Università degli Studi di Padova

Dipartimento di Scienze Statistiche

Corso di Laurea Triennale in Statistica per l'economia e l'impresa

Relazione finale

Bitcoin come tecnologia trustless e permissionless per lo scambio di valore: un'analisi statistica delle metriche relative all'adozione, la difficoltà di mining e il loro impatto sul prezzo

Relatore:
Professore Erlis Ruli

Laureando:
Lorenzo Dal Fabbro
Matricola 1101912

Anno Accademico 2022-2023

Indice

Grazie alla mia determinazione.

“Don’t trust,
verify.”

Introduzione

Bitcoin nasce con l'intento di escludere qualsiasi intermediario finanziario da uno scambio di valore, permettendo la comunicazione diretta tra le due parti interessate.
Erano gli anni dell'esplosione di internet, ed iniziava ad emergere la necessità di avere una moneta digitale utilizzabile per i servizi che stavano nascendo in maniera sempre più numerosa. C'erano stati diversi tentativi di creare la moneta di internet, che però non soddisfavano le caratteristiche di sicurezza necessarie.
Bitcoin è l'ultima evoluzione di questo percorso: con le firme digitali viene esclusa la necessità di una terza parte che funga da garante e viene proposta una soluzione al problema della doppia spesa grazie al sistema di consenso chiamato Proof of Work.
Parlando di Bitcoin ritorna spesso il concetto di Blockchain, erroneamente associato ad esso come tecnologia rivoluzionaria portata dalla valuta digitale. In realtà il concetto di Blockchain preesisteva già molto tempo prima della pubblicazione del whitepaper di Satoshi. Si parla molto di Blockchain in maniera speculativa, per descrivere progetti che apparentemente riportano le caratteristiche di Bitcoin, ma che in realtà condividono solo l'utilizzo di essa. Bitcoin è l'unione della Blockchain al consenso Proof of Work, che è il tassello fondamentale affinchè l'utente sia spinto a non aver la necessità di doversi fidare di qualcun altro, anzi al contrario spinge a voler verificare il lavoro degli altri utenti, ed è questo il punto di forza per un sistema trustless, sicuro, e libero da ogni censura.
Ad oggi Bitcoin è inarrestabile, non esiste alcuna entità in grado di bloccare il continuo flusso di transazioni che ogni giorno vengono convalidate dalla fitta rete di nodi validatori, in costante crescita, che rappresentano il motore del network. Il continuo incremento del network inoltre rende il sistema sempre più distribuito, andando quindi ad allontanare l'eventualità di centralizza-

zione che comporterebbe una minaccia per la sicurezza del protocollo stesso. Nei prossimi capitoli si andrà ad analizzare nello specifico il funzionamento di Bitcoin e successivamente accennare ad un altro progetto, Ethereum, per capirne le differenze, cercando di mettere in evidenza le caratteristiche che rendono Bitcoin unico in tutto il panorama delle criptovalute. Verrà approfondito il concetto di stablecoin, elencando le tipologie più comuni, e infine si darà spazio ad un'analisi riguardo il mining di Bitcoin, basato sul sistema di consenso Proof of Work, che rappresenta il cuore pulsante del protocollo, e garantisce la sicurezza e la distribuzione, concetti fondamentali allo scopo di Bitcoin. L'analisi è volta a valutare la sostenibilità del sistema e se, e come, questo ha un impatto sul prezzo della criptovaluta.

Bitcoin
2.1 Cenni storici

Il 31 ottobre 2008 veniva pubblicato sulla mailing list di un sito di criptografia (metzdowd.com) il whitepaper di Bitcoin, da parte dell'utente Satoshi Nakamoto. In questo documento viene descritto un sistema peer-to-peer di trasferimento di denaro che non necessita di un'istituzione finanziaria che operi da garante tra le due entità tra cui avviene lo scambio. L'innovazione che Bitcoin porta è un sistema che possa evitare che si verifichi il fenomeno del double spending, in cui un token possa essere speso due o più volte.
Nel sistema finanziario tradizionale, la soluzione al double spending è garantito da un ente che fa da garante, è quindi necessario in questo caso porre la fiducia in esso. Bitcoin si definisce un sistema trustless, in quanto non c'è la necessità di riporre fiducia in qualcuno.
Risulta chiaro il fatto che non sia stato scelto a caso il timing della pubblicazione del whitepaper, anzi si pensa proprio si sia voluto aspettare il momento opportuno e che quindi il tutto fosse già pronto da tempo. Pochi giorni prima della pubblicazione, il 15 settembre, falliva Lehman Brothers[1], come apice di una crisi spinta da politiche monetarie molto espansive attuate dalla FED, da una deregolamentazione del settore finanziario (amministrazione Bush) e dalla bolla del mercato immobiliare USA. La scelta di timing per la pubblicazione del whitepaper suona come una denuncia contro un sistema finanziario insostenibile.
La letteratura crittografica presenta vari accenni negli anni precedenti riguardo la tecnologia della blockchain. Addirittura nel 1991 se ne parla per la prima volta, quando i ricercatori Stuart Haber e W. Scott Stornetta teorizzano una soluzione computazionale pratica per marcare i documenti digitali in modo che non potessero essere retrodatati o manomessi. Si mettono

[1]Lehman Brothers Holdings Inc. è stata una società statunitense attiva nei servizi finanziari a livello globale risultata insolvente a settembre del 2008. Le ripercussioni hanno coinvolto tutto il mondo, dando inizio alla crisi finanziaria del 2008.

quindi le basi per lo sviluppo della blockchain, ma la tecnologia non verrà utilizzata per via soprattutto dell'assenza di un'applicazione che l'avrebbe potuta sfruttare. Degno di nota è il lavoro di Nick Szabo, statunitense di origini ungheresi laureato in informatica, che nel 1998 presenta una valuta digitale chiamata BitGold, che non vedrà mai la nascita. Szabo riprende il concetto di Proof of Work inizialmente ideato da Adam Back nel 1997 con HashCash[2]. Szabo crea però le basi per il futuro di Bitcoin, descrivendo una valuta decentralizzata e sicura, accessibile a tutti, ma rimaneva il problema del double spending. Nonostante ciò il lavoro di Szabo sarà fondamentale per lo sviluppo dei concetti chiave per Bitcoin; "Trusted third parties are "security holes" è una sua famosa citazione, che fa capire quanto si dedicherà al problema sicurezza, analizzando in profondità i difetti del concetto di denaro come lo intendiamo oggi, cercando una valida alternativa ad esso. Nel 2004 l'informatico Hal Finney si interessa alla questione, riprendendo il lavoro di Adam Back, introducendo il concetto di RPoW (Reusable Proof of Work). Con la RPoW si risolveva il problema della doppia spesa, grazie a un registro distribuito che consentiva agli utenti di tutto il mondo di verificarne l'integrità in tempo reale.

Il 3 gennaio 2009 viene minato da Nakamoto il blocco genesi, introducendolo così nel software. All'interno dell'unica transazione presente nel blocco viene scritto un messaggio, sia per dare una prova temporale che per enfatizzare le ragioni alla base dello sviluppo di Bitcoin: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" altro non è che il titolo che riportava quel giorno il quotidiano The Times. Era quindi un chiaro riferimento alla situazione finanziaria del momento.

[2]HashCash è un protocollo di posta elettronica sviluppato per contrastare lo spam e gli attacchi Dos, tramite una prova di lavoro che doveva compiere l'utente per inviare un messaggio. La prova di lavoro consisteva nell'eseguire un problema computazionale dal processore, che richiedeva qualche secondo per essere risolto. In questo modo per creare una grande quantità di messaggi era necessaria una grande quantità di tempo.

