potenza” di stake ad un altro validator, ottenendo una parte delle ricompense in base al contributo offerto.
La sicurezza della rete è elevata, grazie al blocco di moneta nella rete nessuno è incentivato ad elaborare transazioni fraudolente in quanto è possibile perdere una parte della quota che bloccata e il relativo diritto a partecipare in futuro al sistema. Quindi, finchè l’importo in staking è maggiore delle ricompense ottenute, il validator perderebbe più monete di quante ne guadagnerebbe con un’attività truffaldina.
La PoS ostacola anche schemi di attacchi informatici già noti, come l’attacco del 51% dove un nodo per controllare la rete deve possedere in staking una quota superiore alla metà di quella presente sul mercato. Ciò comporta un grande investimento nell’acquisto di moneta che, dopo l’attacco, potrebbe deprezzarsi, data la probabile perdita di fiducia da parte di tutti gli utilizzatori del sistema che magari decidono di uscire completamente dal mercato, vendendo tutta la criptovaluta posseduta. Questa situazione funge da deterrente per prevenire questa tipologia di attacchi, mantenendo ad un buon livello la sicurezza della rete. Il discorso però potrebbe essere totalmente diverso nel caso il prezzo di un token crollasse o la blockchain avesse una bassa capitalizzazione di mercato, in quanto diventerebbe conveniente acquistare almeno il 51% della moneta e prendere il controllo della stessa. Quindi è importante applicare questo protocollo di consenso sotto opportune valutazioni, per evitare effetti indesiderati.

2.5 Fork

Con il termine “fork” si indica il fenomeno di suddivisione della blockchain in diversi rami. Esistono diverse casistiche e motivazioni per il quale questo può succedere ma una prima classificazione importante da fare è la modalità in cui una fork può avvenire: in modo accidentale o intenzionale.

2.5.1 Fork accidentali

Questa tipologia di biforcazione accade quando due o più miners, nel caso della PoW, risolvono il problema crittografico allo stesso tempo. In tal caso, diversi nodi riescono ad inserire nella catena

blocchi non equivalenti tra loro, implicando quindi la suddivisione della catena e la creazione di nuovi rami.

A questo punto, non è chiaro su quale ramificazione continuare a lavorare quindi i nuovi blocchi sono considerati tutti come momentaneamente possibili. Sono gli stessi miners a prendere questa scelta, finché non si palesa su quale ramo la maggioranza ha deciso di continuare a lavorare.

I miners, infatti, pongono molta attenzione su questo avvenimento e tendono a spostarsi sulla biforcazione più lunga che ha la probabilità più alta di diventare quella definitiva. La motivazione che spinge a questa scelta è semplice, cercano di diminuire la probabilità di effettuare del lavoro che verrebbe considerato invano in quanto le transazioni contenute nei blocchi abbandonati non saranno mai validate. Se ciò non accade, i miners non ricevono le ricompense dal lavoro svolto e quindi avranno impegnato tempo e risorse senza remunerazione di alcun genere. Grazie a questo, le fork accidentali tendono a risolversi molto velocemente.

2.5.2 Fork intenzionali

La blockchain è basata su un insieme di regole per poter far funzionare correttamente il protocollo, e queste possono essere soggette a proposte di miglioramenti e/o modifiche da parte dei diversi nodi che potrebbero tradursi anche in cambiamenti importanti o addirittura radicali. In questo processo la natura della decentralizzazione richiede un accordo tra i vari partecipanti della rete, che, se non raggiunto, porta alla creazione di una biforcazione.

Pur condividendo l'intera cronologia della blockchain originaria, ogni fork è diretta in una nuova direzione e in base alla retrocompatibilità di questo nuovo protocollo generato si possono distinguere due tipologie di fork intenzionali: "soft fork" e "hard fork" [5].

- Soft fork: permette ai nodi nella rete che non aggiornano il software alla nuova versione di continuare a operare regolarmente; quindi, le transazioni eseguite con il nuovo protocollo devono essere riconosciute come valide anche con le vecchie regole. Sostanzialmente una soft fork non è una vera fork, nel senso che non causa una divisione della blockchain, che rimane unica. Questa fork permette di effettuare un aggiornamento del protocollo in modo graduale, accettando le "vecchie" regole per un certo periodo di tempo finché tutti i nodi non si allineano alle nuove direttive. (*Figura 1*)

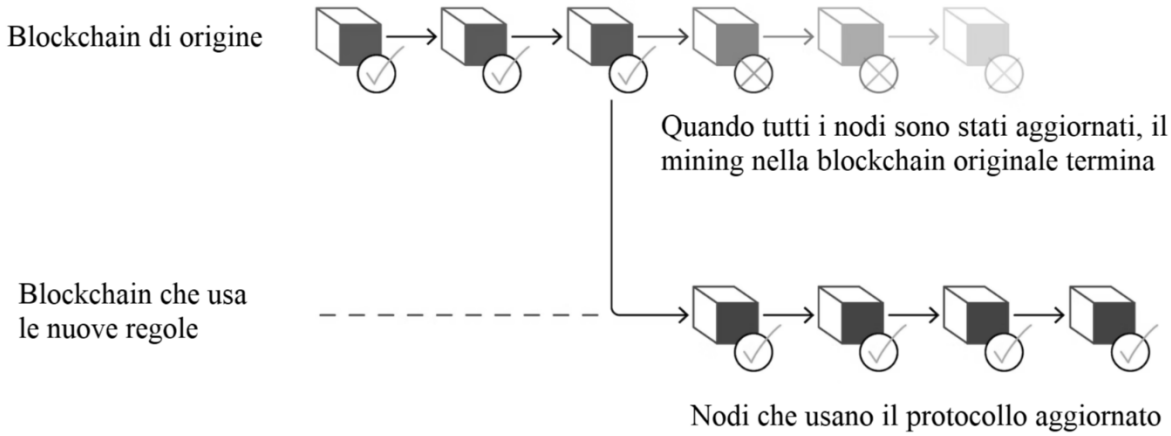

Figura 1: illustrazione funzionamento soft fork

- Hard fork: il nuovo protocollo non è compatibile con quello già presente, quindi, in questo caso la blockchain si divide in due, la blockchain originale e la nuova versione che segue le nuove regole, condividendo però tutti i blocchi fino al momento della suddivisione. Quindi dopo la fork ci sono due reti in esecuzione in parallelo che continueranno a propagare blocchi e transazioni, ma non stanno più lavorando sulla stessa blockchain. Di conseguenza anche la comunità a supporto della blockchain inziale tende a dividersi perché miners, sviluppatori e utenti devono decidere su quale delle due reti concentrarsi. (*Figura* 2)

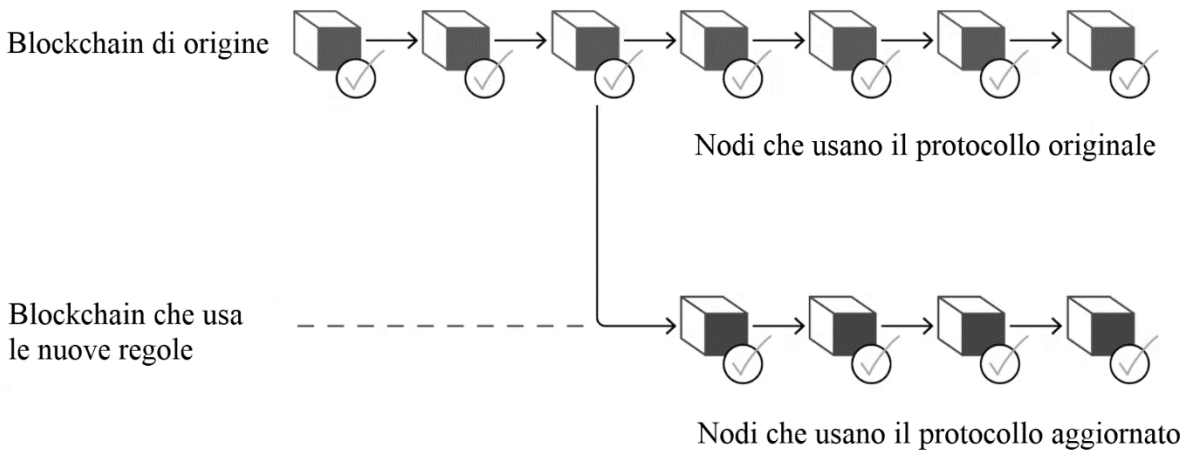

Figura 2: illustrazione funzionamento hard fork

2.6 Le criptovalute

Il primo utilizzo della blockchain rientra nel settore finanziario, con la creazione di token, ossia assets rappresentati digitalmente che possiedono valore, comunemente denominati criptovalute.
Più precisamente, una criptovaluta è una moneta digitale, utilizzata come mezzo di scambio o detenuta a scopo di investimento, che non esiste in forma fisica ed è decentralizzata; quindi, non sottoposta all'emissione, alla garanzia o al controllo da parte di banche centrali o autorità pubbliche. La criptovaluta, ove ci sia consenso tra i partecipanti alla relativa transazione, può essere scambiata in modalità peer-to-peer per acquistare beni e servizi, senza l'ausilio di intermediari.
Una volta emesse, le valute virtuali possono essere acquistate e vendute su piattaforme di scambio utilizzando denaro a corso legale (per esempio, EUR, USD, ecc.) o salvate in un "wallet".
La maggior parte delle criptomonete sono progettate per ridurre gradualmente la loro emissione, di conseguenza, solo un numero limitato di moneta sarà in circolazione per ogni determinata blockchain. Un bene che ha un flusso facilmente aumentabile non funziona bene come denaro, perché non appena si decide di utilizzarlo come moneta ci sarà l'incentivo immediato ad aumentarne la produzione, per arricchirsi, e se è possibile farlo senza troppo sforzo, il valore del denaro tenderà a diminuire. Inoltre, la sua logica decentralizzata, comparata con le valute ordinarie, rende le criptomonete meno suscettibili a confische da parte delle autorità senza particolari motivazione. Le transazioni effettuate con le criptomonete offrono un buon livello di privacy, grazie alla caratteristica di pseudonimia degli utilizzatori che varia a seconda del protocollo utilizzato.
Chiunque può creare una valuta digitale; quindi, in qualsiasi momento ci possono essere centinaia o persino migliaia di criptovalute in circolazione. Per creare/distribuire asset di questo tipo si può ricorrere ad una cosiddetta "initial coin offering" (ICO).

2.6.1 Initial Coin Offering

Una initial coin offering è un mezzo non ancora regolamentato per raccogliere fondi nel settore finanziario. Le ICO furono proprio lanciate per accumulare investimenti per nuove criptovalute, saltando la banca o gli operatori finanziari, andando a raccogliere liquidità (in criptomoneta) direttamente dalle persone. In tal caso questa ICO, rappresenta un investimento monetario che

consiste nell'acquisto di una criptovaluta prima che venga listata nel mercato, credendo nel progetto che sta alla base di questa nuova moneta digitale con la prospettiva di crescita e conseguente aumento di valore nel tempo.
In seguito, la finalità principale è diventata quella di finanziare direttamente delle idee imprenditoriali., offrendo al mercato un token (security token), che può rappresentare solo un diritto ad avere una remunerazione proporzionale al successo della start-up o essere a tutti gli effetti una sorta di azione, rappresentando quindi una quota di proprietà con l'annesso diritto di voto sulle decisioni gestionali future.

2.6.2 I Wallet

Per poter negoziare criptovalute, è necessario avere un software (o hardware) dedicato, detto "wallet". A differenza di quanto accade per i normali portafogli, che contengono effettivamente denaro contante, i portafogli di criptovaluta effettivamente non contengono la criptovaluta stessa e sono identificati da un codice alfanumerico. I fondi esistono nella blockchain, ed è possibile accedervi solo se si possiede una determinata "password", la chiave privata.
Infatti, alla base del funzionamento dei wallet c'è un sistema di chiavi:

- Chiave pubblica: rappresenta l'indirizzo di ricezione e viene inviata al mittente quando si vuole riceve un pagamento in criptovaluta.
- Chiave privata: dimostra la proprietà del denaro digitale e consente di effettuare transazioni. Essa è personale e deve essere conosciuta solo dal legittimo proprietario e quindi conservata in modo sicuro. La sua mancanza comporta l'impossibilità di utilizzo della criptovaluta, e quindi sostanzialmente la perdita della moneta.

Quindi, è molto importante mantenere al sicuro il portafoglio hardware o utilizzare un provider di portafogli online affidabile. Esistono diverse tipologie di wallet, si differenziano a seconda della piattaforma utilizzata, o a seconda del loro grado di autonomia nell'interazione con la rete:

- Desktop wallet: può essere utilizzato direttamente da un computer, è di semplice utilizzo ma la sua sicurezza dipende molto dall'attaccabilità del supporto hardware.
- Mobile wallet: è il tipo più comune e diffuso, permette di archiviare, inviare e ricevere criptovalute direttamente da smartphone, attraverso apposite applicazioni.

- Web wallet: sono accessibili tramite un browser web, e memorizzano tutte le informazioni, comprese le chiavi, su un server di proprietà di terzi. Potenzialmente poco sicuro, dipende dalla scelta del provider a cui ci si affida.
- Hardware wallet: le chiavi sono archiviate in una unità USB che viene collegata ad un computer quando si vuole utilizzare la criptovaluta. Queste periferiche sono appositamente progettate per gestire un wallet, e sono infatti considerate molto sicure.
- Paper wallet: le chiavi vengono scritte o stampate su un supporto fisico per la memorizzazione a lungo termine, è un sistema low-tech ma molto sicuro.

I primi tre sono denominati "hot wallet" perché sono sempre in rete; quindi, sono di facile accesso e utilizzo ma allo stesso tempo anche più semplici da raggiungere ad utenti malintenzionati.
Invece, gli altri sistemi descritti sono denominati "cold wallet", sopperiscono alla problematica di essere sempre online ma hanno funzionalità limitate, con il rischio che essi vengano persi e/o distrutti.
La scelta del dispositivo da utilizzare per accumulare e gestire criptovaluta non è semplice, molto spesso dipende dal tipo di utilizzo a cui è destinato e alle competenze tecnico-informatiche dell'utente. Infatti, nonostante tutte le proprietà di sicurezza dei vari wallet, un aspetto su cui porre attenzione è il fattore umano, che attraverso le sue scelte e azioni in questo ambito può facilmente compromettere la sicurezza della sua moneta.

Capitolo 3

Bitcoin

3.1 La nascita del Bitcoin

Un anonimo inventore, noto con lo pseudonimo di Satoshi Nakamoto, ha pubblicato a novembre 2008 un articolo intitolato "Bitcoin: A Peer-to-Peer Electronic Cash System" [6], nel quale ha definito la creazione di una criptomoneta digitale, anonima e distribuita, gestita da una rete peer-to-peer di utenti senza l'uso di un ente centrale. Nello stesso white paper[4], ha annunciato che aveva già programmato l'intero sistema per convincere sé stesso che poteva risolvere i problemi dell'ecosistema esistente.
In particolare, per differenziare i diversi concetti il termine Bitcoin si riferisce alla tecnologia blockchain mentre, bitcoin con l'iniziale in carattere minuscolo si riferisce alla criptovaluta.
L'identità del creatore è completamente anonima, ci sono diverse teorie su chi sia effettivamente Satoshi Nakamoto e da dove provenga, ma la realtà dei fatti indica che non si è a conoscenza nemmeno se si stia parlando di una persona o di un gruppo di utenti.
Prima della pubblicazione del white paper, il 18 agosto 2008, è stato registrato il dominio "bitcoin.org", il sito web dedicato a Bitcoin, dando inizio alla pubblicazione ufficiale del progetto.
L'evento che più di tutti ha preceduto una serie di cambiamenti senza precedenti è accaduto il 3 gennaio 2009, quando è stato creato il "genesis block", ossia il primo blocco della catena di Bitcoin, che ha incarnato la prima implementazione funzionante di una blockchain che il mondo aveva mai visto. In quel momento Bitcoin era visto da molti come un gioco destinato a poche persone, ma così non è stato, ha avuto rapidamente successo e i suoi utilizzatori sono aumentati significativamente in pochissimo tempo. Il 22 maggio 2010, è stata effettuato il primo pagamento in bitcoin di un bene materiale: due pizze, pagate diecimila bitcoin (BTC).

[4] Documento informativo, solitamente emesso da un'azienda, per promuovere o evidenziare le caratteristiche di una soluzione, di un prodotto o di un servizio.

3.2 Obiettivi del protocollo

Fino a quel momento, i pagamenti elettronici si affidavano esclusivamente alle istituzioni finanziarie, principalmente banche, che garantivano il corretto funzionamento del sistema.
Bitcoin ha voluto rivoluzionare questo ecosistema, riducendo i costi di intermediazione ed eliminando direttamente la necessità di coinvolgimento di terze parti. Questo per essenzialmente due motivi: abbassare i costi del servizio e rendere più sicuri i pagamenti.
Uno dei vantaggi di questa tecnologia è la capacità di rendere le transazioni non reversibili, una volta che sono andate a buon fine, infatti, non si possono più manomettere. In questo modo viene ridotta ai minimi termini la doverosa fiducia nei confronti dell'altro nodo coinvolto nella transazione, che era garantita dalla presenza dell'intermediario, ma che non è più necessaria perché ci pensa direttamente la blockchain a rendere intrinsecamente sicura la negoziazione.

3.3 Il back-end di Bitcon

3.3.1 Le transazioni

Uno degli elementi più importanti di Bitcoin è la transazione. Essa è un trasferimento di denaro, in questo caso criptovaluta, da un indirizzo A ad un indirizzo B.
Ogni transazione contiene al suo interno diverse informazioni:

- "Lock time": tempo da attendere per poter eseguire la transazione. Se maggiore di zero però, non fornisce nessuna garanzia che il pagamento alla scadenza verrà effettuato.
- "In-Counter": numero di indirizzi di input.
- "Input": lista di indirizzi e relativi valori, precedentemente ricevuti e non spesi, che verranno utilizzati come debito di pagamento.
- "Out-Counter numero di indirizzi di output.
- "Output": lista di indirizzi e relativi valori, che indicano le destinazioni e il valore da coprire con la transazione.

Questa transazione viene firmata con la chiave privata del mittente, per dimostrare che esso può effettivamente spendere quei bitcoin, e inviata nella rete dove i nodi si occupano di validare la firma crittografica e l'ammontare delle cifre coinvolte.

La blockchain di Bitcoin è costituita da un enorme elenco di questi messaggi, collegati tra di loro mediante una catena di firme digitali, infatti, è possibile ripercorrere a ritroso tutte le transazioni, fino ad arrivare all'origine dei bitcoin. Chi vuole trasferire denaro, firma digitalmente l'hash della transazione precedente e la chiave pubblica del proprietario successivo (*Figura 3)*.

In questo modo, tramite la così detta "transaction chain", è possibile tenere traccia dei cambiamenti di proprietà della moneta. Inoltre, ogni transazione è caratterizzata da una "transaction fee" che indica il prezzo che chi scrive la transazione è disposto a pagare per vedere realizzata la sua operazione. Essa non è indicata esplicitamente, e può essere anche nulla, ma si può ricavare facendo la differenza tra la somma degli input e la somma degli output. È un parametro che usano i miners per scegliere quali transazioni eseguire e quindi, di conseguenza, va a determinare la velocità di inserimento della transazione nella catena. La priorità dell'attività del miners ovviamente è il profitto, quindi hanno precedenza le transazioni con margini di guadagno superiori.

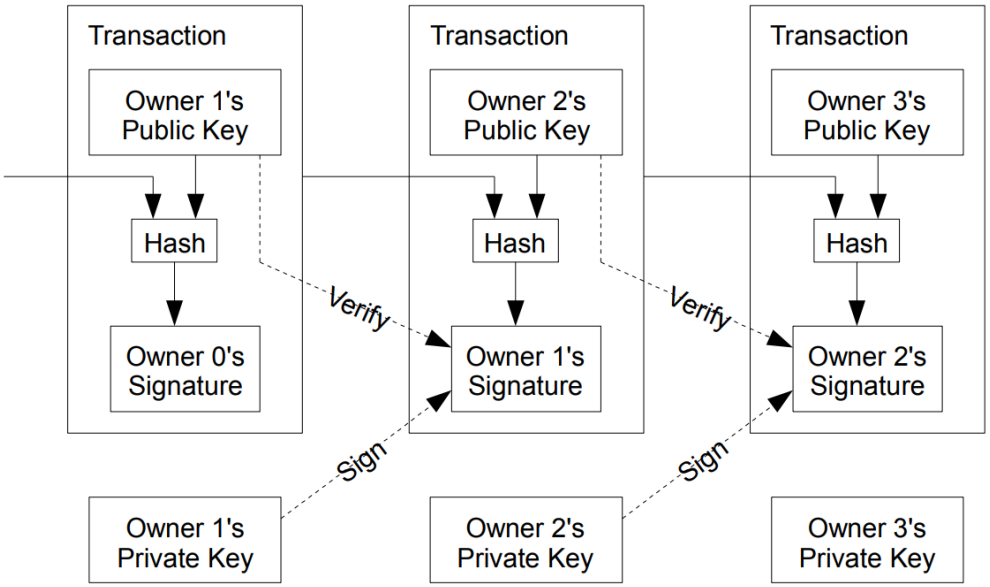

Figura 3: catena di transazioni

3.3.2 Lo schema a blocchi

Le transazioni non sono inserite all'interno della blockchain una alla volta, ma sono prima raggruppate in gruppi, chiamati blocchi. Un blocco ha una dimensione complessiva di 1MB ed è composto da due parti: l'header e il body, dove il primo include dei campi per la gestione del blocco stesso e l'hash dell'header del blocco precedente (*Figura 4*), mentre il secondo contiene la lista delle transazioni che devono essere validate dalla rete

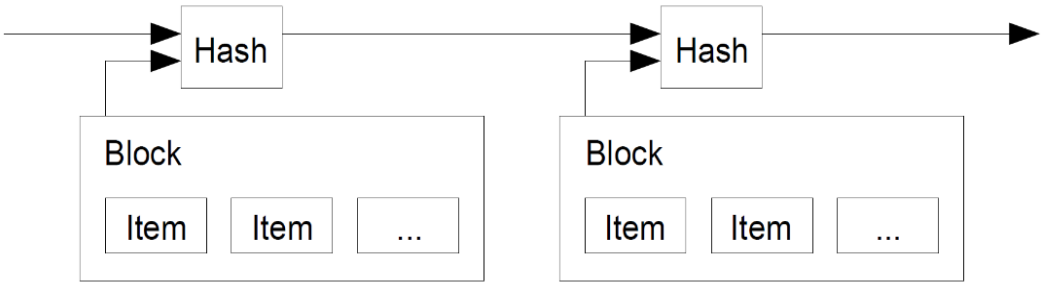

Figura 4: collegamento dei blocchi

3.3.3 Il suo funzionamento

Per poter eliminare l'intermediazione di un ente finanziario, bisogna risolvere tutte le complicazioni ad esso correlate. Uno dei potenziali problemi da prevenire è il "double spending", ossia la possibilità di utilizzare più volte la stessa moneta, che nei sistemi centralizzati viene controllato direttamente dalla banca o dall'intermediario incaricato di gestire la transazione. In una rete peer-to-peer, ogni nodo deve aver la capacità di verificare direttamente se, per esempio, la criptovaluta che ha ricevuto è stata mandata simultaneamente a qualcun altro, per evitare di essere truffato.
La soluzione proposta da Satoshi Nakamoto descrive l'utilizzo di un server di timestamp[5] distribuito, che genera una prova computazionale dell'ordine cronologico delle transazioni.
Per ottenere questo risultato, le transazioni devono essere disponibili pubblicamente ma questo è garantito dal fatto che tutti i nodi ricevono ogni nuova transazione che viene creata.

[5] Sequenza di caratteri che rappresenta una data e/o un orario per accertare l'effettivo avvenimento di un certo evento.

Poi, occorre un sistema che consenta ai partecipanti della rete di concordare sull'ordine di ricezione delle varie transazioni e sull'inserimento di un nuovo blocco. Ogni nodo, quindi, raggruppa le nuove transazioni che gli arrivano in un blocco, che, una volta completato viene inserito come input al server di timestamp, il quale lo marca temporalmente. Quindi, tutte le transazioni al suo interno verranno considerate accadute allo stesso momento.

A questo punto, per poter inserire il blocco nella blockchain entra in gioco il protocollo di consenso, che nel caso di Bitcoin è la Proof- of-Work (PoW). Dopo i vari tentativi di risoluzione, tramite la modifica del "nonce", alla scoperta del risultato corretto il nodo invia il blocco alla rete, i peer che lo ricevono controllano la validità di tutte le transazioni al suo interno e poi, se ritenuto corretto, lo aggiungono alla catena. (*Figura 5*)

La dimostrazione di accettazione del blocco da parte del nodo è l'utilizzo del suo hash nella creazione del blocco successivo; confidando che la catena possa proseguire per quella strada.

È possibile che più nodi validino un blocco allo stesso tempo, creando una biforcazione (fork) della catena. In generale, però, i nodi considerano come ramificazione corretta quella più lunga, quindi continueranno a lavorare su quella, ed eventualmente cambieranno ramo se si accorgono che ne esiste una più estesa. Ogni nuovo blocco che viene inserito nella catena conferma le transazioni dei blocchi precedenti e Bitcoin, in particolare, considera che una transazione confermata deve avere almeno sei blocchi in successione al blocco di appartenenza.

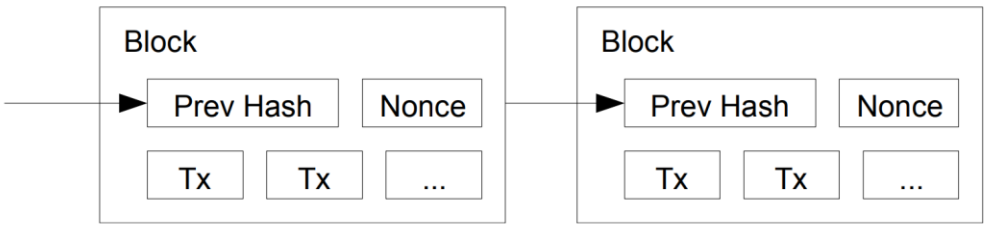

Figura 5: contenuto e collegamento dei blocchi

3.3.4 Tipologie di nodi

- Full-node client: ogni nodo di questo tipo memorizza l'intera blockchain (quindi tutte le transazioni di tutti gli utenti dall'inizio di Bitcoin), e gestisce tutti gli aspetti del protocollo, compresa la verifica di tutte le transazioni che vengono proposte alla rete. Sono richieste delle caratteristiche per poter essere un nodo di questo tipo, tra cui un minimo di GB di RAM, di spazio libero su disco, e una connessione a internet ad alta velocità. Ma non solo, è richiesta anche un'attività giornaliera di almeno sei ore.
- Light client: noto anche come simple-payment-verification (SPV), non memorizza l'intera blockchain ma solo gli header di tutti i blocchi e si connette ai full-node per avere le informazioni sulle transazioni. Questo collegamento è necessario per verificare se chi vuole eseguire un pagamento ha in effetti ricevuto a sua volta su quell'indirizzo abbastanza bitcoin senza averli già spesi, in quanto serve l'intera blockchain. Può però autonomamente creare, verificare e inviare transazioni alla rete Bitcoin.

3.3.5 Protocollo di consenso di Bitcoin

La tecnologia di Bitcoin utilizza come protocollo di consenso la proof-of-work. La funzione utilizzata per il calcolo dell'hash è SHA-256, e i vincoli che l'output deve soddisfare mirano ad un certo numero di bit iniziali pari a zero. Più questo numero è basso, più è semplice la risoluzione dell'enigma. Infatti, la rete aggiusta periodicamente il target, più precisamente ogni 2.016 blocchi, in modo tale da tenere sotto controllo la loro aggiunta, attestando una velocità media di un blocco ogni dieci minuti. Questo perché se venissero inseriti troppo rapidamente si potrebbero creare lunghe biforcazioni, che potrebbero durare molto tempo, allungando di conseguenza i tempi per avere la certezza matematica che la transazione non finisca in un blocco abbandonato. Considerando i vincoli del protocollo alla dimensione dei blocchi, Bitcoin riesce ad elaborare mediamente circa sette transazioni al secondo. Per un confronto diretto, Visa ha una velocità di punta di circa 24000 operazioni al secondo e PayPal di quasi 200 quindi le prestazioni in questo campo sono minori rispetto alle soluzioni centralizzate.
Per incentivare i miners alla risoluzione del problema e quindi al diritto di poter inserire il blocco nella catena, oltre alle fee di tutte le transazioni nel blocco, c'è una ricompensa di 6,25 bitcoin.