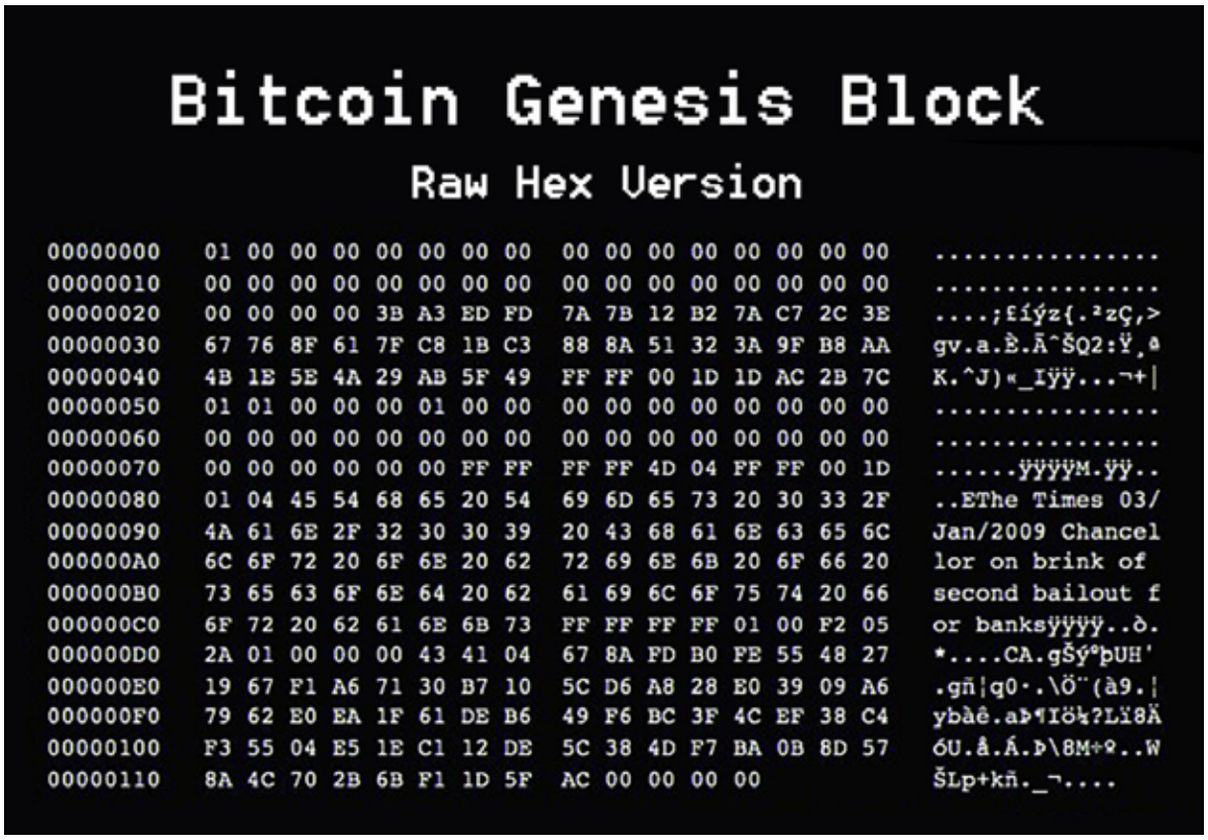


Figura 2.1: Blocco genesi di Bitcoin

Il 9 gennaio è la data di rilascio del primo client Bitcoin e viene minato il primo blocco effettivo, dando così realmente inizio al network come lo conosciamo oggi.

Il 12 gennaio Hal Finney riceve la prima transazione di Bitcoin, inviata dallo stesso Nakamoto.
Bisognerà aspettare ottobre 2009 per poter scambiare bitcoin con valute a corso legale, grazie alla piattaforma "New Liberty Standard", dove si poteva scambiare 1,309.03 BTC per 1$. Il prezzo era calcolato dall'amministratore del sito tramite un semplice modello che paragonava il valore al prezzo dell'energia elettrica consumata per l'attività di mining di quella quantità di BTC. Prima di esso i BTC minati nei blocchi iniziali venivano addirittura regalati tramite siti o forum per incentivare l'utilizzo del network.

La prima transazione di Bitcoin per l'acquisto di un bene viene ricondotta

a Laszlo Hanyecz, che nel maggio del 2010 scrive sul forum Bitcointalk che avrebbe pagato 10,000 BTC (all'epoca valutati 40$) a chiunque gli avrebbe mandato due pizze a casa. La richiesta fu accolta qualche giorno dopo da un utente che comprò le pizze e le fece recapitare a casa di Laszlo. Questa transazione certifica bitcoin come mezzo di scambio, e mette in moto la visione nakamotiana della sua creatura: una valuta accettata internazionalmente, in cui prevale la sua componente deflazionistica vista l'offerta prefissata e limitata di 21 milioni di bitcoin, etichettandola come moneta deflazionistica. Per questo motivo ad oggi Bitcoin è visto più come riserva di valore che come valuta utilizzabile per acquistare beni o servizi.

Da qui nasce il dibattito per cui una valuta deflazionistica non incentiverebbe la gente a spenderla, a differenza delle valute tradizionali, di natura inflazionistica, andando contro il sistema capitalistico su cui si basa l'economia mondiale.

L'ultimo messaggio pubblico di Satoshi risale all'11 dicembre 2010, in cui si esprimeva riguardo WikiLeaks[3]. In quel periodo infatti Julian Assange ipotizzava di utilizzare Bitcoin per raccogliere finanziamenti, in modo da aggirare i blocchi imposti dai governi sui sistemi di pagamento tradizionali. Satoshi vedeva in questo un pericolo per Bitcoin, che ai tempi era ancora un progetto agli albori, e non voleva che venisse associato a contesti negativi. A riguardo scrive: "It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us." Dopo questo messaggio non si avranno più notizie di Satoshi.
Assange messo alle strette dai governi ignorerà il consiglio e nel giugno del 2011 introdurrà la possibilità di ricevere finanziamenti tramite Bitcoin.

[3] Wikileaks è un'organizzazione internazionale no profit fondata nel 2006 che raccoglie informazioni e documenti coperti da segreto, di natura per lo più governativa, su argomenti militari, industriali o bancari.

Un altro evento che porterà attenzione su Bitcoin riguarda il capitolo di Silk Road[4].
Bitcoin era lo strumento ideale per i pagamenti, per via della privacy che garantiva. Tramite il registro distribuito si può risalire a tutte le transazioni e gli address coinvolti, ma non è possibile collegare un individuo fisico ad un address, a meno che questo non dichiari chiaramente il possesso. Questo fatto porterà l'opinione pubblica a collegare Bitcoin a situazioni di natura criminale. Si stima che nel corso degli anni, fino all'arresto di Ulbricht nell'ottobre del 2013, la piattaforma abbia guadagnato fino a 600,000 BTC.
Altri eventi che hanno fatto parlare di Bitcoin sono stati l'hackeraggio di Mt.Gox, exchange che al tempo gestiva il 70% del traffico di Bitcoin, in cui vennero sottratti dalla piattaforma circa 850,000 BTC tra il 2011 e il 2014 ai danni di circa 130,000 creditori, dei quali 200,000 circa recuperati in seguito. Nell'estate del 2016 toccò a Bitfinex, allora il maggior exchange al mondo per depositi in dollari, in cui vennero sottratti 119,756 BTC, per un controvalore all'epoca di 75 milioni di dollari, di cui una parte, circa 94,000 recuperata di recente dal Dipartimento di Giustizia di New York (ad oggi circa 4 miliardi di dollari).

Nel susseguirsi degli anni, nonostante le varie vicende, il prezzo di Bitcoin ha continuato ad aumentare, in parallelo alla sua adozione. È stato nel settembre 2021 per la prima volta nella storia dichiarato valuta a corso legale assieme al dollaro dalla Repubblica di El Salvador, piccolo paese dell'America Centrale.
Secondo una ricerca del FinTech Times, il 57% della popolazione del Continente Nero – più di 600 milioni di persone – non ha un conto corrente. Ma tre africani su quattro utilizzano un telefonino con accesso a Internet. L'adozione delle criptovalute potrebbe essere un modo per rendere alla portata di molti uno strumento di pagamento semplice e senza barriere di adozione.

[4] Silk Road è un noto sito e-commerce presente nel dark web, nato come sito di compravendita di libri banditi, e in seguito anche di droga, armi e servizi di qualunque tipo (hackeraggio, spionaggio, ingaggio di killer, ecc).

2.2 Cos'è la blockchain?

La blockchain è un registro che cataloga informazioni a blocchi, dove ogni blocco è concatenato al blocco precedente, formando per l'appunto, una catena di blocchi, letteralmente blockchain.
Più specificatamente è:

- Un registro con la possibilità di sola aggiunta di informazioni (in blocchi) marcate temporalmente (append-only log and timestamping);

- Un database verificabile, reso sicuro tramite la crittografia. Vi sono varie funzioni crittografiche che assicurano tale scopo: le funzioni di hashing rendono resistenti i dati alla manomissione e assicurano l'integrità degli stessi; le firme digitali, basate sull'algoritmo ECDSA[5] (Elliptic Curve Digital Signature Algorithm), sono utilizzate per il consenso tra i nodi della rete; il metodo di consenso, per trovare un accordo tra i nodi del protocollo.

- Il protocollo di consenso risolve il famoso costo di fiducia del problema dei generali bizantini[6], vari metodi di risoluzione possono essere implementati, e determinano la formazione di blockchain cosiddette permissioned (i nodi che accedono alla rete devono essere autorizzati) e permissionless (non serve autorizzazione per accedere al registro distribuito).
Entrando maggiormente nei tecnicismi, si illustreranno come queste proprietà vengono ottemperate e come operano nello specifico.
Nel proseguo parlando di blockchain si farà riferimento alla blockchain di

[5] Standard Elliptic Curve Digital Signature Algorithm è un algoritmo di generazione di firma basato sulla crittografia a curva ellittica, proposto per la prima volta nel 1992 da Scott Vanstone, divenuto standard ISO nel 1998, successivamente standard ANSI nel 1999, e infine standard IEEE nel 2000.

[6] Il problema dei generali Bizantini è un problema informatico teorizzato dai matematici Leslie Lamport, Marshall Pease e Robert Shostak nel 1982, e consiste nel permettere ai generali Bizantini, notoriamente non affidabili, di prendere una decisione unanime nonostante la presenza di generali disonesti. Facendo un parallelismo con Bitcoin, i nodi devono raggiungere un consenso sullo stato attuale del sistema.

Bitcoin, che in quanto precursore è considerato nel panorama crypto come la proxy del settore[7].

2.3 Caratteristiche della blockchain di Bitcoin

- **Registro distribuito, sempre online**: il registro può essere condiviso, aggiornato ad ogni transazione e replicato in modo selettivo tra i partecipanti quasi in tempo reale. I partecipanti possono sapere da dove proviene il valore e come la sua proprietà è cambiata nel tempo. Il registro è sempre online essendo condiviso tra una moltitudine di nodi, non esiste il rischio di single point of failure[8].

- **Privacy e immutabilità**: vengono utilizzati permessi e crittografia per impedire l'accesso non autorizzato alla rete e autenticare gli utenti. A seconda delle tecnologie crittografiche, si potrebbe fornire ulteriore privacy per l'utente che effettua le transazioni o le sue transazioni. Dopo che le condizioni sono state concordate, i partecipanti non possono manomettere la registrazione della transazione sul registro a causa del meccanismo di concatenazione dell'hash. Infatti, nessun partecipante può modificare una transazione dopo che è stata archiviata nel registro. Quindi, se una transazione viene eseguita in modo errato, è necessario utilizzare una nuova transazione per annullare l'errore ed entrambe le transazioni saranno visibili.

- **Trasparenza e verificabilità**: i partecipanti al network hanno accesso alle medesime registrazioni sul registro. Le transazioni sono contrassegnate da data ed ora e possono essere verificate quasi in tempo reale. L'esistenza

[7] Dal 2015, anno della ICO di Ethereum, Bitcoin non è più l'unica entità a capitalizzare nel mercato crypto. Da allora la sua capitalizzazione di mercato ha oscillato in un range tra il 70% e il 40% della totalità della capitalizzazione di mercato dell'intero settore. Le variazioni sul suo prezzo influiscono in maniera importante su quello delle altre crypto presenti nel mercato.

[8] In informatica con single point of failure si intende una parte del sistema hardware e software il cui malfunzionamento può portare ad anomalie di funzionamento o addirittura alla cessazione del servizio.

di un registro condiviso offre la possibilità di determinare la proprietà di un bene o tutte le informazioni su una transazione. Infatti, controllando lo storico del registro è possibile verificare se un bene appartiene ad un determinato utente perché tutti i passaggi di proprietà di quel bene dovrebbero essere visibili e autenticati. Nel caso della blockchain di Bitcoin, i dati racchiusi in questo registro distribuito sono le transazioni verificatesi della moneta nativa bitcoin all'interno del network Bitcoin.

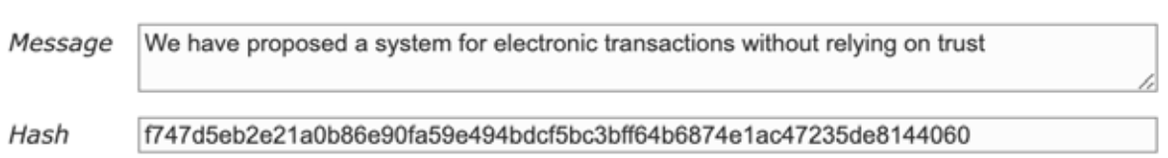
- **Basato sul consenso**: per convalidare una transazione tutti i partecipanti al processo di consenso devono concordare sulla sua validità. Ogni rete blockchain (quindi ogni progetto cripto) può stabilire le condizioni dalle quali può avvenire la validazione di una transazione. Bitcoin utilizza la Proof of Work, Ethereum è passato il 15 settembre 2022 da Proof of Work Proof of Stake, con l'aggiornamento denominato "The Merge". In seguito verranno approfonditi questi aspetti.
Le caratteristiche sopra esplicitate vengono raggiunte grazie alla crittografia, i vari protocolli differiscono in termini di sicurezza del network e proprietà dello stesso mediante l'utilizzo di differenti meccanismi crittografici.

2.4 Funzioni di Hash

La funzione di hash è una funzione matematica che attraverso un algoritmo genera, da un input di dimensione variabile, un output di lunghezza fissa univocamente espresso. Essa implica la compressione dei dati, attraverso un processo di scissione dei bit in ingresso e riassemblaggio con una variabile casuale per creare una stringa univoca in uscita di lunghezza fissa. Attraverso questo procedimento, file di diverse dimensioni e formato (video, immagini, o qualsiasi file digitale) possono essere riscritti (attraverso la funzione hash) come una stringa di dimensione fissa. La dimensione della stringa dipende dalla funzione di hash utilizzata.
Ci sono diversi tipi di funzioni hash, quella usata da Bitcoin è il Secure Hash Algorithm 256 (SHA-256), che rilascia come output una stringa di 256 bit di

64 caratteri alfanumerici.

Di seguito vediamo degli esempi di messaggi sottoposti ad hashing secondo standard SHA-256:



L'hashing porta ad una condensazione di informazioni in una stringa fissa, presentando l'accuratezza e l'integrità dei dati da tre principali proprietà di sicurezza: **collision-free property, hiding property e puzzle-friendly**.

- La proprietà di **collision-free** significa che nessuno può trovare due input diversi che producono lo stesso hash in uscita. Questo non implica che la collisione non esista, ma la probabilità di trovarne una è trascurabile. Non è stata provata l'esistenza di una funzione hash con la caratteristica di collisione-free, ma poiché la probabilità di trovarne una è minima, SHA-256 e SHA-512 vengono considerate come se fossero senza collisioni. Questa

caratteristica permette di usare le funzioni hash come digest dei messaggi, perché assumendo la collision-free di SHA-256 e SHA-512, ciò implica che trovare un output hash uguale da due input, implica l'uguaglianza degli input. Un'applicazione di questa proprietà potrebbe essere il riconoscimento di file, per fare un clustering di dati basterebbe applicare la funzione di hash al campione sotto osservazione, gli hash uguali dell'output corrispondono allo stesso dato anche in entrata.

- La seconda proprietà è detta **hiding property** (proprietà di occultamento) e presuppone che sia impossibile trovare l'input generatore a partire dall'output dell'hash, il che significa che la funzione di hash è una funzione unidirezionale, nel senso che non c'è un'operazione inversa.

- L'ultima caratteristica è detta **puzzle-friendly property** ed assume che per ogni possibile output y della funzione di hash H, se una variabile k è scelta da una distribuzione con alta sub-entropia, non esiste un algoritmo per trovare una x tale che $H(k|x) = y$, con la variabile di input k concatenata alla variabile x. Questa caratteristica può essere applicata ad un puzzle di ricerca: costruire un problema matematico che richiede la ricerca in una distribuzione di probabilità molto estesa per trovare una soluzione senza scorciatoie, ovvero non esiste nessuna strategia risolutiva che renda meglio che provare un valore casuale di x per risolvere il problema, consistendo in pura forza bruta in potenza computazionale. Questa caratteristica è la chiave essenziale per il processo di mining (analizzato in seguito), per produrre una prova di lavoro (Proof of Work).
Lo scopo della funzione hash è quello di condensare le informazioni, mentre il ruolo della crittografia è quello di proteggere i dati. Entrambi i protocolli sono i fondamenti del sistema Bitcoin.

2.5 Firme digitali

Bitcoin utilizza un sistema di crittografia asimmetrica[9] denominato crittografia a chiave pubblica (PKC). Le firme digitali sono uno strumento efficace già noto nel sistema finanziario tradizionale, utilizzato per praticamente tutti i sistemi di pagamento elettronico.

Ogni utente nella rete Bitcoin ha una chiave privata e una chiave pubblica correlata, generata a partire dalla chiave privata. La chiave privata ha una dimensione di 256 bit, mentre la chiave pubblica di 512 bit. La chiave pubblica hashata due volte determina l'indirizzo bitcoin che l'utente fornisce per ricevere bitcoin (come un IBAN, o un nome utente). Dall'indirizzo non è quindi possibile risalire direttamente alla chiave pubblica, inoltre è un metodo per rendere gli indirizzi più compatti. Correlata alla chiave pubblica, c'è la chiave privata (password), necessaria per convalidare le transazioni. Se qualcuno conosce una chiave privata collegata ad una chiave pubblica può agire come proprietario di quel portafoglio, per questo motivo bisogna evitare di condividere la chiave privata con altri.

La chiave pubblica è generata a partire dalla chiave privata tramite un'operazione crittografica basata, nel caso di Bitcoin, sullo standard ECDSA a 512 bit.

Per creare una firma digitale ci si avvale della chiave privata, che verrà utilizzata per firmare un messaggio noto. Si potrà successivamente verificare l'autenticità della firma utilizzando la chiave pubblica associata alla chiave privata utilizzata dal firmatario. In questo modo non è necessario condividere la chiave privata.

Vediamo nel particolare quali sono i passaggi per creare una firma digitale di un determinato messaggio, e per verificarla.

1) Si esegue l'hash del messaggio tramite SHA-256, in modo da avere una

[9] La crittografia a chiave asimmetrica è un sistema che prevede di potersi scambiare messaggi tramite un canale insicuro. Prima dell'avvento della crittografia asimmetrica si utilizzava la crittografia simmetrica, dove il mittente invia al destinatario un messaggio cifrato su un canale insicuro e una chiave di decifrazione su un canale sicuro. La validità di questo sistema è basata sulla segretezza della chiave di decifrazione.

stringa con un numero di caratteri prefissata.

2) Si utilizza la chiave privata per criptare l'hash del messaggio. L'output generato rappresenta la firma. Chiaramente la firma digitale dipende direttamente dal contenuto del messaggio, e quindi varia al variare del messaggio, a differenza di una firma tradizionale scritta a mano, che è sempre uguale.

3) A questo punto il mittente manda sia il messaggio che la firma al destinatario, che potrà verificarne l'autenticità.