Questa ricompensa si dimezza ogni quattro anni, con un processo che viene denominato “halving”, nel 2009 si ottenevano ben 50 bitcoin e nel 2024 questo premio si deprezzerà a 3,125 bitcoin. Come già visto precedentemente, ogni blocco raggruppa un insieme di transazioni ma la prima è diversa dalle altre. Viene definita “coinbase transaction” e le sue peculiarità sono che l’input è un indirizzo speciale, detto “coinbase”, che non corrisponde all’output di nessuna precedente transazione, e che il suo output contiene uno o più indirizzi bitcoin del miner che ha inserito il blocco, per un totale di criptomoneta definita dal protocollo. È proprio questo il modo in cui vengono creati i bitcoin, in quanto questa ricompensa arriva dal “nulla”. Inoltre, il campo “coinbase” con il passare del tempo ha assunto un ulteriore utilizzo. Vista la crescita del livello di difficoltà nel risolvere il problema per aggiungere un blocco, il “nonce” non era più sufficiente per trovare la soluzione; quindi, è stato utilizzato quel campo come sorgente di altri valori, che funzionavano sostanzialmente da “extra nonce”. È facile verificare che a gennaio del 2140, si raggiungerà il limite massimo dei 21 milioni di bitcoin e i miners non avranno più nessuna ricompensa per i blocchi minati in aggiunta alle commissioni delle transazioni. Questo potrebbe portare ad un progressivo aumento delle “fee” per incentivare sufficientemente i miners a lavorare. L’aumento nell’utilizzo di questo protocollo, ha portato alla nascita di alcuni circuiti integrati specifici, detti ASICS (Application Specific Integrated Circuit), che hanno una progettazione focalizzata sulla risoluzione di un unico problema e consentono quindi di raggiungere delle prestazioni in termini di velocità e consumo elettrico difficilmente ottenibili con l’uso di soluzioni più generiche. Alcune criptomonete per rispondere al rischio di centralizzazione dovuta alla diffusione degli ASICS hanno adottato una PoW ideata con l’obiettivo di non essere eseguibile con ASICS. In media, per un computer standard, ci possono volere anni affinché esso possa risolvere un blocco; infatti, sono nate le “mining pool” che permettono ai miners di lavorare collettivamente dividendosi le ricompense in base al contributo fornito. Far parte di un mining pool è molto positivo per un miner, perché ottiene remunerazioni più uniformi e prevedibili, ma l’aumento di queste sta creando un livello di aggregazione che va contro la filosofia e la forza della blockchain, che è la decentralizzazione. C’è il concreto rischio che il controllo del protocollo di consenso per l’inserimento dei nuovi blocchi finisca in poche mani, con il conseguente problema per la sicurezza della blockchain.

3.4 Le limitazioni nel suo utilizzo

3.4.1 Consumo energetico, falso mito?

Una delle principali limitazioni, dato l'utilizzo della proof-of-work, è il costo economico e ambientale che l'esecuzione del protocollo comporta. Secondo il "Cambridge Bitcoin Electricity Consumption Index (CBECI)" [7] mediamente Bitcoin consuma attualmente circa 87 TWh all'anno. Questo valore è considerevole e rappresenta lo 0,65% di tutta l'energia globale [8], diventando quindi paragonabile annuale elettrico di interi stati. Infatti, nella *Tabella 1* che riporta i consumi elettrici annuali di diversi paesi e aziende nel 2019, è possibile notare che la Norvegia consumava in media 124TWh mentre un'azienda come Google solamente 12TWh.

Nome	**Popolazione (Milioni)**	**Consumo annuale elettrico (TWh)**
Cina	1443	6,453
Stati Uniti	330	3,990
Germania	83	524
Norvegia	5,4	124
Bitcoin	-	87
Bangladesh	165,5	71
Svizzera	8,5	56
Google	-	12
Facebook	-	5

Tabella 1: comparazione consumo elettrico annuale

Diventa difficile sostenere che Bitcoin non consuma una grande quantità di energia per il suo funzionamento, ma bisogna tenere in considerazione anche il suo obiettivo e la qualità del servizio che mette a disposizione. Infatti, è grazie alla enorme computazione che svolge che riesce ad offrire un livello di sicurezza non eguagliabile al momento.

Inoltre, un dato importante da sottolineare è sicuramente il confronto diretto con i classici sistemi di pagamento centralizzati. In questo caso, bisogna tenere in considerazione tutti gli aspetti coinvolti nei classici sistemi come, ad esempio, la gestione del denaro contante nei sistemi ATM, i pagamenti con la carta di credito, i pagamenti nei punti vendita (POS) e il consumo di energia di tutto l'ecosistema bancario e interbancario. Questo tema è stato approfondito da Micheal Khazzaka, con la pubblicazione di uno studio intitolato "Bitcoin: Cryptopayments Energy Efficiency" [9], in cui ha dimostrato che Bitcoin in media consuma almeno ventotto volte meno energia dei classici sistemi di pagamento. In particolare, il consumo per tutti i sistemi monetari e di pagamento classici si attesta circa a 2252,72 TWh all'anno. Questo dimostra che lo studio e il confronto tra i vari sistemi è molto complesso e occorre valutare i singoli dati contestualizzandoli nel contesto in cui li si sta valutando.

3.4.2 Privacy

Nella blockchain di Bitcoin tutte le transazioni sono salvate in chiaro. Essa si definisce "pseudoanonima" perché in ogni transazione sono indicati gli indirizzi bitcoin di input e di output ma non è noto a quali persone fisiche appartengano tali indirizzi; quindi, non è possibile collegare le transazioni a nessuno. Questo però può accadere quando si vogliono trasformare i bitcoin in una valuta fiat, come per esempio l'euro. Per cifre importanti l'unica soluzione è utilizzare un exchange[6] centralizzato, che per legge chiede l'inserimento dei documenti di riconoscimento e quindi la dichiarazione di un'identità. In questo passaggio si perde l'anonimato dei bitcoin. L'unico modo per tenerli anonimi e nascosti è non interagire con indirizzi e con wallet che hanno seguito la procedura KYC[7]. Anche in questo caso però, alcuni collegamenti sono ancora inevitabili.
Ogni persona accumula criptovaluta, bitcoin in questo caso, tramite delle transazioni che hanno come output un indirizzo associato al proprio wallet. Questo perché i portafogli di Bitcoin possono generare molti indirizzi diversi, e anonimi per la blockchain in quanto non ha modo di sapere a quali wallet o a quali persone appartengano quelli indirizzi.

[6] Sono piattaforme online che permettono di acquistare o vendere tutte le principali criptovalute presenti nel mercato.
[7] "Know Your Customer", è l'insieme di procedure mirate all'acquisizione di dati certi, quali l'identità dei clienti/utenti.

In questi indirizzi vengono raccolte le UTXO[8], ossia gli output delle transazioni ricevute che non sono ancora stati utilizzati. Esse sono tutte entità separate all'interno del portafoglio, a tal punto che se si ricevono cinque transazioni da 0,2 BTC si ha un totale di 1 BTC che però è diverso di ricevere direttamente la stessa cifra in un'unica transazione anche se l'importo è il medesimo. Questa differenza si nota nel momento in cui bisogna effettuare una transazione; quindi, quando bisogna usare una o più UTXO per coprire l'importo dovuto. La scelta degli output non spesi contenuti nel wallet influenzano la privacy e le commissioni della transazione [10].

In particolare, per la privacy, quando sono specificati più indirizzi di input si sta dichiarando automaticamente che lo stesso proprietario possiede più indirizzi bitcoin. Inoltre, se viene utilizzata una UTXO con un valore superiore dell'ammontare della transazione, si richiede automaticamente il resto che viene inviato come nuovo UTXO. A questo punto, possono nascere considerazioni quali che l'utente possiede sicuramente, almeno, il resto di quella transazione nel proprio wallet e che quell'importo sarà molto probabilmente utilizzato in futuro come indirizzo di input.

Essendo la blockchain pubblica in cui tutte le transazioni sono visualizzabili, è possibile tracciare il movimento di questa criptovaluta e monitorare le transazioni future in cui essa verrà impiegata.

Per ridurre questi collegamenti logici si potrebbero usare indirizzi sempre diversi quando si deve ricevere bitcoin, arrivando ad avere un solo UTXO per indirizzo in modo tale che il mittente non possa fare queste considerazioni. Se poi questi, però, verranno utilizzati come input per un'unica transazione si vanifica tutto il lavoro di protezione della privacy fatto fino a quel punto.

Inoltre, l'utilizzo di maggiori quantità di indirizzi di input comporta dei maggiori costi di transazione, in quanto parzialmente essi sono calcolati anche tenendo in considerazione la quantità di dati richiesti per la transazione, che include il numero di input e il numero di output.

La soluzione perfetta sarebbe di essere a conoscenza di quanti bitcoin serviranno in futuro per ogni transazione in modo tale da archiviare un singolo UTXO in un singolo indirizzo per l'importo esatto di cui si avrà necessità, ma è difficilmente applicabile. Un'alternativa fattibile sfrutta lo stesso concetto di base, con l'archiviazione di UTXO di varie dimensioni in modo tale da avere un'ampia scelta nel momento in cui si desidera utilizzare bitcoin come mezzo di pagamento.

[8] "Unspend Transaction Output", quantità di criptovaluta che si riceve dopo l'esecuzione di una transazione che può essere utilizzata come input in una nuova transazione.

3.4.3 Prestazioni

Il problema più rilevante, dato l'obiettivo della sua nascita, è sicuramente la lentezza e la scarsa scalabilità che offre alla sua rete. Le prestazioni del sistema blockchain vengono valutate solitamente in base a due dimensioni, la latenza e il throughput: la prima misura la velocità con cui una transazione viene confermata e validata mentre la seconda misura il numero transazioni che vengono effettuate in un determinato lasso di tempo [11]. L'utente medio, nella valutazione di una blockchain, valuta maggiormente la latenza e le commissioni di transazione, quindi ricerca un protocollo in cui le transazioni vengano confermate nel modo più rapido e a minor costo possibile.

La latenza è una metrica complessa da misurare, in quanto in momenti diversi si possono ottenere risultati discrepanti tra di loro. Uno dei fattori che può incidere in questa misurazione è il "batching", ossia il processo di raggruppamento delle transazioni in un unico blocco.

Un nodo Bitcoin inserisce le nuove transazioni che riceve in un blocco fino all'esaurimento dello spazio; quindi, alcune transazioni devono attendere il completamento del blocco, altre aggiungendosi alla fine vengono confermate immediatamente e non subiscono nessuna latenza dovuta dal processo. In ogni caso, il tempo che intercorre tra la creazione di due blocchi è di dieci minuti, quindi il tempo medio per la conferma di una transazione, a livello teorico, si stima essere circa la metà quindi almeno cinque minuti. Prendendo le statistiche reali di questo dato, in particolare la mediana di ogni giorno dal 1° gennaio 2022 al 25 novembre 2022 (*Figura 6*) e calcolando successivamente la media dei valori raccolti si ottiene un risultato di 7,14 minuti. Per la misura giornaliera è stata utilizzata la mediana in quanto possono presentarsi dei dati molto estremi che altererebbero la misura della media; quindi, per questa tipologia di distribuzione fortemente asimmetrica la mediana fornisce un risultato più affidabile.

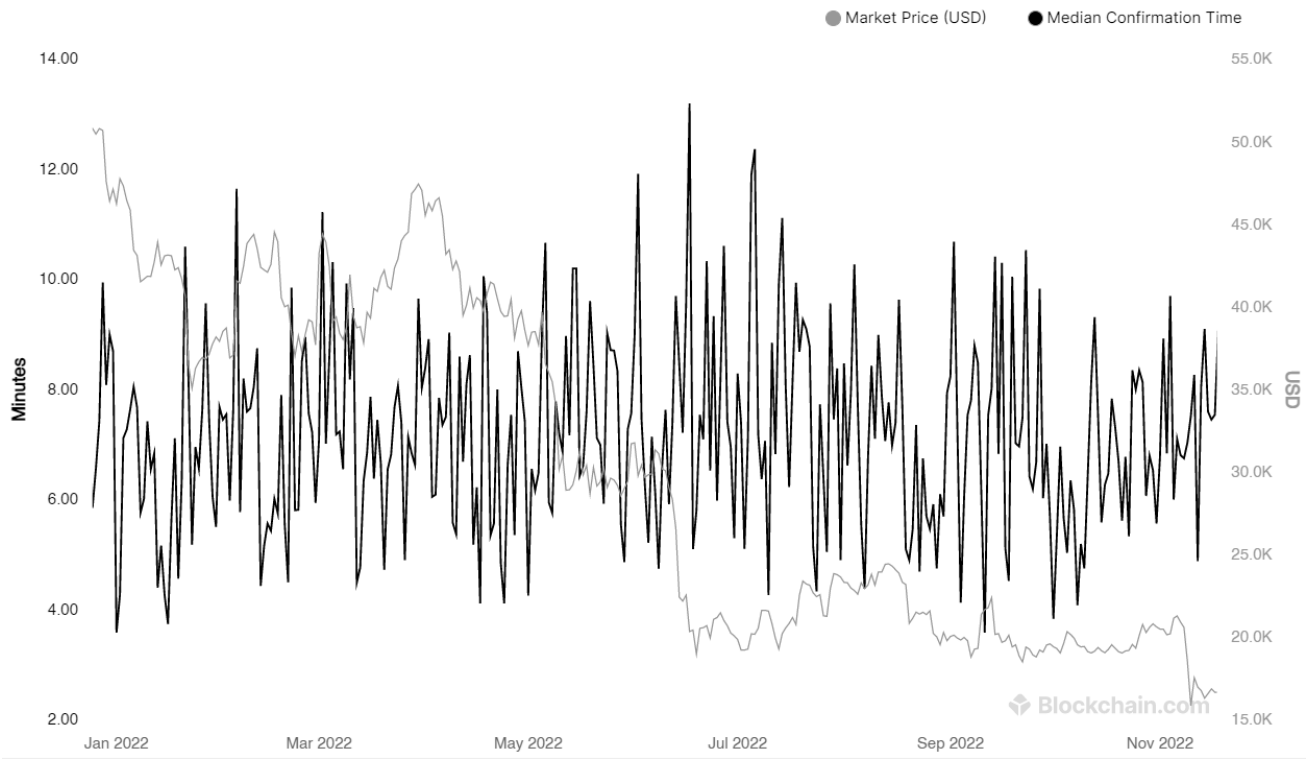

Figura 6: mediana giornliera del tempo di conferma delle transazioni Bitcoin nel 2022

Per quanto riguarda il throughput invece, si utilizza lo standard delle "transazioni al secondo", TPS (Transaction Per Second). Anch'esso soffre di problemi di misurazione in quanto le transazioni non sono tutte uguali, soprattutto nelle blockchain che offrono una programmazione generica.