4) Il destinatario esegue l'hash del messaggio sempre tramite SHA-256, trasmesso in chiaro dal mittente, e decripta la firma utilizzando la chiave pubblica. Se il risultato di questa operazione equivale all'hash del messaggio, la firma risulta valida.

Bitcoin (BTC) è "una moneta elettronica costituita da una catena di firme digitali", dove per trasferire monete dal proprietario al ricevitore, il primo deve firmare digitalmente un hash ricavato a partire dalle informazioni della transazione precedente e la chiave pubblica del prossimo proprietario, con la sua chiave privata, e aggiungere questa informazione alla moneta spesa (figura 2.2).

In questo modo la moneta rivela la sua storia di proprietà. Questo, unito al metodo di consenso Proof of Work, evita la doppia spesa poiché tutte le transazioni nella rete sono annunciate pubblicamente e verificate con un processo chiamato mining. I requisiti della firma sono la possibilità di verificare una firma valida e l'impossibilità di falsificare la firma, cioè nessuno può firmare un messaggio con una SK diversa.

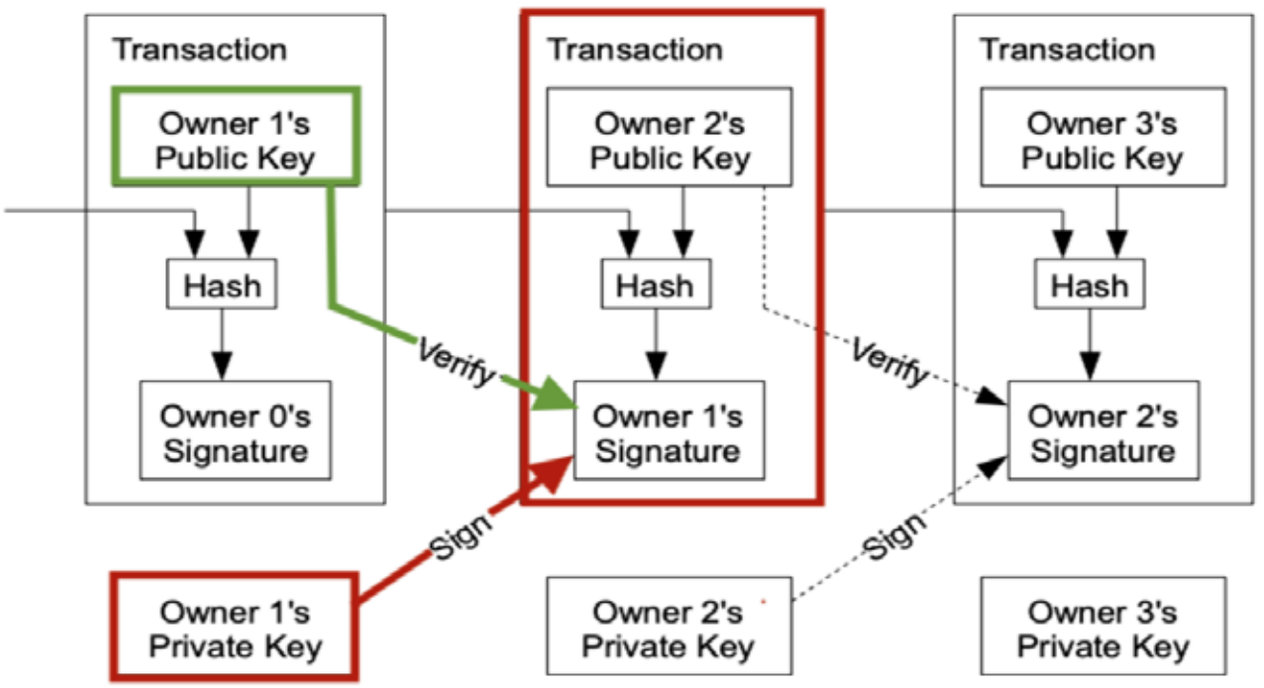


Figura 2.2: Schema rappresentativo del funzionamento delle firme digitali

Le tre principali caratteristiche delle firme digitali sono le seguenti:

1) **Integrità dei dati**: il destinatario può verificare che il messaggio non è stato modificato durante il tragitto, perchè qualsiasi modifica produrrebbe una firma totalmente diversa.

2) **Autenticità**: finchè le chiavi private del mittente rimangono segrete, il destinatario può utilizzare la chiave pubblica ricevuta per verificare che le firme digitali siano state create dal mittente e da nessun altro.

3) **Non disconoscibilità**: una volta che la firma è stata generata, il firmatario non potrà negare di averlo fatto.

Lo standard ECDSA è considerato impossibile da violare a causa della trascurabile probabilità di farlo, la sua buona casualità è essenziale nei processi di generazione delle chiavi pubbliche/private e nella firma.

2.6 Struttura dei blocchi

Ogni blocco della blockchain contiene due sezioni: un header (intestazione del blocco) ed un body (corpo).

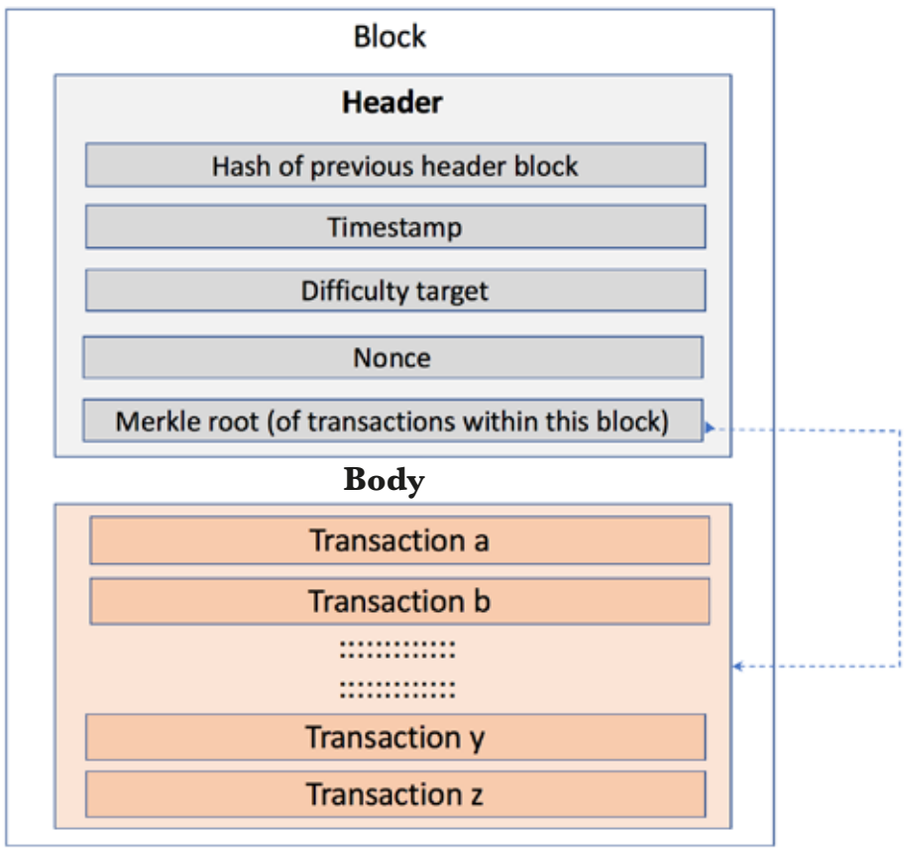


Figura 2.3: Struttura di un blocco

Il **block header** nel caso della blockchain di bitcoin contiene una serie di informazioni quali:

- **Versione del blocco**: numero che rappresenta l'insieme delle regole di convalida del blocco da seguire. È la versione di aggiornamento del software Bitcoin[10] caricata dalla comunità Bitcoin. Per esempio, in Bitcoin la versione 0.1.0 è stata introdotta nel blocco genesi e la versione 0.2.0 introduce la necessità di una specifica sul parametro altezza del blocco.

[10] Attualmente Bitcoin è aggiornato alla versione 23.0.0, quest'ultimo aggiornamento è stato rilasciato il 25 aprile 2022 dal team di sviluppo.

- **Merkle tree root hash**: valore di hash della radice dell'albero di Merkle. L'albero di Merkle è una struttura di dati specifica che memorizza tutte le transazioni contenute nel blocco. È una struttura piramidale inversa in cui tutti gli ID delle transazioni si trovano sullo stesso livello, chiamato Merkle tree leafs. Gli ID delle transazioni sono hashati in coppia insieme, se il numero di transazioni è dispari l'ultimo ID della transazione viene hashato per sé stesso. I risultati di questa fase di hashing formano un altro livello, dove viene ripetuto questo processo di hashing in coppia dei valori. Il processo viene ripetuto in loop fino a quando non viene raggiunto l'ultimo valore di hash, che rappresenta la radice di Merkle, che riassume tutte le transazioni registrate nel blocco.

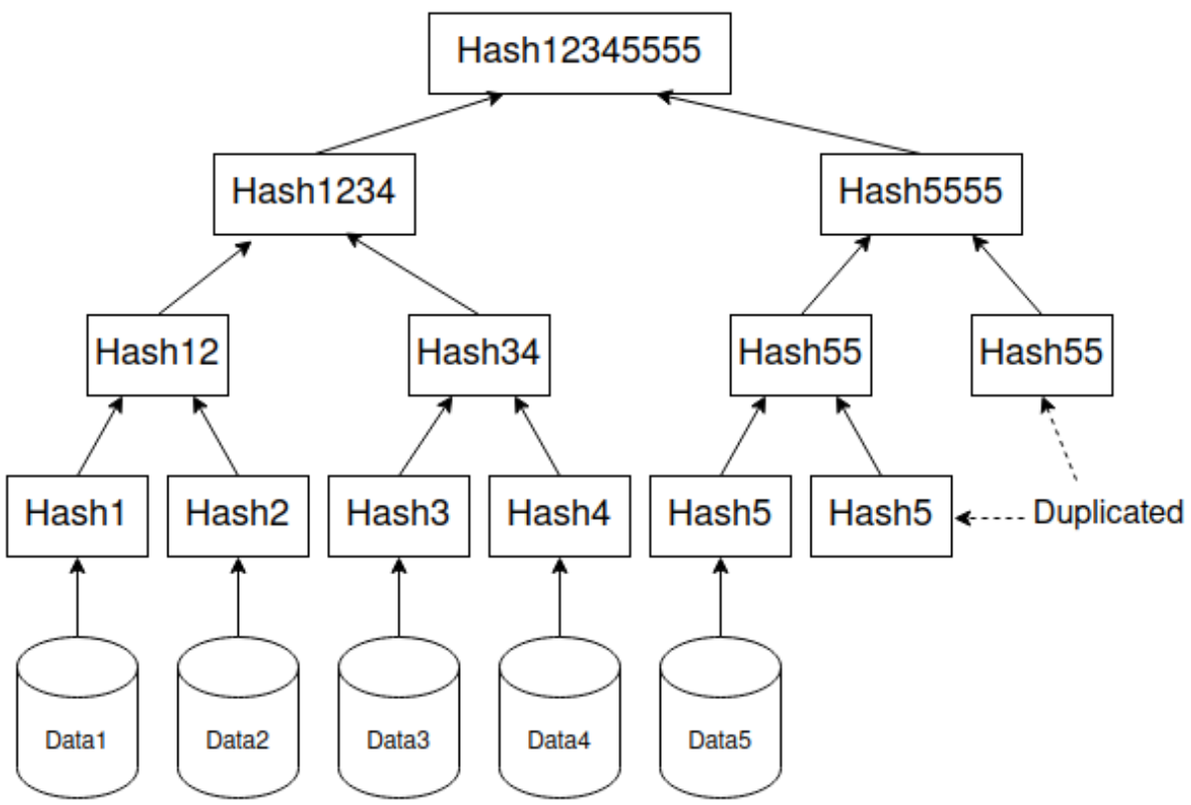


Figura 2.4: Struttura di un Merkel Tree

-**Timestamp**: tempo corrente in cui il blocco è attaccato nella catena, si riferisce al tempo in cui il minatore ha iniziato ad estrarre il blocco, espresso in Unix epoch. Ci sono due limitazioni:

- deve essere strettamente maggiore del tempo mediano degli 11 blocchi precedenti;
- i full nodes (discussi nella prossima sezione) non accettano blocchi con intestazioni più di due ore nel futuro secondo il loro orologio.

- **Target nBits**: rappresenta la difficoltà del processo di mining necessaria per validare il blocco. È una soglia target, chiamata anche hash target, ed è un valore numerico soglia: il block header deve essere "less than or equal to" al fine di validare il blocco. I minatori devono convalidare il blocco in base a questo limite. Approfondiremo questo aspetto nel capitolo relativo al mining.

- **Nonce**: è l'abbreviazione di numero usato solo una volta (n-once). Questo valore deve essere trovato dai minatori per convalidare i blocchi. La nonce è un parametro che i minatori devono trovare con un processo deterministico (trial and error): è una stringa casuale di numeri aggiunta al contenuto dell'hash del blocco, e poi ri-hashata. Se l'hash soddisfa i requisiti stabiliti nel Target nBits, allora il blocco viene aggiunto alla Blockchain. Questo processo è chiamato Proof of Work.

- **Parent block hash**: un hash SHA256 nell'ordine interno di byte dell'intestazione del blocco precedente. Questo certifica che nessun blocco precedente può essere modificato senza modificare anche la sua intestazione.

Il **corpo del blocco** (block body) contiene il **Transaction counter**, ovvero un contatore delle transazioni validate all'interno del blocco stesso, dove le transazioni sono ordinate come sono state disposte nella riga 1 dell'albero di Merkle. La dimensione del Transaction counter dipende dalla dimensione massima consentita per il blocco. Quest'ultima è decisa dal protocollo

Bitcoin, attualmente la dimensione massima del blocco è di 1 MvByte[11]. Il protocollo Bitcoin può essere modificato dalla comunità Bitcoin, composta da minatori e sviluppatori, attraverso la Bitcoin Improvement Proposal (BIP). Quando una BIP ottiene la maggioranza può essere aggiornata nella versione del software Bitcoin.

Di seguito viene riportata la rappresentazione di un blocco (nello specifico del blocco 763598), da parte di un explorer che, oltre a raccogliere le informazioni di ogni blocco a partire dal blocco genesi, mostra in tempo reale la creazione dei blocchi di Bitcoin. L'insieme di quadrati sulla destra è la raffigurazione astratta delle diverse transazioni di dimensioni diverse, inserite nello spazio disponibile del blocco. Il quadratino in basso a sinistra, raffigurato in verde, rappresenta la Coinbase Transaction.

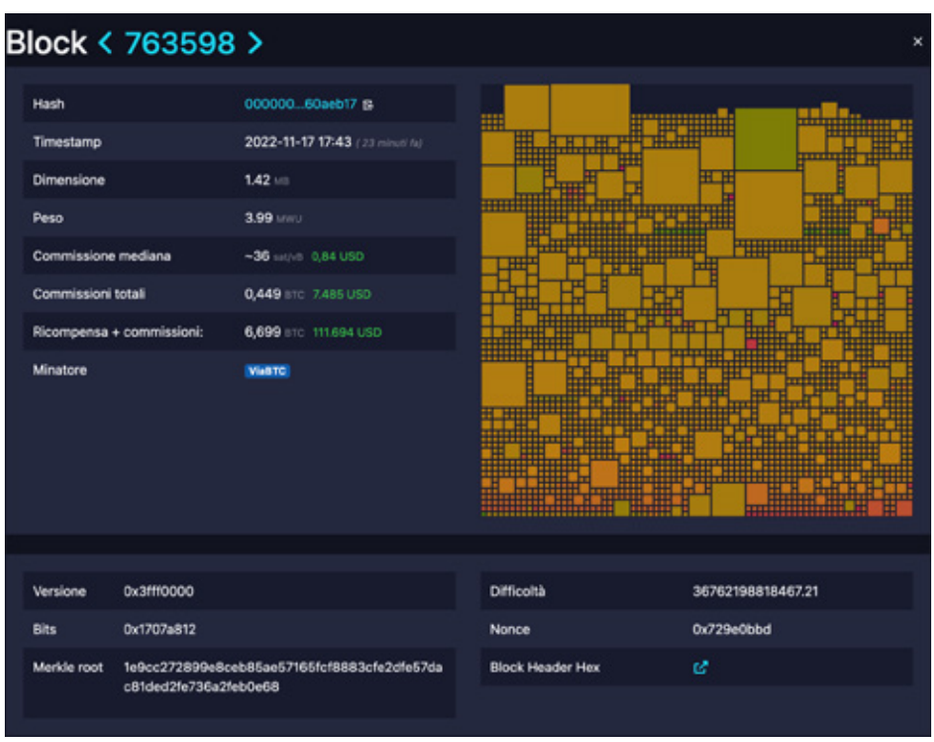


Figura 2.5: Blocco numero 763598

[11] Il vByte è l'unità di misura per lo spazio dei blocchi. Un vByte corrisponde a 4 weight units. Il weight unit è stato introdotto con l'upgrade SegWit nel 2017. Prima di esso i blocchi si misuravano in byte, ed erano grandi 1 milione di byte (1MB), dopo il Segwit i blocchi sono stati limitati a 4 milioni di weight units, o 1MvByte. Questo rende le transazioni fatte con lo standard SegWit più economiche di quelle tradizionali, perchè ogni vByte include 4 weight units, a differenza di una transazione tradizionale dove un Byte è equivalente a un weight unit.

2.7 Transazioni e Utxo

Le transazioni tra due utenti sono definite transazioni **P2PKH** (Pay to PubKey Hash). Una transazione è una comunicazione trasmessa al network in cui un proprietario di bitcoin autorizza il trasferimento di tutti o una parte di token ad un altro proprietario. Di fatto il vecchio possessore delle monete rinuncia alla loro proprietà, ed assegna come nuovo proprietario l'utente destinatario. Pertanto è la moneta a riportare all'interno di essa le informazioni sul suo proprietario, e non viceversa. Ogni transazione è composta da uno o più input e da uno o più output, viene quindi spostato valore dagli input agli output. La differenza tra input e output è rappresentata dalle commissioni di transazione. In gergo tecnico input e output sono denominati UTXO, ovvero "unspent transaction output". In sostanza la blockchain rivela la cronologia dei proprietari dei vari UTXO.