Bitcoin processa solamente sette transazioni al secondo, che paragonato alle prestazioni dei circuiti bancari presenti nel mercato risulta notevolmente basso. In media, Mastercard ha la capacità di processare 5000 transazioni al secondo, mentre Visa ha dichiarato, in una recente intervista, di poter gestire ben 24.000 transazioni al secondo per un totale di 150 milioni ogni giorno [12][11].

Questo limitato valore di TPS in Bitcoin causa, di conseguenza, l'aumento delle "fee" nelle situazioni di alta domanda di processazione delle transazioni. Nell'aprile 2021, in contemporanea all'aumento vertiginoso del prezzo di bitcoin, queste commissioni hanno raggiunto un record storico di 62 dollari per transazione (Figura 7). Da quel momento però sono scese vistosamente, fino a raggiungere nell'ultimo anno la media di circa 1,63 dollari per transazione.

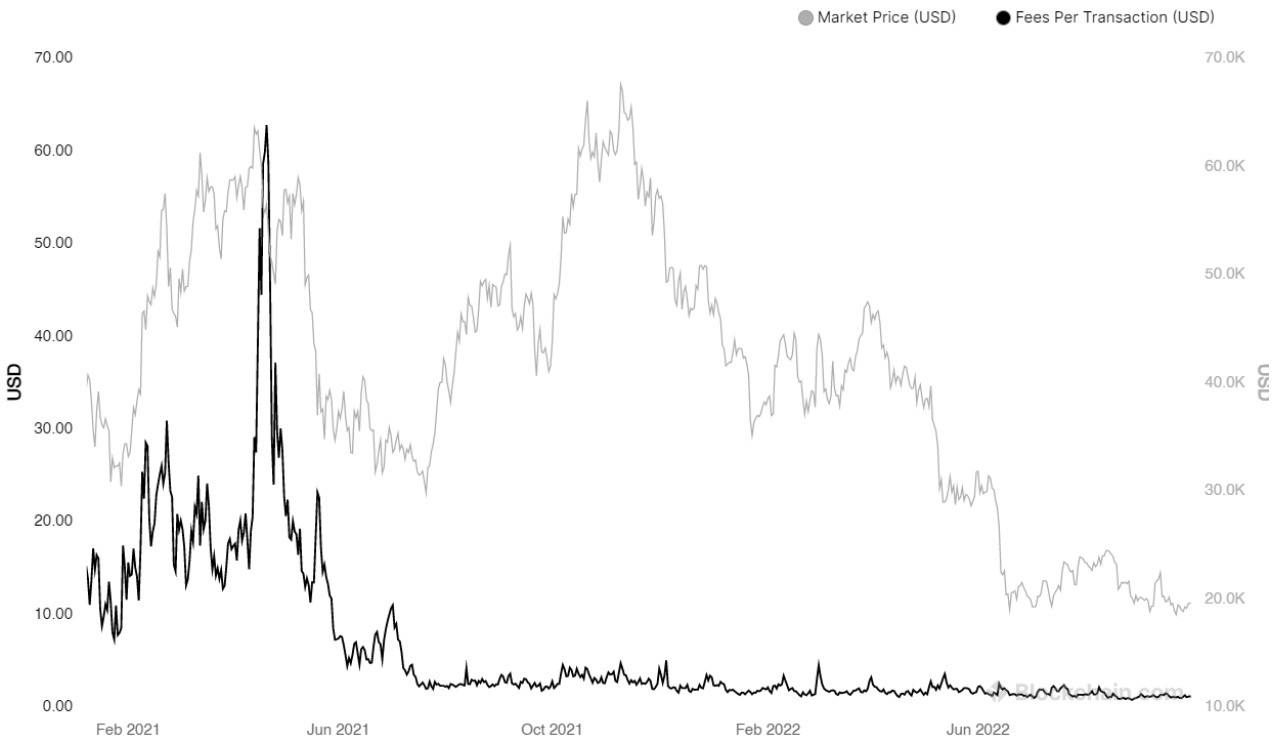

Figura 7: commissioni per transazione Bitcoin

Questi importi però, che vengono visti dagli utenti finali solamente come costo, servono a ricompensare adeguatamente i vari miners che permettono l'esecuzione della blockchain, scoraggiando comportamenti scorretti. La difficoltà sta nel trovare un giusto bilanciamento in modo tale da avere un costo di transazione competitivo con il mercato che non vada però a diminuire la sicurezza della rete.

Attualmente quindi, Bitcoin è un'ottima tecnologia con una limitazione spiccata per la scalabilità, in quanto a livello di sicurezza e decentralizzazione offre buoni risultati, come riassunto nella *Figura 8.*

Questo non è un problema di semplice risoluzione, perché anche riducendo il tempo di inserimento tra un blocco e l'altro si rischierebbe di creare delle "fork" più lunghe con possibili conseguenze per la sicurezza e per la latenza. Oppure si potrebbe pensare di aumentare la dimensione dei blocchi, in modo tale che possano contenere un numero maggiore di transazioni, ma questo intaccherebbe la scalabilità perché non sarebbe alla portata di tutti i nodi l'archiviazione dell'intera blockchain di dimensione maggiorata.

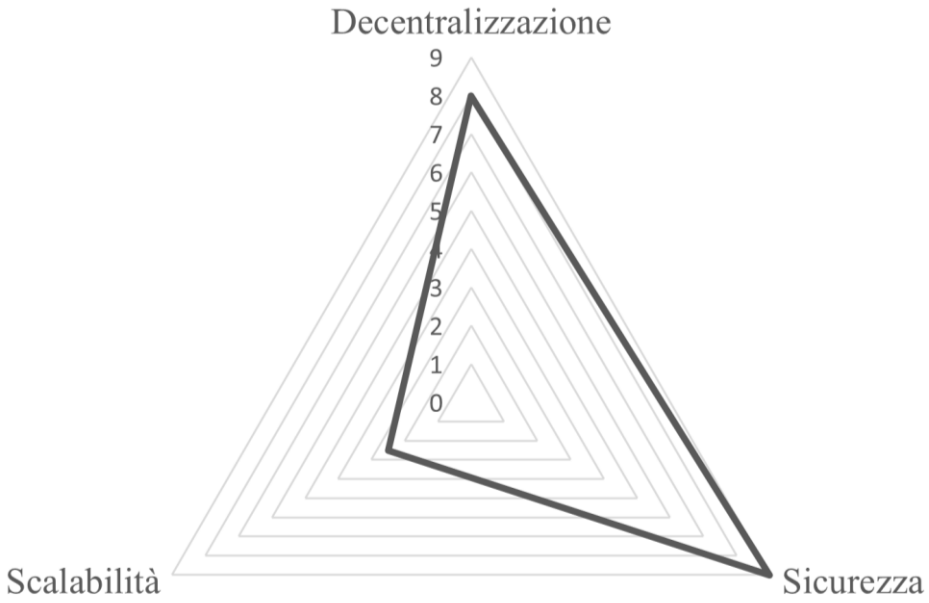

Figura 8: proprietà del Bitcoin

3.5 Lightning Network: innovazione?

La soluzione più efficiente per risolvere il principale problema di bitcoin è stata trovata off-chain, ossia con un protocollo che viene eseguito esternamente alla blockchain che prende il nome di Lightning Network. Esso permette transazioni quasi istantanee con costi molto bassi, andando ad eliminare le limitazioni del protocollo nativo dovute al basso throughput[9].

Questo protocollo dichiara una velocità vicina al milione di transazioni per secondo, valore che renderebbe bitcoin il sistema di pagamento più rapido e scalabile al mondo. L'elemento fondamentale del protocollo è il canale di pagamento off-chain, dove al suo interno due utenti della rete bitcoin hanno la possibilità di scambiare denaro.

Per la sua apertura, viene effettuata una transazione on-chain, che deve essere firmata da entrambi i nodi che vi partecipano. Successivamente, i due nodi vanno ad effettuare una transazione che corrisponde ad un deposito di un certo ammontare di bitcoin che sarà utilizzato per il trasferimento nel canale. A quel punto i due nodi possono scambiare bitcoin off-chain a costo zero, mantenendo i

[9] Frequenza con cui vengono trasmessi i dati, in questo caso riferito alla processazione delle transazioni.

bilanci aggiornati. Terminata la loro comunicazione, il canale viene chiuso, effettuando la seconda transazione on-chain del protocollo, che va a certificare il saldo finale di entrambi i partecipanti. Questa tecnologia permette di non dover validare ogni singola transazione, in quanto è richiesta solamente una conferma da parte del mittente e del destinatario dei fondi, garantendo allo stesso tempo la tracciabilità e la trasparenza tramite le due transazioni del protocollo sulla blockchain. Inoltre, i nodi non richiedono una grande capacità di elaborazione in quanto si può utilizzare semplicemente un Raspberry Pi, che in caso di comunicazione diretta tra due nodi consuma circa 5W e processa una transazione in meno di un secondo

3.5.1 Comunicazione a più nodi

Il protocollo Lighting Network, per ottimizzare il throughput, permette di effettuare transazioni sfruttando il collegamento dei i diversi nodi. Questo evita l'apertura di un canale dedicato per ogni singola coppia di utenti che vuole comunicare.
Se un nodo A vuole comunicare con nodo C ma non possiede nessun canale diretto, ma ne ha uno aperto con B che a sua volta è canalizzato a C può sfruttare questa ramificazione di collegamenti.
In particolare, in questo caso, C genera una "invoice" che è possibile inquadrare come una richiesta di pagamento che invia a B, che a sua volta genera la propria richiesta e la invia ad A. Quest'ultimo genera la transazione e la invia a B che infine inoltrerà al nodo destinatario C.

3.5.2 Risultati e conclusioni

Considerando i vantaggi ottenibili con l'utilizzo di Lightning Network si ottiene che una transazione effettuata con l'abbinamento di Bitcoin a questo protocollo off-chain permette di avere transazioni in media 345 mila volte più veloci dei classici sistemi di pagamento. Anche se paragonato a schemi di pagamento istantaneo dei sistemi tradizionali, risulta 14 volte più veloce.
Inoltre, Bitcoin Lightning scala molto più rapidamente rispetto ai pagamenti istantanei con una capacità teorica di circa 31 trilioni di transazioni all'anno comparate con 31 miliardi, diventando anche 96 milioni di volte più efficiente dal punto di vista energetico di un pagamento classico.

In conclusione, Lightning Network è un protocollo ancora in costante sviluppo ma i vantaggi derivanti dal suo utilizzo sono notevoli, dalla riduzione del traffico delle transazioni all'interno di bitcoin, all'esecuzione quasi istantanea dei trasferimenti tra due nodi. Non mancano però degli svantaggi, che ad oggi, hanno limitato la sua diffusione, come ad esempio, la necessità di essere connessi e attivi in un canale di pagamento anche quando si deve incassare l'approvvigionamento. Questo ha portato alla diffusione di wallet dedicati, creando un ulteriore passaggio che gli utilizzatori devono fare, quindi la ricerca di un provider affidabile, con delle commissioni adeguate al servizio che non coprano i vantaggi di questa soluzione.

Capitolo 4

Evoluzione della blockchain

4.1 Bitcoin, più di una criptomoneta

Bitcoin è nato per essere semplice e sicuro con l'obiettivo di rappresentare una possibile alternativa alle monete fiat, di natura digitale, anonima, distribuita e gestita da una rete peer-to-peer di utenti, senza una autorità centrale. Con il tempo sono state approfondite e indagate anche nuove possibilità, per avere qualcosa di più di una semplice criptomoneta.

Questo è stato reso possibile grazie al Bitcoin Script, il linguaggio di programmazione di Bitcoin che consente l'elaborazione delle transazioni sulla blockchain. È un linguaggio molto semplice e richiede un'elaborazione minima, ma ha delle funzionalità limitate come ad esempio l'impossibilità di creare dei loop, ossia dei cicli. Questo riduce la creazione di errori nel sistema, in quanto è possibile sapere con certezza quando e come finità uno script, eliminando completamente la possibilità di bloccare l'intera blockchain. Ma porta con sé anche delle limitazioni, infatti in questa direzione si sono spinti molto in avanti soprattutto altre blockchain.

In seguito all'invenzione del Bitcoin, dal 2011 in poi sono nati diversi progetti con lo scopo di definire nuovi protocolli e nuove criptovalute, che hanno preso il nome di "altcoin". Secondo alcune stime, al giorno d'oggi potrebbero essercene in circolazione circa sedicimila.

La maggior parte delle altcoin, come fa intendere la parola stessa, sono monete digitali alternative a Bitcoin, quindi, hanno lo scopo principale di fungere da riserva di valore e di gestire pagamenti peer-to-peer decentralizzati. Alcune derivano direttamente da Bitcoin, sono sue hard fork, come Bitcoin Cash, Bitcoin SV e Bitcoin Gold. Altre, hanno l'obiettivo di aumentare e migliorare le funzionalità offerte, con fini anche diversi dal semplice pagamento decentralizzato.

In modo molto generale le blockchain si possono dividere in diverse generazioni [13]:

- Prima generazione: progettate per migliorare i sistemi finanziari esistenti offrendo una piattaforma di pagamento decentralizzata. L'esempio più eclatante è Bitcoin.

- Seconda generazione: aggiungono uno strato di “condizioni” alle transazioni in modo che le persone possano concordare i termini in contratti intelligenti piuttosto che affidarsi a intermediari. L’esempio emblematico è Ethereum con gli smart contracts.
- Terza generazione: mirano a risolvere limitazione fondamentali nella blockchain, tra cui la scalabilità e l’interoperabilità. Si possono nominare come esempio Ripple, Cardano, Algorand ed Ethereum 2.0.