INPUT: ciascun input è dato da un precedente output. L'utilizzo di questi input è vincolato dal possesso della chiave privata ad essi associata.

OUTPUT: di conseguenza un output è il risultato di uno o più input, che hanno cambiato proprietario. Se il valore che il mittente voleva inviare tramite la transazione è minore della somma degli input utilizzati, verrà generato un altro output, che rappresenta il resto della transazione, che ritornerà, sotto forma di UTXO, in possesso del mandante.

Nell'immagine seguente sono rappresentati gli input e gli output di una comune transazione Bitcoin.

Figura 2.6: Transazione con resto

Possiamo vedere a sinistra gli UTXO sotto il controllo delle chiavi private appartenenti a questo indirizzo pubblico:
`1JieD8Fuqkrtyde85o8Z2f7osQdfxBWKaL`

L'utente in questione ha deciso di trasferire l'equivalente di 0,00920000 BTC all'utente in possesso delle chiavi private collegate a questo indirizzo pubblico:
`1CP8m7gT81yaopwnAJLF652b7tCywW4er9`

Viene quindi generato un UTXO di quel valore, ora in possesso del ricevente della transazione. Il secondo output presente nella parte destra rappresenta il resto della transazione. Infatti la somma degli input è maggiore del valore che il primo utente voleva trasferire. Questo UTXO viene rimandato al mittente, e sarà disponibile ad essere speso da esso.
Si noti però che la somma degli input è leggermente superiore alla somma degli output, questa differenza è data dalla commissione di transazione, e verrà inviata al miner, come incentivo per la risoluzione del blocco. In questa transazione la commissione, detta "transaction fee" è pari a 0,00019632 BTC.

Di seguito sono rappresentati gli input e gli output di una transazione senza resto, e successivamente un'altra con resto, ma con un unico input.

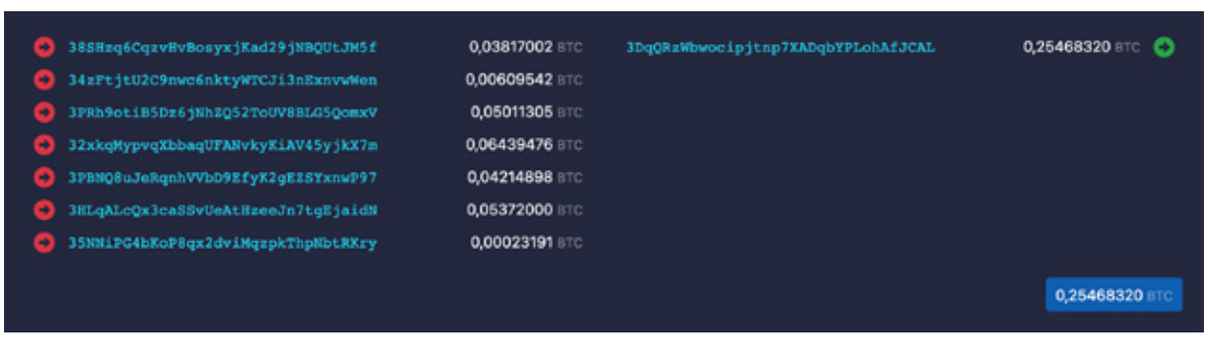


Figura 2.7: Transazione senza resto

Figura 2.8: Transazione con un unico input

La dimensione di una transazione dipende dalle informazioni contenute in essa, quindi anche dal numero di input e output. Si vedrà in seguito che il costo delle commissioni è proporzionale al peso della transazione. Banalmente si possono trasformare più UTXO in un unico, semplicemente inviando a se stessi questi UTXO, andando a crearne quindi uno solo. La Coinbase Transaction, accennata in precedenza, è l'altro tipo di transazione oltre al P2PKH, ed a differenza di questa è priva di input, e presenta un unico output. Essa va a creare un UTXO che, come già visto, verrà inviato ad un indirizzo pubblico appartenente al miner responsabile della risoluzione del blocco. Visto che l'emissione di nuovi bitcoin dipende unicamente dalla Coinbase transaction, ne consegue che tutti gli UTXO sono generati a partire dagli UTXO creati dalle Coinbase transaction.

2.8 Network e nodi

Il protocollo Bitcoin si basa su diversi nodi per funzionare come registro (libro mastro) distribuito delle transazioni di bitcoin (moneta virtuale del protocollo). Grazie al suo design, è resistente alla censura e non richiede la presenza di terze parti per la convalida delle transazioni, essendo un circuito completamente P2P, indipendentemente dalla distanza che separa i due utenti. Ci sono diversi tipi di nodi, definiti in base alle loro funzioni specifiche:

- **Full nodes**: nodi che supportano e garantiscono la sicurezza della rete e che dispongono di una copia dell'intera blockchain. Hanno la funzione di verificare e trasmettere le proprie transazioni (o quelle di terzi, che non avendo un proprio Full node devono necessariamente appoggiarsi ad un Full

node a scelta o casuale) alla Mempool, che analizzeremo in seguito. Inoltre, aggiornano la blockchain ogni volta che viene generato un nuovo blocco, verificando che questo rispetti tutte le regole imposte dal software, quindi che sia corretta la quantità di bitcoin estratti, che le firme digitali delle transazioni siano valide, che la dimensione del blocco non superi il limite previsto. Per sostenere il network di Bitcoin, molte organizzazioni e utenti, su base volontaria, possiedono un full node per assicurare il processo di convalida e l'aggiunta di nuovi blocchi alla blockchain. I full nodes possono essere visibili oppure nascosti.

- **Listening nodes**: sono full nodes non nascosti, le cui funzioni sono la comunicazione e la fornitura di informazioni a qualsiasi altro nodo che decide di avere un'interazione con esso. Conosciuti anche come supernodes, potrebbero essere visti come un punto di ridistribuzione che agisce come fonte di dati e come ponte di comunicazione. I nodi di ascolto affidabili funzionano tipicamente 24/7.

- **Miner's nodes**: i miners sono nodi adibiti a creare i nuovi blocchi, inserendo le transazioni prese dalla Mempool, per poi comunicarli al resto del network composto dagli altri miner's nodes, che valuteranno se aggiungerlo alla catena o scartarlo. Una transazione non risulta attendibile fintanto che non viene impressa in un blocco, e questo accettato dal network. Si noti che un blocco può essere scartato dai nodi, per vari motivi, pertanto una transazione è da considerarsi confermata dopo un numero il più elevato possibile di conferme[12].
Le conferme sono rappresentate dal fatto che a quel blocco vengono concatenati altri blocchi. Come già accennato in precedenza, infatti, può capitare che vengano a formarsi due biforcazioni della blockchain, e il network ac-

[12] Tecnicamente una transazione con una sola conferma può essere annullata se si dispone di sufficiente potenza di calcolo per ricalcolare l'ultimo blocco e quello precedente, contenente la transazione. Già dopo tre conferme risulta abbastanza improbabile l'annullamento, servirebbe infatti ricalcolare tre blocchi più quello della transazione, oltre la sesta conferma la transazione è considerata irreversibile.

cetterà solo quella più lunga, scartando l'altra. I minatori possono essere individuali oppure collaborare assieme per formare una Mining Pool, in questo caso mettendo a disposizione la propria forza computazionale, per poi spartirsi in maniera proporzionale l'eventuale ricompensa. In seguito verrà descritto nel dettaglio il processo di mining nei suoi particolari.

- **Lighitweight or SPV clients**: I client SPV (Simplified Payment Verification) sono coloro che fanno uso della rete Bitcoin, ma non agiscono come un full node, poiché non mantengono né una copia della blockchain né partecipano al processo di convalida e verifica delle transazioni. I client SPV possono verificare le transazioni, se sono state incluse o meno in un blocco ricavando le informazioni da un altro Full node.

Inizialmente, con la versione 0.1.0 di Bitcoin, i nodi erano tutti uguali, svolgevano quindi sia il ruolo di full node, che di miner. Successivamente i compiti sono stati suddivisi, e si è arrivati a distinguere i nodi in base al tipo di lavoro che andavano a svolgere. I full nodes quindi si limitano a validare le transazioni e inviarle nella Mempool, mentre i miner's nodes si occupano esclusivamente di eseguire la Proof of Work sui blocchi.

2.9 Mempool

Approfondiamo ora il concetto di Mempool, citato in precedenza. Facendo un parallelismo, potremmo considerare la Mempool come la sala d'attesa in cui risiedono le transazioni prima di essere inserite in un blocco. La logica della scelta di quali transazioni includere in un blocco da parte del miner si basa sul principio di convenienza, si darà quindi priorità alle transazioni che pagano costi di commissione più elevati. Da qui si capisce che un utente, per ridurre i tempi di convalida, quindi ottenere la priorità per la propria transazione, dovrà impostare una commissione più alta rispetto alla maggior parte delle transazioni presenti in Mempool, come incentivo ai miner. Le commissioni rappresentano il costo che sei disposto a pagare per ottenere lo

spazio necessario alla tua transazione all'interno del prossimo blocco, che è limitato come da protocollo. Quindi, come già accennato in precedenza, più una transazione occupa spazio, più le commissioni saranno maggiori, queste ultime si calcolano in sats/vByte.