4.2 Smart contracts

4.2.1 Nascita e progresso del protocollo

Il termine è stato coniato da Nick Szabo nel lontano 1994 in cui, tramite un documento intitolato proprio “Smart Contracts” [14], ha enunciato la creazione di un protocollo di transazione computerizzato che esegue i termini di un contratto. Gli obiettivi generali della progettazione di contratti intelligenti sono soddisfare condizioni contrattuali comuni (come termini di pagamento, privilegi, riservatezza), ridurre al minimo le eccezioni sia dannose che accidentali e diminuire la necessità di intermediari fidati. Gli obiettivi economici correlati includono la riduzione delle perdite per frode, i costi di arbitrio e altri costi di transazione.

Szabo nei due anni successivi ha pubblicato nuove definizioni, ma il concetto di base rimaneva lo stesso, automatizzare il processo di attuazione degli obblighi contrattuali. Quindi il sistema manuale presente a quel tempo, grazie all’utilizzo di questi contratti intelligenti con la conseguente riduzione dell’intervento umano, è stato snellito e velocizzato. Gli smart contracts funzionano seguendo semplici istruzioni condizionali, che verificano le condizioni, e quando sono soddisfatte eseguono delle azioni predefinite.

Sono già utilizzati nel mondo reale, ad esempio nei pagamenti con le carte di credito contactless per acquistare biglietti del treno, della metropolitana oppure per il funzionamento dei servizi di sharing. Ad esempio, il noleggio di un’autovettura richiederebbe tradizionalmente la firma fisica di un documento, quindi un contratto, e un deposito a copertura di eventuali danni. Al giorno d’oggi non è più necessario per noleggi a breve termine, in quanto è sufficiente scaricare un’applicazione sullo smartphone, caricare i propri documenti di identificazione, utilizzarla per sbloccare l’autovettura,

quindi dare inizio al noleggio effettivo. Quando la macchina viene parcheggiata e chiusa, entrano in gioco le clausole del contratto in modo automatico, senza intervento umano, addebitando sul conto di pagamento associato all'account l'importo dovuto.

4.2.2 L'incontro con la blockchain

La nascita degli smart contracts non ha nulla a che vedere con la blockchain. Questi due concetti sono stati abbinati dal protocollo di Ethereum, nel 2015, una blockchain open source sulla quale possono essere sviluppate e gestite applicazioni decentralizzate.
Tramite la blockchain e le sue caratteristiche, l'utilizzo e la popolarità degli smart contracts sono aumentati esponenzialmente. La fiducia peer-to-peer e l'integrità dei risultati di un programma consentono agli smart contracts di poter verificare le clausole di un contratto in totale trasparenza [15]. Gli accordi sono secretati attraverso il processo di consenso quando le parti attuano il contratto, e i termini scritti in pezzi di codice assieme alle azioni da performare in caso di attivazione.
Uno smart contracts sulla blockchain consente, quindi, ai vari nodi di ispezionare il codice per assicurarsi che soddisfi le clausole pattuite, quindi avere una automatizzazione nell'esecuzione di obblighi contrattuali visibili a tutti i partecipanti della rete e non solo alle parti coinvolte.
Inoltre, aggiunge la sicurezza che un contratto firmato, una volta registrato sulla blockchain, diventi immodificabile e non annullabile. Il segnale che fa scattare l'esecuzione di uno smart contract solitamente arriva dall'esterno della blockchain, tramite gli oracoli. Essi sono servizi di terze parti che creano il collegamento con il mondo reale, ma non sono la fonte dei dati, sono semplicemente degli applicativi che recuperano, verificano e autenticano i dati prelevati da fonti esterne prima di inviarli alla blockchain. (*Figura 9*). Le proprietà fondamentali che deve avere un oracolo sono fornire dati non manipolabili, usare diverse fonti per ridurre i rischi di errore o di frode, lasciare trasparenza nella verifica delle informazioni fornite ed essere protetto da possibili attacchi.
L'utilizzo e la diffusione dei contratti intelligenti sono però minate dalla difficoltà che si può incontrare nella programmazione di questi codici, nel momento in cui le parti che stanno stipulando un accordo non hanno conoscenze tecniche.

Ciò comporta la necessità della presenza di intermediari che, in questa situazione, sono programmatori che si occupano di tradurre il contratto in un linguaggio comprensibile alla tecnologia blockchain, introducendo inevitabilmente dei costi.
Altre limitazioni si presentano durante la creazione di contratti molto complessi, in quanto il codice per la stesura di smart contracts è molto rigido e riduce lo spazio ad ambiguità che, ad esempio, sono presenti sia nella lingua italiana che in quella inglese.

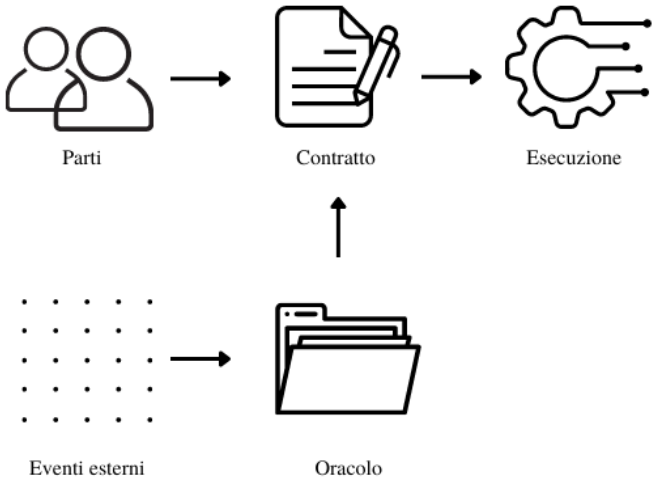

Figura 9: funzionamento smart contract

4.2.3 Caso d'uso reale, gli NFT

Le applicazioni basate su contratti intelligenti sono di diverso tipo, dai videogiochi, alla finanza decentralizzata, fino ad arrivare alla condivisione delle cartelle cliniche tra diversi istituti medici. La crescita e lo sviluppo dei contratti intelligenti hanno aperto molte porte a nuovi settori ed utilizzi, portando il loro impiego in un numero inquantificabile di settori. Negli ultimi anni sono esplosi nel mercato gli NFT (Non Fungible Token), token digitali che attestano la proprietà di un acquisto, che non possono essere contraffatti, sostituiti o divisi grazie alle loro proprietà univoche.

Con una capitalizzazione che ha sfiorato i 41 miliardi di dollari nel 2021, che si avvicina al valore totale dell'intero mercato globale delle belle arti [16], gli NFT sono diventati il caso d'uso di maggior successo degli smart contracts.

In particolare, essi entrano in gioco proprio nella la creazione di NFT, assegnando la proprietà all'acquirente e gestendo un possibile accordo di vendita.

Il contratto intelligente contiene diverse informazioni sull'NFT, come il creatore dell'opera e la cronologia della proprietà. In questo modo, il possessore del token può dimostrare i suoi diritti senza la necessità di rivolgersi ad intermediari. Inoltre, l'NFT può rappresentare anche la proprietà o la partecipazione in quote di oggetti del mondo reale.

Capitolo 5

Trilemma delle blockchain

5.1 Introduzione del problema

La tecnologia blockchain si trova ad affrontare un problema unico nel suo genere, il "trilemma blockchain". Riguarda i tre pilastri chiave di questa tecnologia: decentralizzazione, sicurezza e scalabilità. È stato inventato da Vitalik Buterin (co-fondatore di Ethereum) e afferma che tutte le blockchain sono costrette a trovare dei compromessi con queste proprietà; quindi, che per ottenere dei miglioramenti in una dimensione bisogna necessariamente sacrificare parte delle altre due.
Questo è stato riscontrato principalmente nelle due migliori blockchain per capitalizzazione, Bitcoin ed Ethereum in quanto hanno preceduto la nascita di questo trilemma e hanno probabilmente creato le basi per questi studi. Molte altre blockchain, consapevoli su che aspetti lavorare, hanno migliorato la tecnologia arrivando a dichiarare di aver risolto questo enigma.

5.2 Come ottimizzare la tecnologia

Gli sviluppatori stanno testando e sviluppando approcci differenti per risolvere questo trilemma, a partire dalla modifica diretta della blockchain, quindi utilizzando una soluzione di "livello 1", all'esecuzione di ottimizzazioni tecnologiche sopra a blockchain esistenti, quindi di "livello 2".

5.2.1 Alcune soluzioni di livello 1

- Miglioramento dei meccanismi di consenso: proof-of-work è il protocollo più utilizzato, la sua necessità di miners, algoritmi di crittografia ed enormi quantità di potenza di calcolo decentralizzato lo rendono sicuro ma molto lento. Per superare questo muro, sono state studiate soluzioni alternative, infatti, Ethereum per questa ragione ha recentemente eseguito l'aggiornamento ad Ethereum 2.0 siglando ufficialmente il suo passaggio da proof-of-work a

proof-of-stake. Altre blockchain, invece, data la conoscenza di questo trilemma sono state progettate direttamente con protocolli di consenso differenti.

- Sharding: questa soluzione consiste nel suddividere una rete in blockchain più piccole e veloci, in modo da poter gestire un maggior numero di transazioni. Questo modo di partizionare per distribuire il carico di lavoro e di archiviazione su una rete peer-to-peer aumenta il throughput transazionale, in quanto ogni nodo non è responsabile del carico dell'intera rete ma conserva solamente le informazioni relative alla sua partizione, o shard. Le informazioni contenute in uno shard sono ancora condivise con gli altri nodi, il che mantiene il sistema decentralizzato, trasparente e sicuro, l'unica differenza è che i nodi non elaborano e memorizzano tutte le transazioni della rete [17].

5.2.2 Alcune soluzioni di livello 2

- Nested Blockchains: in questo tipo di sistema esistono due blockchain. È presente una blockchain principale, o mainchain, che stabilisce solamente le regole per l'intera rete, perché le esecuzioni vengono effettuate su una rete interconnessa di catene secondarie. Esistono quindi diversi livelli di blockchain costruiti uno sopra l'altro e collegati tramite una connessione a catena genitore-figlio. La catena dei genitori delega le operazioni alla catena dei figli, che eseguono i task e ritornano il risultato alla catena principale. La catena di base non prende mai parte alle funzioni nella rete al meno che non debba risolvere una controversia.
- Canali di stato: creano una comunicazione bidirezionale tra una blockchain e dei canali transazionali off-chain. Questi canali sono eseguiti da smart contracts che permettono di fare transazioni istantanee, dirette e a costi quasi pari a zero. A transazioni ultimate il canale di stato viene chiuso salvando le informazioni di apertura e chiusura nella blockchain.
  Un esempio di questo protocollo è il Lightning Network utilizzato su Bitcoin.

Capitolo 6

Altcoin

6.1 Ethereum

Questa blockchain è l'altcoin per eccellenza, come dimostra la capitalizzazione del mercato che la classifica al secondo posto, subito dopo Bitcoin, con 138 miliardi di dollari. Diversamente da quest'ultimo, il suo obiettivo non è solamente quello di consentire i pagamenti peer-to.peer, ma anche fornire un "sistema operativo" per applicazioni decentralizzate, chiamate dApp.

Ethereum raggiunge questo obiettivo integrando un linguaggio di programmazione Turing-completo[10], che permette a tutti i nodi di scrivere applicazioni e smart contracts. Tutto questo è possibile tramite la "Ethereum virtual machine" (EVM), la macchina virtuale di Ethereum, che è un'entità singola gestita da migliaia di computer collegati che eseguono un client Ethereum.

Il protocollo ha lo scopo di mantenere la continua, ininterrotta e immutabile operazione di questa speciale macchina di stato in cui risiedono tutti i conti e i contratti intelligenti sviluppati in questo contesto [18].

Ethereum stesso si definisce senza "funzionalità", ma fornisce gli strumenti e un linguaggio per poterle creare matematicamente. In particolare, gli sviluppatori pagano Ether, la criptovaluta associata alla blockchain, per avere accesso alla potenza di calcolo decentralizzato della rete. A differenza di Bitcoin, Ethereum nei pagamenti opera in modo similare ai conti bancari, ossia non si basa sugli output di transazione non spesi (UTXO) come Bitcoin ma sui saldi correnti, chiamati stati, di tutti i conti al suo interno. Sono state sviluppate delle dApp per aumentare la privacy, tra cui "Tornado Cash" che offusca le transazioni attraverso la crittografia e permette di generare una prova che dimostra che si è a conoscenza di un segreto senza rivelarlo. In questo modo, rende invisibili i collegamenti tra mittente e destinatario di una transazione. I fondi vengono depositati su uno smart contract e viene generata una nota che permette di ritirare i fondi su un indirizzo diverso, senza

[10] Un linguaggio di programmazione è detto Touring-completo se consente di implementare una qualsiasi macchina di Turing.

lasciare alcun collegamento con la transazione originale [19]. Questa applicazione decentralizzata è stata recentemente coinvolta in una vicenda di cronaca, l'8 agosto 2022 è stato vietato il suo utilizzo nel suolo americano. Il Dipartimento del Tesoro sostiene che "Tornado Cash" ha avuto un ruolo centrale nel riciclaggio di quasi sette miliardi di dollari. Il codice è perfettamente legale, anzi, questa storia dimostra la sua funzionalità, soltanto che l'utilizzo che ne è stato fatto in questo caso è di natura malevola.

Questo protocollo è nato con la proof-of-work come meccanismo di consenso, incontrando limitazioni simili a Bitcoin. L'aumentare della sua diffusione ha posto la community davanti al problema della scalabilità, delle elevate commissioni di transazione, e delle performance del sistema. Ethereum riusciva a gestire solamente quindici transazioni per secondo e la commissione media richiesta dalla rete Ethereum aveva raggiunto a novembre 2021 un valore massimo di 62,11 dollari, per poi calare fino ad arrivare il 25 novembre 2022 a 1,94 dollari. Nell'ultimo anno si è registrato un picco giornaliero che ha raggiunto i 200,06 dollari, che ha alzato la media annuale a circa 11,10 dollari. La latenza media per inserire un blocco nella catena è attualmente, a novembre 2022, di circa 12,06 secondi [20]. Questo è il valore più basso di sempre nella sua storia, dopo aver toccato il massimo di 30,31 secondi a settembre 2017, è iniziato a calare, con velocità sempre maggiore anche grazie anche all'aggiornamento ad Ethereum a 2.0, trattato successivamente.

Inoltre, date le proprietà della proof-of-work, anche il consumo energetico era molto alto, ha toccato addirittura un picco di 93.982 TWh di energia all'anno, per attestarsi in media a circa 22TWh.

Il problema da risolvere era proprio quello del trilemma blockchain, migliorare le prestazioni del protocollo in sicurezza, decentralizzazione e scalabilità senza trascurare nessuna di esse.

Già dal 2015, infatti, Vitalik Buterin e gli altri ingegneri di Ethereum hanno iniziato a lavorare ad una transizione, una serie di aggiornamenti che potessero dare la svolta al futuro del protocollo [21]. Questo processo di miglioramento è suddiviso in cinque fasi: "The Merge", "The Surge", "The Verge", "The Purge" e "The Splurge". Ognuna di esse ha un obiettivo specifico di miglioramento, ma sono collegate dallo scopo comune di aumentare la scalabilità della rete, il numero di transazioni al secondo e diminuire i costi relativi al suo funzionamento.

Il primo passo, "The Merge", è stato concluso con successo il 15 settembre 2022, migrando il meccanismo di consenso da proof-of-work a proof-of-stake. Questo passaggio ha ridotto il consumo

energetico di Ethereum di circa il 99,98% portando il consumo annuale a circa 0.0026 TWh [22], rendendo la blockchain molto più sostenibile a lungo termine a livello ambientale (*Figura 10*).

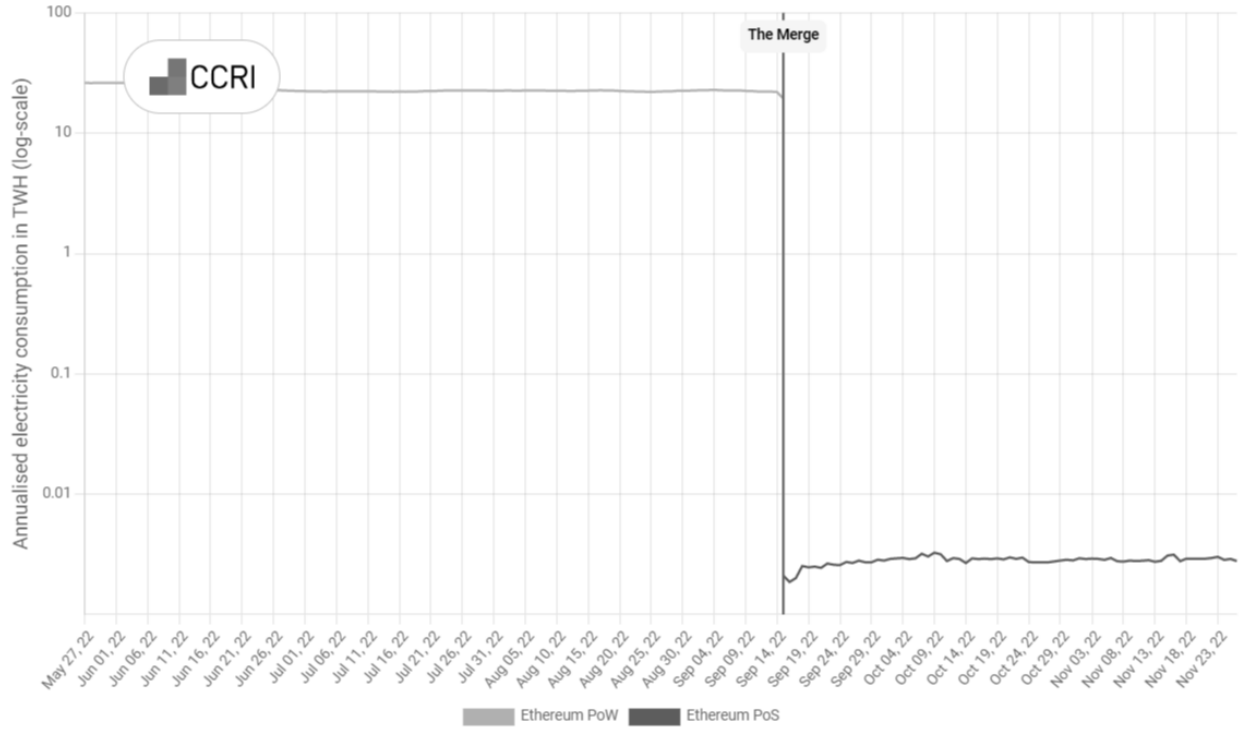

Figura 10: consumo elettrico annuale Ethereum

L'impatto di PoS non termina qui, molti più nodi possono diventare validators in quanto non è più richiesta una potenza di calcolo elevata ma è sufficiente mettere in staking 32 ETH.

Con la seconda fase "The Surge", verrà implementato lo sharding, un processo di divisione orizzontale della blockchain in 64 frammenti per distribuire il carico, ridurre la congestione della rete e aumentare quindi di conseguenza le sue prestazioni in termini di transazioni al secondo.

In questo modo, si alleggerisce ancora di più la dipendenza dai costosi requisiti hardware, alleggerendo il carico per ciascun validator, aumentando la partecipazione alla rete rendendola ancora più decentralizzata e sicura. Questo elemento viene ridotto nuovamente nella terza fase, "The Verge", con l'introduzione dei "Verkle Trees", che richiedono una prova crittografica più complessa da implementare ma con l'opportunità di grandi guadagni in termini di scalabilità. Il concetto è stato

proposto per la prima volta da Vitalik nel 2017 ed è ancora in fase di ricerca e sviluppo. “The Purge” è mirata all’eliminazione dei dati storici in eccesso, riducendo la congestione della rete e i requisiti di spazio ad ogni nodo. I client non devono archiviare in modo permanente tutti i blocchi storici, in particolare smetteranno di archiviare i dati che hanno più di un anno.
Infine, l’ultima fase è chiamata “The Splurge”, dopo che la transizione ad Ethereum 2.0 sarà stata quasi completata gli sviluppatori si concentreranno su aggiornamenti e miglioramenti minori per garantire il corretto funzionamento del sistema. Lo stesso co-fondatore Buterin, ha descritto questa fase come “il divertimento una volta che tutte le fasi precedenti si sono unite”.
Dopo questo processo di transizione si stima che Ethereum possa eseguire circa 100.000 transazioni al secondo, aprendo le porte ad una nuova era di opportunità in ambito blockchain.

6.1.1 Considerazioni sul trilemma in Ethereum

Allo stato attuale solo la fase “The Merge” è stata eseguita correttamente; quindi, l’unico cambiamento effettuato è quello del protocollo di consenso. Le transazioni al secondo di Ethereum, infatti, sono rimaste pressoché inalterate. I passi in avanti affrontati sono quindi la diminuzione del consumo di energia elettrica e la diminuzione dei requisiti hardware richiesti per avere la possibilità di creare nuovi blocchi. Quindi di conseguenza è leggermente aumentata la decentralizzazione in quanto i costi per la partecipazione sono diminuiti e i nodi hanno quindi una soglia di partecipazione più sostenibile. Per quanto riguarda la sicurezza, le sanzioni economiche poste dalla PoS per gli utenti malevoli, rendono gli attacchi molto più costosi rispetto al proof-of-work, perché i validators rischiano di perdere sia le ricompense per il lavoro svolto sia l’importo messo in staking. In aggiunta, precisazione non di poco conto, quest’ultimo valore caso dell’attacco 51% dovrebbe ammontare alla metà degli ETH in circolazione; quindi, il rischio per l’attaccante è considerevole. Un altro vantaggio di PoS è la sua capacità nel preparare un contro attacco quando l’utente malevolo cerca di rendere canonica la propria fork. I validators onesti potrebbero continuare a costruire sulla catena di minoranza e ignorare la biforcazione errata oppure potrebbero decidere di rimuovere forzatamente l’intruso dalla rete e di distruggere i suoi ETH in staking.
Tuttavia, l’attacco ad una rete PoW presenta delle limitazioni logistiche in quanto l’utente deve trovare un modo di acquisire e alimentare tutto l’hardware, che potrebbe significare aver la necessità

di accedere ad una quantità di energia paragonabile a quella usata da un intero stato. Tutto questo rende molto impegnativo l'attacco ad una rete basata su PoW.

In conclusione, la sicurezza si può considerare rimasta ad un ottimo livello anche se leggermente inferiore a Bitcoin, ma è una valutazione preliminare in quanto il progetto è stato studiato e valutato dopo una prima fase, dove il meglio potrebbe ancora dover arrivare.

Gli investitori sono molto curiosi nel vedere gli aggiornamenti in atto, la strada sembra lunga ma allo stesso tempo promettente, soprattutto iniziando già da un buon punto di partenza (Figura 11: proprietà Ethereum*Figura 11*).

Figura 11: proprietà Ethereum

6.2 Algorand

Algorand è una piattaforma blockchain fondata nel 2017 da Silvio Micali, professore al MIT di Boston, ritenuto il più importante informatico italiano nel mondo. È un progetto in grande sviluppo e di grande prospettiva, a marzo 2021 ha collaborato con la SIAE per la gestione dei diritti d'autore e nel primo semestre del 2022 ha stretto un accordo di sponsorizzazione e partnership tecnica con la FIFA, l'organizzazione sportiva più riconosciuta a livello globale.

Algorand punta ad essere un sistema in cui sviluppare applicazione decentralizzate, fornire servizi di finanza decentralizzata e in cui creare token non fungibili (NFT).

Questa tecnologia offre un sistema alternativo per la validazione e l'aggiunta dei blocchi nella rete, utilizza la pure-proof-of-stake (PPoS) come protocollo di consenso con l'ambizione di aver risolto il trilemma della blockchain. Essa può tollerare un numero arbitrario di utenti malintenzionati purché quelli onesti detengano più di due terzi dei token nel mercato. Ogni utente che possiede il token ALGO può aderire al protocollo di consenso, dichiarando la sua volontà con la generazione e registrazione di una chiave di partecipazione. Questo meccanismo aumenta la privacy degli utenti perché non espongono le loro chiavi che usano, per esempio, per firmare le transazioni. La chiave di partecipazione, dopo un certo numero di round viene rimossa e per continuare nella proposta e alla conferma dei blocchi bisogna generarne una nuova.

La PPoS è un'evoluzione della PoS, che si compone di due fasi:

- Fase di proposta: viene generato un seme casuale e inviato a tutti i nodi. Questo valore, assieme alla chiave di partecipazione segreta, viene usato come input per una funzione casuale verificabile (VRF[11]) che ogni nodo esegue per scoprire se è stato selezionato per partecipare. Essendo un algoritmo eseguito in locale, con la propria chiave segreta, solo i diretti interessati sono a conoscenza di aver vinto la selezione e possono creare un nuovo blocco e diffonderlo nella rete. L'utente include anche la prova crittografica del VRF nel blocco proposto per dimostrare l'appartenenza al comitato. Fino a quel punto, però, nessuno è a conoscenza dei nodi vincitori.

[11] "Verifiable Random Function": funzione che prende in ingresso dei dati e produce un output pseudocasuale, con in aggiunta una prova che chiunque può utilizzare per verificare il risultato.

- Fase di votazione: anche in questo caso si usa una VRF per formare un comitato di nodi che verifichino i blocchi. Quando gli utenti hanno scoperto di essere in questo gruppo analizzano i blocchi proposti che hanno ricevuto, compresa la prova crittografica del VRF, e votano se uno qualsiasi di questi blocchi debba essere inserito nella catena. Se il comitato raggiunge il consenso su un nuovo blocco, esso viene diffuso nella blockchain. Poiché solo un blocco può avere la soglia richiesta di voti da parte del comitato sorteggiato non è possibile che due blocchi vengano aggiunti alla catena contemporaneamente.

Tutti i token presenti nella rete hanno la stessa probabilità di essere scelti, ma, basandosi sulla PoS, chi ha maggior quantità di ALGO in staking ha una maggiore probabilità di essere selezionato e quindi di poter proporre o partecipare alla validazione di un blocco.

Il meccanismo PPoS aumenta la sicurezza della rete in quanto la scelta dei partecipanti al protocollo è totalmente causale e basata sulla crittografia. Una volta scelto il comitato di validazione, ad esempio, ormai è troppo tardi per un attacco o corruzione del nodo in quanto il blocco ha già iniziato a propargarsi in tutta la rete e non è più possibile tornare indietro con la transazione.

Inoltre, una volta eseguita la validazione di un blocco l'algoritmo ricomincia, quindi per ogni blocco c'è una nuova selezione di tutti i partecipanti al protocollo di consenso.

Con l'ultimo aggiornamento, il 3.9.2, Algorand esegue tutto questo processo in brevissimo tempo, passando da 4,4 secondi a 3,9 secondi; quindi, la sua latenza è decisamente bassa e permette al protocollo di essere altamente scalabile. Inoltre, ogni singolo blocco ora è in grado di contenere fino a 26.000 transazioni portando, a livello teorico, la rete a poter eseguire fino a 6.000 transazioni al secondo [23]. Anche se il sito ufficiale di Algorand al 26 novembre riportava un valore effettivo pari a 13 TPS.

Gli sviluppatori però, hanno già dichiarato il loro prossimo obiettivo prestazionale, che è quello di raggiungere i 10.000 TPS continuando a ridurre i tempi di round per migliorare ulteriormente l'esperienza finale dell'utente e aprire le porte a più opportunità di adozione nel futuro.

Le commissioni vengono calcolate in base alle dimensioni della transazione e un utente può scegliere di incrementare questo importo per aumentare la priorità e velocizzare l'inserimento in un blocco quando il traffico è elevato. L'importo minimo per una transazione è solamente di 0,001 ALGO, che al rapporto attuale con il dollaro si traduce in 0,0002457 dollari.

Anche il consumo energetico è stato ottimizzato rispetto alle altre blockchain concorrenti, infatti è uno dei protocolli che attualmente consuma meno con un utilizzo medio di 0,000652 TWh annui.
Per connettersi alla rete Algorand, i nodi hanno bisogno di un software di virtualizzazione chiamato "Algorand Virtual Machine" (AVM), che è responsabile della valutazione degli smart contratcs prima di eseguirli sulla rete. Se una chiamata ad uno smart contract fallisce, eventuali modifiche prodotte da tale esecuzione non verranno salavate nella blockchain, viceversa se ha esito positivo le modifiche verranno registrate nella catena.
Algorand ha un'architettura a due livelli, dove il primo si occupa dell'esecuzione di operazioni di "base" che sono meno onerose a livello computazionale mentre nel secondo livello vengono eseguite quelle più pesanti, off-chain, salvando il risultato nella catena e certificando quindi la transazione. In questo caso entrambi sono integrati nativamente in Algorand, e questo permette loro di essere ottimizzati.