2.10 Proof of work e politica monetaria

Abbiamo in precedenza visto che i miners sono i nodi validatori che gestiscono e supportano l'infrastruttura Bitcoin. Sono imprenditori che investono in infrastrutture tecnologiche specifiche per assicurare la convalida continua dei blocchi per la rete. Il protocollo Bitcoin per incentivare questo ruolo, per avere la potenza computazionale per far funzionare la rete, li ricompensa attraverso la Coinbase transaction. Il processo di convalida che porta alla produzione di nuovi blocchi inizia con la scelta e la verifica delle transazioni da includere all'interno del blocco. Successivamente il miner dovrà prendere l'hash relativo all'ultimo blocco aggiunto alla blockchain, e includere questa informazione all'interno del blocco nuovo. A questo punto cerca di risolvere per primo la prova di lavoro, che in caso positivo verrà preso in esame dal resto della rete, e se ritenuto valido verrà aggiunto alla blockchain.

- Proof of Work:
La Proof of Work è un processo che richiede ai membri di una rete di utilizzare forza computazionale per risolvere un puzzle matematico arbitrario. Bitcoin riprende il concetto di Proof of Work da Adam Back, utilizzato in HashCash, che sfrutta le proprietà delle funzioni di hash. Il puzzle matematico consiste nel trovare un hash che rispetti le regole imposte dal protocollo di Bitcoin. I miners hanno la possibilità di raggiungere l'obiettivo modificando il parametro nonce, aggiunto a un dato arbitrario convertito in numero esadecimale, con un processo di forza bruta di tipo trial and error. Il risultato dell'hash è completamente differente per ogni incremento del valore di nonce, ed il protocollo considera il problema risolto se il risultato dell'hash è minore di un valore soglia T, fissato dalla rete. Più piccolo è questo valore,

più è alta la difficoltà del problema. La soluzione si ottiene quindi trovando un x, tale che $H(x) < T$.

Il dato arbitrario sottoposto a funzione di hash è il block header del blocco da validare, variando in maniera incrementale il valore nonce all'interno di esso. Si sottopone questo dato a un doppio hash SHA256, e si confronta il risultato con il valore T: se è minore di T, il miner ha risolto il problema e il blocco viene comunicato alla rete, che se lo reputa valido verrà aggiunto alla blockchain.

In questo modo, il protocollo bitcoin assicura che la maggior parte della potenza di hash sia utilizzata per sostenere la rete bitcoin, con la conseguenza di integrità e protezione dei dati, disincentivando l'utilizzo della forza computazionale in maniera antagonista.

- **Difficoltà**:
La difficoltà del processo di mining, come specificato in precedenza, è indicata dal Target nbit, da cui dipende il valore T indicato nel paragrafo precedente. In base alla potenza di calcolo dei minatori, questa soglia viene aggiornata dal protocollo bitcoin ogni due settimane circa (in realtà ogni 2016 blocchi, che calcolando una media di 10 minuti per blocco si traduce in due settimane) permettendo ai minatori di risolvere il problema di hashing con una media di 10 minuti. Di solito accade che nei primi giorni in cui l'aggiornamento è stato introdotto che i minatori riescano a validare il blocco con una media di 10-11 minuti, e, con l'aumentare dei giorni, all'aumentare della forza computazionale del network, il tempo di validazione cali drasticamente fino al successivo aggiornamento del sistema. In pratica, il Target nBits è il numero di zeri con cui deve iniziare l'hash del blocco, nell'esempio precedente T, più zeri sono richiesti, più potenza computazionale è necessaria.

- Politica monetaria:
La prima transazione inserita in un nuovo blocco è obbligatoriamente la Coinbase transaction, in cui il miner che convalida il blocco, indirizza la ricompensa del blocco per il processo di mining ad un indirizzo pubblico di sua scelta. La Coinbase transaction comprende due parti: Transaction fees e Block subsidy, dove la prima si riferisce alle commissioni pagate da coloro che effettuano transazioni nel circuito, mentre la seconda si riferisce ad un sussidio dato al miner, consistente in nuovi bitcoin generati dal protocollo.

Il sussidio di blocco, consistente in nuovi bitcoin emessi dal protocollo, determina la politica monetaria del progetto Bitcoin. Il sussidio diminuisce ad un ritmo programmato: ogni 210'000 blocchi aggiunti alla catena (circa 4 anni), il sussidio si dimezza, questo processo è identificato come halving. All'inizio il protocollo Bitcoin dava una ricompensa di 50 BTC. Attualmente siamo ad una block subsidy di 6,25 BTC.

Il protocollo ha fissato un numero massimo di bitcoin nel circuito di 21 milioni di BTC. In figura 2.9 è illustrata la politica monetaria. La Coinbase transaction è un tassello fondamentale di Bitcoin, preso direttamente dal concetto di RPOW (Reusable Proof of Work) formulato da Hal Finney in una mail condivisa nella mailing list dei cypherpunks datata 15 agosto 2004.

L'idea è quella di trasformare la prova di lavoro svolta dal miner in token, quindi renderla trasferibile. In pratica è lo stesso concetto per cui paghiamo un professionista per il lavoro svolto. Ed è da qui che i token bitcoin prendono un valore reale, rendendoli oggetto di scambio di valore.

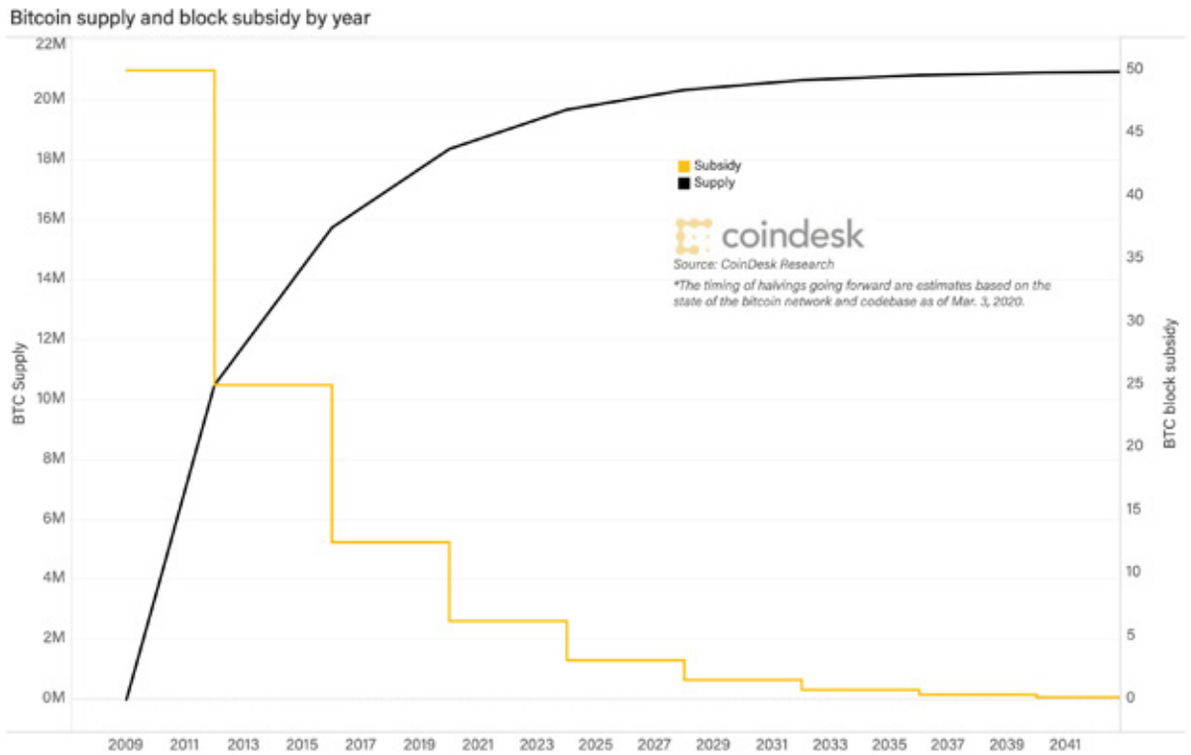


Figura 2.9: Grafico che confronta la ricompensa ai miners con la quantità circolante di bitcoin

La PoW non è l'unico meccanismo di consenso che si propone di risolvere il problema del double spending, dopo la creazione di Bitcoin altri hanno concettualizzato altri meccanismi di consenso per risolvere il problema della doppia spesa, come la Proof of Stake, la Pure proof of Stake, la proof of history, ecc. La PoW è il meccanismo di consenso più maturo e il longevo ad ora. Il concetto di PoW deriva dal principio di Landauer[13] per cui ogni calcolo non reversibile deve consumare un minimo di energia, e poiché SHA-256 non è un processo reversibile, l'energia viene convertita in bit. Per queste ragioni, di solito i minatori investono molto in infrastrutture dedicate e si installano in luoghi dove l'energia costa poco e il clima è freddo, in questo modo possono risparmiare sui costi di mantenimento del raffreddamento.

[13] Il principio di Landauer è stato enunciato da Charles Bennett nel 2003 come segue: Qualunque manipolazione dell'informazione logicamente irreversibile, come la cancellazione di un bit o la confluenza di due percorsi computazionali, deve essere accompagnata da un corrispondente aumento dell'entropia dei gradi di libertà non contenenti informazione dell'apparato che processa l'informazione o del suo ambiente.