6.2.1 Considerazioni sul trilemma in Algorand

Algorand con questo meccanismo della PPoS raggruppa tutte le proprietà per risolvere il trilemma della blockchain. Un protocollo studiato da Micali e dal gruppo di sviluppo di Algorand, che ha preso come base di partenza il protocollo di consenso proof-of-stake migliorando i punti carenti. Dalla creazione dei blocchi da parte di un nodo casuale che cambia ad ogni round, al comitato di validazione degli stessi che è a sua volta scelto tramite una funziona casuale che riduce la possibilità di attacchi sui nodi decisionali che ha migliorato la sicurezza. Dei possibili problemi di questa proprietà sono la decisione di eliminare le penalizzazioni per nodi che si comportano in modo scorretto, che riduce la pericolosità di avere un comportamento malevolo, e il fatto della distribuzione delle ricompense senza incentivi per la creazione di blocchi validi. Allo stesso tempo però, sono riusciti a mantenere la privacy degli utenti, facendo generare chiavi apposite per la partecipazione al protocollo di consenso, senza mettere in pericolo le chiavi necessarie per l'esecuzione delle transazioni. Inoltre, PPoS non richiede di mettere i propri token di ALGO in staking ma è sufficiente possedere anche solamene un ALGO, rendendo il tutto più conveniente. Questo permette di ampliare gli orizzonti di partecipazione al protocollo di consenso a molti più nodi, aumentando la sua decentralizzazione e anche scalabilità. Questo basso prerequisito, unito alla poca energia e spazio di archiviazione richiesto per l'esecuzione

di un nodo, ha portato al raggiungimento attuale di 1500 nodi alla partecipazione del consenso di Algorand.

Inoltre, un altro fattore che può spingere i clienti verso la scelta di questo protocollo è il contributo che fornisce sul tema del cambiamento climatico. Oltre al risparmio energetico, Micali ha affermato di aver a cuore il pianeta e quindi ha fatto, e sta facendo, il possibile per rendere la sua blockchain più verde possibile, introducendo anche il tema della sostenibilità. Giusto per paragone, rispetto alla blockchain di Bitcoin, la creazione di smart contracts, e transazioni su Algorand comportano emissioni di CO2 120 milioni di volte inferiori. Infatti, punta ad essere la prima rete blockchain a raggiungere la neutralità del carbonio, stringendo anche collaborazione con ClimateTrade[12] per compensare il basso livello di carbonio prodotto dalla rete. Questo protocollo assegna automaticamente una parte di ogni commissione di transazione per compensare le emissioni di carbonio. Inoltre, ha integrato la blockchain Algorand per fornire trasparenza e tracciabilità nei mercati del carbonio. Algorand ha tutti gli elementi necessari per diventare un punto di riferimento nell'ecosistema blockchain, raggiunge throughput di transazione paragonabili alle entità di pagamento centralizzate ma con finalità immediata, costi di transazione vicino allo zero 24 ore su 24, 7 giorni su 7. (*Figura 12)*

Figura 12: proprietà Algorand

[12] Leader nella trasparenza e tracciabilità delle emissioni di CO2 che utilizza la tecnologia blockchain per migliorare l'efficienza degli sforzi di sostenibilità delle aziende.

6.3 Solana

Solana è una blockchain decentralizzata di livello 1, costruita per sviluppare smart contracts ed applicazioni scalabili. È stata creata nel 2017 da Anatoly Yakovenko, un ex dirigente di Qualcomm e il suo primo punto di forza è proprio la sua capacità a scalare; infatti, punta ad essere più rapida, più economica e più sostenibile sul lungo periodo rispetto alle altre blockchain. Inoltre, un altro elemento focale di Solana è l'efficienza, abbinata alla semplicità d'uso per avvicinare sempre più persone ad utilizzare questa tecnologia [24].

Il sistema si basa sulla proof-of-stake per convalidare le informazioni e una speciale innovazione chiamata a proof-of-history (PoH) che consente una maggiore velocità di validazione. Questa scelta la rende estremamente efficiente, utilizzando un'energia per transazione nella stessa scala di alcune ricerche su Google, e minore rispetto ad altri normali usi domestici come il funzionamento del frigorifero [24]. Nonostante il basso consumo energetico per transazione di Solana, la rete PoS utilizza ancora molta energia in generale rispetto ad altre declinazioni della stessa.

Secondo il CCRI[13], la blockchain Solana consuma in media 0,166 Wh di elettricità per transazione, diventando il protocollo PoS più efficiente dal punto di vista energetico in termini di elettricità utilizzata. Questo risultato però dipende ma molti fattori, tra cui il numero di transazioni che avvengono nella rete, e il consumo complessivo di elettricità per transazione dipende anche dai nodi connessi alla rispettiva rete. Teoricamente, se aumenta il numero di transazioni, aumenta il consumo di elettricità ma diminuisce il consumo per singola transazione [25].

Nonostante il basso consumo energetico per transazione di Solana, il consumo medio annuo è di circa 0,003641 TWh. In *Figura 13*, sono rappresentati i consumi elettrici in MWh delle blockchain Algorand, Ethereum 2.0 e Solana e, quest'ultima, è la rete con il valore più elevato.

[13] "Crypto Carbon Ratings Institute", società orientata alla ricerca che fornisce dati sugli aspetti di sostenibilità di criptovalute, blockchain e altre tecnologie.

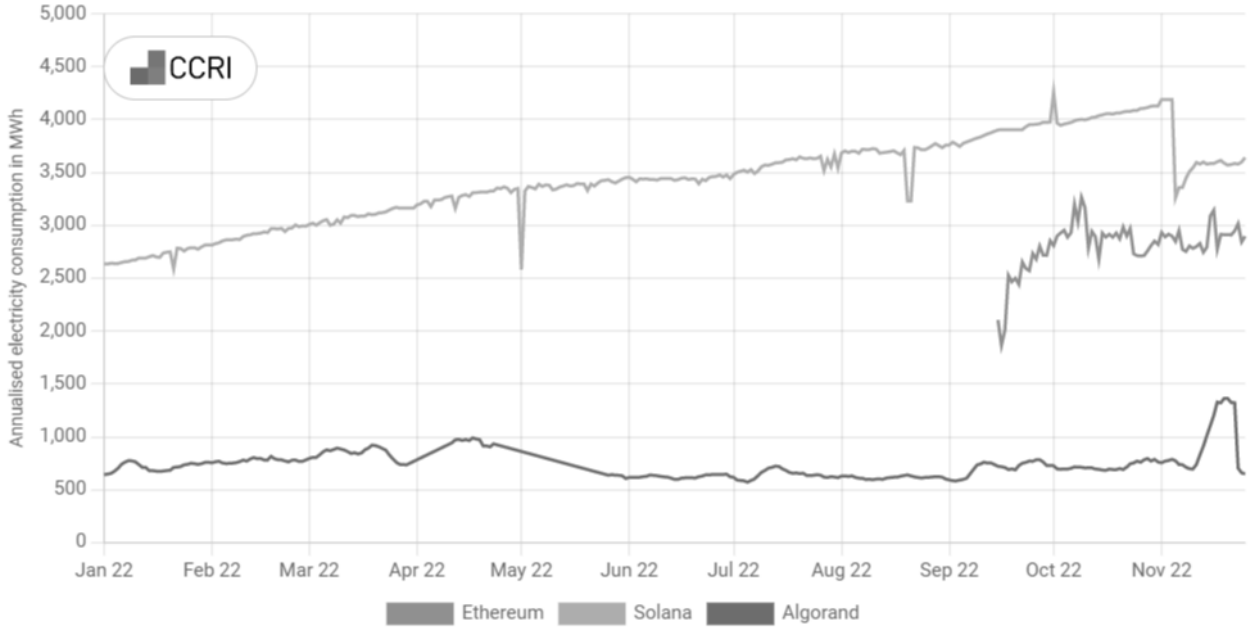

Figura 13: Consumo elettrico annuo di Solana, Ethereum e Algorand nel 2022

Inoltre, come Algorand, anche Solana punta al tema della sostenibilità e nel 2021 ha dichiarato che è riuscita a raggiungere la neutralità del carbone. La Fondazione Solana finanzia un processo chiamato "Refrigerant Destruction" che è stato eletto da Green America[14] come uno dei modi più efficaci per ridurre le emissioni di carbonio.

Tornando al funzionamento di Solana, il componente particolare è la PoH, una sequenza di calcoli che colloca gli eventi in ordine temporale, garantendo una sincronizzazione rapida dei diversi blocchi nella rete.

Il sistema PoH può essere rappresentato come un orologio crittografico che fornisce un timestamp ad ogni transazione. Esso si si basa su una funzione ricorsiva di ritardo verificabile (VDF), che esegue l'hash degli eventi in arrivo e rileva quando si sono verificati gli eventi. Quando gli altri nodi eseguono la sequenza di hash, possono venire a conoscenza dell'ordine in cui si sono verificati gli eventi senza dover convalidare l'ora con altri nodi.

[14] Organizzazione senza scopo di lucro con sede negli Stati Uniti che promuove un consumismo etico e attento all'ambiente.

PoH permette alla rete di essere molto veloce e Solana afferma di poter raggiungere i 50/65.000 TPS. Ma realmente le statistiche sono molto più basse e si attestano su 3000/5000 TPS, anche se genera un blocco in soli 0,4 secondi. A suo favore, inoltre, si schierano le commissioni, che sono solamente 0.00025 dollari per transazione.
Dal punto di vista della privacy, in Solana è possibile tracciare ogni transazione dall'inizio della blockchain. Si può facilmente controllare la cronologia delle transazioni di ogni portafoglio, avendo di conseguenza un livello di privacy relativamente basso. Come in Ethereum, con Tornado Cash, anche in Solana sono nate delle soluzioni per risolvere questo problema. In particolare, per rendere private le transazioni si può utilizzare Solbank. Esso mira ad essere un browser wallet Solana privato, che riunisce i fondi di ogni utente in un portafoglio comune, ed esegue le transazioni di ogni utente. Quando esso restituisce i fondi al portafoglio e crea un nuovo portafoglio senza la cronologia delle transazioni. In questo modo protegge maggiormente la privacy degli utenti in quanto tutte le transazioni vengono effettuate dallo stesso portafoglio.

6.3.1 Considerazioni sul trilemma in Solana

Solana, è un protocollo relativamente molto giovane rispetto alla concorrenza, infatti è stata lanciata ufficialmente a marzo 2020. La sua valuta SOL è stata listata nel mercato a meno di 2 dollari e i lati positivi del suo protocollo ha fatto sognare gli investitori che hanno portato il suo valore nel giro di un anno ad un massimo storico di 260 dollari.
Ha diverse potenzialità, la prima da notare è sicuramente la rapidità degli scambi teorici che si possono ottenere nella rete, che si traduce in efficienza dei servizi offerti. Questo grazie anche alle commissioni molto basse, che incentivano l'uso della rete. La piattaforma blockchain Solana ha permesso tutto questo tramite l'utilizzo un meccanismo di consenso ibrido che compromette il decentramento per massimizzare la velocità. L'innovativa combinazione di PoS e PoH rende Solana un progetto unico nel settore blockchain, ma non è riuscita a risolvere il famoso trilemma blockchain. I validators nella rete Solana sono attualmente 1839, valore che si discosta molto da quello di Ethereum che supera i 400.000. Questo evidenzia la differenza di decentralizzazione della rete, che ha compromesso fino a questo punto la sua esplosione. Una delle limitazioni è l'hardware richiesto, per offrire il throughput molto elevato. In un'intervista ad aprile 2022 Yakovenko ha addirittura

dichiarato che questi requisiti per eseguire un nodo validator potrebbero aumentare con il passare del tempo, minando la decentralizzazione.

Nonostante tutto però è considerata da molti investitori la possibile avversaria di Ethereum nel lungo termine vista la sua struttura e le sue proprietà (*Figura 14*) che saranno migliorate con il passare degli anni, prospettando una buona strada di crescita di fronte a sé.

Un problema emerso però, che è di fondamentale importanza nella scelta di un protocollo, è la sua affidabilità. In confronto ad altre blockchain, Solana ha presentato dei disservizi nella sua breve storia. Il 14 settembre 2021, per ben oltre 17 ore, l'intero sistema si è spento. Questo è stato causato da un sovraccarico della rete che ha causato opinioni contrastanti data la sua natura prettamente puntata alla scalabilità. Ma non è stato l'unica vicenda, infatti è successo anche altre volte nel 2022.

Questo fatto ha esternato due punti di vista, uno positivo ed uno negativo: la sicurezza della rete è stata sufficiente da non esporre risorse del sistema durante gli attacchi e/o interruzioni, e dall'altro lato sono state messe in discussione le proprietà della rete, abbinate alla sua affidabilità.

Figura 14: proprietà Solana

Capitolo 7

Conclusione

La blockchain è in costante evoluzione, presenta ormai diverse tipologie di rete e soluzioni che hanno aperto le porte a vasti scenari di applicazione. I protocolli possono differire per aspetti quali lo scopo del progetto oppure l'implementazione tecnica della tecnologia stessa.

In questo testo, sono state approfondite in primo luogo le tematiche relative alle proprietà della blockchain, necessarie per il suo funzionamento ottimale, che si possono riassumere in decentralizzazione, scalabilità e sicurezza. Tra queste, quella che è risultata più difficile da perfezionare è stata la scalabilità, principalmente per la natura e l'obiettivo con cui la blockchain è cresciuta nei vari anni. Questo si addice principalmente al primo utilizzo pratico della catena di blocchi, ossia Bitcoin. Esso, con lo scopo di sostituire i classici sistemi centralizzati di pagamento, punta alla decentralizzazione, eliminando gli intermediari e utilizzando transazioni peer-to-peer intrinsecamente sicure. A questo punto, entra in gioco anche la sicurezza, che in un sistema finanziario ha una rilevanza sostanzialmente irrinunciabile. Nessun utente sarebbe disposto a rischiare i suoi fondi per poter effettuare transazioni, ad esempio, in modo più semplice e rapido.

Questo è il dibattito che affligge l'ecosistema sotto esame, con Vitalik Buterin che nel 2016 ha riassunto il concetto nel "trilemma della blockchain", infatti, secondo il co-fondatore di Ethereum non sarebbe possibile ottenere tutte e tre le proprietà senza essere obbligati a sacrificare una di esse. Ma nonostante il trilemma sia composto da tre punti, il problema principale riscontrato è tra la scalabilità e la sicurezza-decentralizzazione, che molto spesso sono in contrasto.

È importante sottolineare che non tutti i protocolli hanno lo stesso scopo di progetto; infatti, nel frattempo, sono nate blockchain mirate a supportare applicazioni decentralizzate e piattaforme per lo sviluppo di smart contracts. Ma il trilemma rimane, la ricerca della sua risoluzione è rimasta un tema caldo in quanto può portare benefici alla blockchain, indipendentemente dall'ambito di applicazione e utilizzo. Questa è diventata infatti, in questo studio, una nuova metrica utilizzata per la classificazione dei protocolli nel mercato, portando il loro approfondimento ad un livello successivo.

I risultati hanno dimostrato che la prima grande divisione può essere effettuata a livello generazionale. Infatti, la prima e la seconda generazione che possiamo identificare direttamente come Bitcoin ed Ethereum, sono state eccezionali dal punto di vista dell'innovazione ma presentano diverse problematiche e limitazioni. Gli sviluppatori stanno testando e sviluppando approcci differenti per risolvere il trilemma, a partire dalla modifica diretta della blockchain, all'esecuzione di ottimizzazioni tecnologiche sopra le reti esistenti. Le blockchain di terza generazione, invece, sono state progettate già tenendo in considerazione delle varie problematiche da risolvere, cercando di migliorare tutti gli aspetti limitanti già in fase di progettazione. (Figura 15)

A partire proprio da Bitcoin, esso utilizza il protocollo di consenso proof-of-work, che permette di avere un'ottima sicurezza e decentralizzazione del sistema a discapito della scalabilità. Questo lo ottiene con dei grandi consumi elettrici, causando enorme scalpore nella comunità globale, che ha sfruttato il dato per fare chiasso mediatico. I consumi sono stati paragonati erroneamente a quelli di interi stati, come ad esempio la Norvegia, perché se paragonato ai sistemi tradizionali di pagamento che mira a sostituire, ottiene un risultato ben ventotto volte più basso. La domanda sorge spontanea: perché nessuno acclama che il sistema tradizionale consuma elettricità pari a quattro volte i consumi di tutta la Germania?

Bitcoin presenta delle circoscrizioni a livello prestazionale, in quanto riesce ad eseguire dalle cinque alle sette transazioni per secondo con un tempo di conferma medio pari a 7,14 minuti. Questo causa un conseguente aumento delle commissioni nel caso di alta domanda di processazione, anche se oltre ad un picco di 62 dollari per transazione, nel 2022 esse si sono attestate in media a 1,63 dollari. Una soluzione è aggiungere ed eseguire un protocollo che funziona al di sopra di Bitcoin, quindi definibile a livello 2. Lightning Network, tramite dei canali di stato, permette di effettuare transazioni off-chain, istantanee, dirette e a costi quasi paragonabili allo zero. Riuscirebbe ad aumentare la velocità a circa un milione di transazioni al secondo, con conferme di circa 500ms.

Ma esso è un protocollo ancora in pieno sviluppo, necessita ancora di vari test e di un'attenta valutazione degli svantaggi che potrebbe introdurre.

Ethereum è nato con le stesse limitazioni del protocollo Bitcoin, ma ha recentemente siglato un punto di svolta. Infatti, il 15 settembre 2022, ha concluso il primo di cinque aggiornamenti che hanno lo scopo comune di migliorare il protocollo, principalmente sotto il punto di vista della scalabilità. In questa prima fase, Ethereum è passato da proof-of-work a proof-of-stake riducendo il consumo

elettrico del 99,98% e i requisiti hardware per creare nuovi blocchi. Per quanto riguarda la sicurezza, essa è rimasta ad un buon livello, infatti, se viene preso in considerazione uno degli attacchi più conosciuti, l'attacco del 51%, per prendere il controllo della rete nel caso di PoW bisognerebbe riuscire ad alimentare e far funzionare un hardware capace di superare la metà della potenza di mining in circolazione. Mentre con la proof-of-stake, bisognerebbe acquistare almeno il 51% degli ETH sul mercato. Le prestazioni sono rimaste pressoché inalterate a quindici transazioni al secondo, con un tempo di conferma nella media dei 12,06 secondi e commissioni pari a circa 1,94 dollari. Ma per vedere i risultati del cambiamento in atto bisogna attendere il completamento di tutte le fasi previste.
Analizzando Algorand e Solana è emersa la vera differenza generazionale. Esse, seppur molto giovani, si muovono bene verso la risoluzione del trilemma. Nonostante la loro capitalizzazione di mercato sia molto minore, a lungo termine potrebbero benissimo competere con Bitcoin ed Ethereum. Attualmente, quest'ultime, si stanno concentrando a sviluppare soluzioni per coprire le lacune del protocollo; quindi, necessitano di tempo per trovare e implementare definitivamente i cambiamenti epocali. Le blockchain di terzo livello, invece, stanno lavorando su questo aspetto dalla loro nascita, recuperando parzialmente il divario generazionale in termini di tempo.
Algorand con il suo protocollo di consenso proprietario, pure-proof-of-stake, dichiara esplicitamente di aver risolto il trilemma blockchain. Esso permette di ottimizzare maggiormente i consumi elettrici arrivando ad un valore medio annuale di 0,003641 TWh, e promuove temi di sostenibilità ambientale come dimostra la collaborazione con ClimaTrade. Teoricamente riesce a gestire fino a 6000 transazioni al secondo, ma al momento dello studio il sito ufficiale di Algorand riportava un valore effettivo di 13 TPS. I tempi di conferma sono molto bassi in quanto aggiunge un nuovo blocco in appena 3,9 secondi e le commissioni sono limitate a 0,001 ALGO, che si traduce attualmente in 0,0002457 dollari.
Solana, per il protocollo di consenso si basa su PoS introducendo però un'ottimizzazione denominata proof-of-history, che aumenta la velocità di validazione delle transazioni con un consumo medio di elettricità superiorie a Ethereum ed Algorand con una media annuale di 0,00364116 TWh.
PoH permette a Solana di gestire fino a 65000 TPS anche se, come in precedenza, al momento dello studio il sito ufficiale riporta un valore attuale di circa 4000 transazioni al secondo. Essa però è competitiva sulla latenza, infatti genera un blocco ogni 0,4 secondi e le commissioni si attestano a circa 0,00025 dollari.

In conclusione, ogni protocollo analizzato ha ancora grandi margini di miglioramento. Ma in questo momento storico, dopo lo studio proposto, la scelta di un protocollo blockchain ricadrebbe nella terza generazione. Solana, rispetto ad Algorand, si trova leggermente indietro sia in termini di sviluppo che di problematiche interne da risolvere. Deve migliorare la decentralizzazione del sistema e la sua affidabilità, in quanto nel corso degli ultimi anni ha riportato più volte interruzioni del servizio che hanno fermato l'inserimento dei blocchi. Questo è un elemento chiave in fase di valutazione, che eleva a maggior visibilità chi fa di questa caratteristica un suo punto di forza. Algorand, nonostante sia più lontana dai riflettori rispetto ad altre blockchain, potrebbe rivelarsi la scelta vincente a lungo termine, aggiungendo a suo favore anche una spiccata attenzione al tema della sostenibilità ambientale che al giorno d'oggi è sempre più impattante.

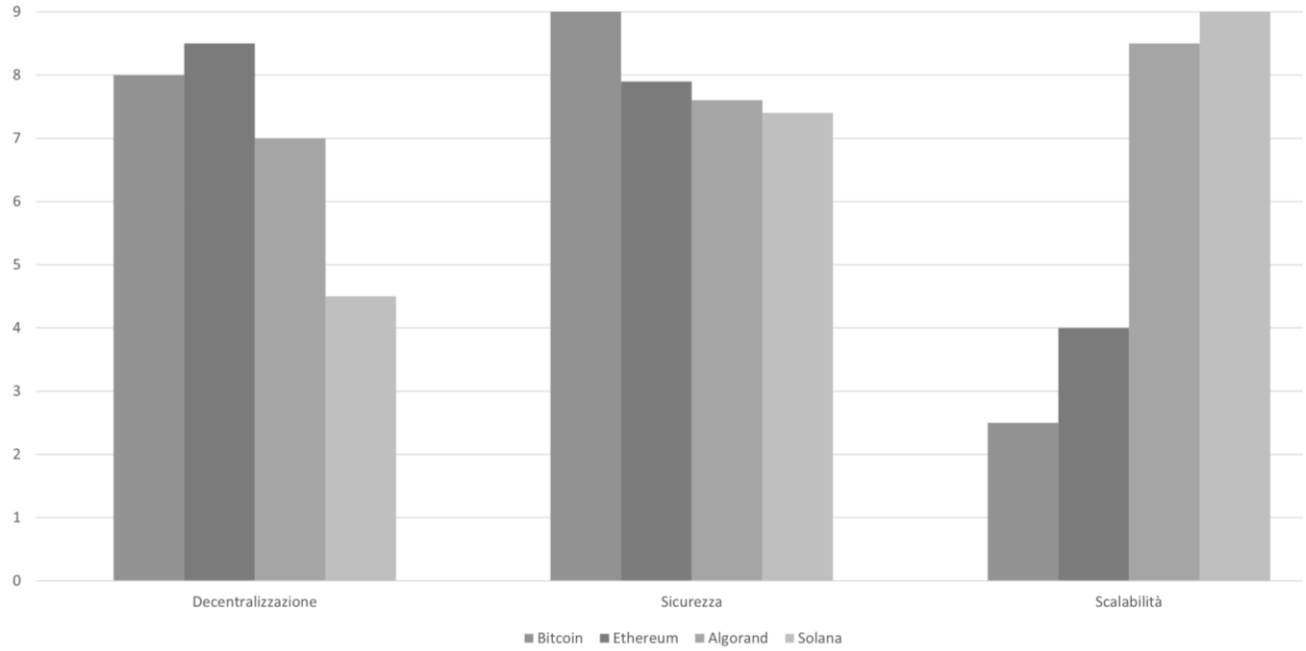

Figura 15: confronto dei protocolli analizzarti

Bibliografia

[1] Darryn Pollock. (2018). The Fourth Industrial Revolution Built On Blockchain And Advanced With AI. https://www.forbes.com/sites/darrynpollock/2018/11/30/the-fourth-industrial-revolution-built-on-blockchain-and-advanced-with-ai/?sh=46f033744242

[2] Team Blockdata. (2018). Top 100 Public Companies Investing in Blockchain & Crypto Companies. https://www.blockdata.tech/blog/general/top-100-public-companies-investing-in-blockchain-and-crypto-companies

[3] Binance Accademy. (2018). Storia della blockchain. https://academy.binance.com/it/articles/history-of-blockchain

[4] Amazon. Cos'è la tecnologia Blockchain. https://aws.amazon.com/it/what-is/blockchain/

[5] Bitpanda. How do Hard and Soft Forks work? https://www.bitpanda.com/academy/en/lessons/how-do-hard-and-soft-forks-work/

[6] Satoshi Nakamoto. (2008). Bitcoin A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[7] University of Cambridge. (2022). Cambridge Bitcoin Electricity Index https://ccaf.io/cbeci/index

[8] Niall McCarthy. (2021). Bitcoin Devours More Electricity Than Many Countries.

https://www.statista.com/chart/18632/estimated-annual-electricity-consumption-of-bitcoin/

[9] Michel Khazzaka (2022). Bitcoin: Cryptopayments Energy Efficiency. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4125499

[10] Tom Honzik. (2022). What is a bitcoin UTXO and why do they matter? https://unchained.com/blog/what-is-a-utxo-bitcoin/

[11] Joseph Bonneau. (2022). Why blockchain performance is hard to measure. https://a16zcrypto.com/why-blockchain-performance-is-hard-to-measure/

[12] Jeffrey Craig. (2021). What Is Transaction Per Second (TPS): A Comparative Look At Networks. https://phemex.com/blogs/what-is-transactions-per-second-tps

[13] Kirsty Moreland. (2022). Le generazioni Blockchain. https://www.ledger.com/academy/blockchain/web-3-the-three-blockchain-generations

[14] Nick Szabo. (1994). Smart Contracts. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[15] Maria G. Vigliotti. (2021). What do we mean by smart contracts? Open challenges in smart contract. https://www.frontiersin.org/articles/10.3389/fbloc.2020.553671/full

[16] Robyn Conti, Giovanni Schmidt. (2022). What Is An NFT? Non-Fungible Tokens Explained. https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token/

[17] Luca Mearian. (2019). Sharding: what it is and why many blockchain protocols rely on it.
https://www.computerworld.com/article/3336187/sharding-what-it-is-and-why-so-many-blockchain-protocols-rely-on-it.html

[18] Vitalik Buterin. (2014). A Next-Generation Smart Contract and Decentralized Application Platform.
https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

[19] Gianni Morselli. (2020). Tornado Cash e la privacy nelle transazioni di Ethereum.
https://cryptonomist.ch/2020/01/11/tornado-cash-privacy-ethereum/

[20] Etherscan. (2022). Ethereum Average Block Time Chart.
https://etherscan.io/chart/blocktime

[21] Clarissa Watson. Francesco Andreoli. (2022). The Merge Is Done. Whats's Next for the Ethereum Ecosystem?
https://consensys.net/blog/news/the-merge-is-done-whats-next-for-the-ethereum-ecosystem/

[22] Crypto Carbon Ratings Institute. Crypto Sustainability Indices
https://indices.carbon-ratings.com

[23] Noah Grossman. (2022). Algorand Boosts Performance 5x in Latest Upgrade.
https://developer.algorand.org/articles/algorand-boosts-performance-5x-in-latest-upgrade

[24] Solana. Blockchain Basis.
https://solana.com/it/learn/blockchain-basics

[25] Elena Partz. (2022). Report crowns Solana for using least energy per transaction, buut there's a catch.
https://cointelegraph.com/news/report-crowns-solana-for-using-least-energy-per-transaction-but-there-s-a-catch