Dato che la risoluzione del blocco è un processo deterministico, con l'aumento della difficoltà nella rete, molti minatori hanno iniziato a collaborare tra loro per acquisire più potenza di calcolo nei cosiddetti mining pool.
È raro, ma potrebbe accadere che due diversi minatori propongono un blocco valido nello stesso momento. In questo caso, ci sarà una temporanea biforcazione in due catene: la catena più lunga continuerà ad essere la blockchain di riferimento, e quella corta verrà abbandonata, con la conseguenza di riassemblare in nuovi blocchi le transazioni approvate in quest'ultima. La blockchain di riferimento è la blockchain posseduta nella memoria locale della maggioranza dei minatori.
Un altro problema in relazione alla doppia spesa sorge se un utente crea due transazioni, inviando la stessa moneta a diversi destinatari, e le pubblica entrambe nello stesso momento in diverse parti del mondo, allora a causa della latenza della rete, alcuni nodi della rete riceverebbero la prima transazione e rifiuterebbero la seconda come doppia spesa, mentre altri nodi potrebbero fare il contrario. La soluzione si basa sul meccanismo di consenso esposto nel paragrafo precedente, la catena più lunga è la Blockchain e sarà valida solo una transazione, di conseguenza, quella che è stata più trasmessa e prima accettata in un blocco valido.

Ethereum
3.1 Protocollo

Ethereum è la seconda criptovaluta per capitalizzazione all'interno del settore. Ethereum è stata ideata da Vitalik Buterin, un russo classe 94 trasferitosi in Canada con i genitori all'età di 6 anni. Appassionato di crittografia ed informatica, nel 2011 inizia a scrivere per una rivista del settore, Bitcoin Weekly, guadagnando 5 BTC (circa 3,5$ al tempo) per ogni articolo scritto. Nello stesso anno co-fonda Bitcoin Magazine, rivista in cui tratta l'argomento criptovalute.

La peculiarità di Ethereum, poi in seguito copiata da molti progetti nel settore, è che si pone in essere come una piattaforma informatica distribuita blockchain-based che permette a sviluppatori di costruire e distribuire le loro applicazioni decentralizzate.
Il suo creatore compara il progetto Bitcoin con Ethereum tramite una metafora: "Pensa alla differenza che c'è tra una calcolatrice e uno smartphone: la calcolatrice fa una cosa e la fa bene, mentre su uno smartphone hai una calcolatrice come app, puoi ascoltare musica, navigare sul web e fare molte altre cose" paragonando Bitcoin alla calcolatrice ed Ethereum allo smartphone.
Ethereum si differenzia da Bitcoin in quanto la sua blockchain è un registro distribuito account based a differenza di Bitcoin che è definito transactional based. Bitcoin aggiorna in ogni blocco la storia percorsa da ogni UTXO all'interno del network e da quest'ultima deriva l'ammontare di moneta nativa (BTC) detenuta da ogni partecipante nel network. Ethereum, invece, per ogni blocco aggiunto nella sua blockchain, aggiorna ogni volta lo stato degli account e non la movimentazione precisa delle coin al suo interno.

Ethereum adottando una struttura simile a Bitcoin incorpora linguaggi di programmazione (Solidity e Vyper su tutti), rendendo il protocollo Turing Complete, dove per Turing Complete si intende: "A system (computer sy-

stem, programming language, etc.) that can be used for any algorithm, regardless of complexity, to find a solution".

La caratteristica di Turing Complete di Ethereum significa che esso è in grado di utilizzare la sua base di codice per eseguire praticamente qualsiasi attività, purché abbia le istruzioni corrette, tempo e potenza di elaborazione sufficienti. Al contrario, il linguaggio di scripting utilizzato in Bitcoin è intenzionalmente progettato come Turing Incomplete perché una maggiore complessità potrebbe potenzialmente introdurre problemi, tenendo semplice il suo funzionamento è più facile renderlo maggiormente prevedibile.

Il protocollo Ethereum, come sopra detto, è basato su account, per la precisione vi sono due tipologie di account: gli user account e i contract account. I primi sono controllati da private keys ed appartengono ad umani, per utilizzare questi tipi di account è necessario mandare una transazione con un destinatario ed una quantità di ether e firmarla con la propria private key (come nel circuito di Bitcoin) mentre i secondi sono controllati da codici. Ogni qualvolta che un contract account riceve un messaggio, il suo codice viene attivato, consentendogli di leggere e scrivere nella memoria interna e inviare altri messaggi o creare contratti a sua volta. Questi sono definiti smart contract, ovvero un "insieme di promesse, compresi i protocolli, specificate in forma digitale, all'interno dei quali le parti eseguono tali promesse" (Nick Szabo, 1996). In altre parole, è un programma digitale che contiene i termini e le condizioni di un contratto concordato tra pari, a differenza del nome, uno smart contract non è poi così smart: infatti è un algoritmo che ripete le funzioni al suo interno e non ha niente a che fare con l'IA.
I contratti sono paragonabili ad agenti autonomi che vivono all'interno dell'ambiente di esecuzione di Ethereum, eseguendo sempre un pezzo specifico di codice quando "colpiti" da un messaggio o una transazione e hanno il controllo diretto sul proprio saldo di ether e sul proprio archivio di chiavi/valori per tenere traccia delle variabili persistenti.

L'unione di più smart contract dà vita ad applicazioni decentralizzate. Si può pensare ad Ethereum come un grande computer distribuito, dove i programmi scritti dagli sviluppatori vengono immagazzinati non in server centralizzati ma sulla blockchain di Ethereum, ed essi sono sempre attivi grazie alla Ethereum Virtual Machine.
L'EVM è una macchina virtuale progettata per operare come un ambiente di esecuzione per creare e distribuire smart contract, è praticamente il motore che comprende ed esegue i programmi scritti con il linguaggio di programmazione di Ethereum. L'EVM viene utilizzato in una modalità sandbox, ovvero in un ambiente isolato dalla rete principale, si tratta perciò di un ambiente di test perfetto.
Uno smart contract è compilato mediante vari linguaggi di programmazione, il più utilizzato è Solidity, una volta progettato lo smart contract viene successivamente trasformato in codice binario, perché l'EVM legge ed esegue algoritmi scritti in codice binario.

3.2 Ether

Ether (ETH) è la criptovaluta nativa del protocollo Ethereum ed è utilizzata per pagare per le risorse computazionali ed i costi di transazione per ogni transazione eseguita sul circuito.
ETH, al pari di BTC, può essere utilizzata come moneta per transazioni P2P, a differenza di quest'ultimo essa è utilizzata anche per comprare il gas[14], il quale è a sua volta utilizzato per pagare nel circuito per svolgere i vari calcoli computazionali richiesti dagli smart contracts. Il gas è il costo di esecuzione pagato dall'utilizzatore per l'esecuzione di una transazione.
Il costo del gas varia in ogni momento nel network e dipende dal traffico sulla rete Ethereum.

[14] I prezzi del gas sono indicati in Gwei, che è a sua volta un taglio dell'ETH: ogni Gwei equivale a 0,000000001 ETH (10^-9 ETH). Per esempio, invece di dire che il carburante costa 0,000000001 Ether, puoi dire che costa 1 Gwei. La parola 'gwei' significa 'giga-wei', ed è pari a 1.000.000.000 wei. Wei (dal nome di Wei Dai, creatore di b-money) è l'unità più piccola di ETH.

La formula per il costo di transazione per includere una determinata operazione nella blockchain di Ethereum è la seguente:

Tx Fees = Gas Limit * Gas Price

dove:

Gas Limit = si riferisce all'ammontare di gas utilizzato per la computazione
Gas Price = equivale al prezzo del gas

L'utente che deve svolgere una determinata operazione all'interno del network, impostando un Gas Limit maggiore avrà maggiori possibilità di vedere inclusa da parte del miner la sua operazione nel prossimo blocco, nella stessa logica delle commissioni su Bitcoin.
Operazioni computazionalmente più impegnative, come la scrittura di smart contract complessi o la creazione di applicazioni (essendo queste ultime l'insieme di più smart contracts), richiedono un costo in Ether maggiore rispetto ad operazioni più semplici. Questo meccanismo è un meccanismo economico di efficientamento all'interno del network, dato che il network richiede un costo per l'upload di operazioni, saranno maggiormente incentivate operazioni che apportano un beneficio (con conseguente guadagno per lo sviluppatore che ha progettato lo smart contract) rispetto a futili operazioni.

3.3 Meccanismo di consenso

- Proof of Work:
Il meccanismo di consenso prima del 15 settembre 2022 nella rete Ethereum era basato sulla Proof of Work come nel circuito Bitcoin. La politica monetaria di Ethereum è tuttavia differente da Bitcoin. Infatti se per quest'ultimo è decisa già la politica monetaria e il suo tasso di emissione, per Ether non vi è un massima supply, bensì vi è un tasso di inflazione annuo.

- Proof of Stake:

Il 15 settembre 2022, con l'aggiornamento "The Merge[15]" è avvenuto il passaggio da Eth 1.0 (Ethereum basato su PoW) ad Eth 2.0 (Ethereum con PoS), preceduto da altri aggiornamenti preparatori.

I protocolli Proof of Stake sono una classe di meccanismi di consenso per blockchain che funzionano selezionando i validatori in proporzione alla loro quantità di partecipazioni nella criptovaluta associata. Questo viene fatto per evitare il costo computazionale degli schemi di proof of work.

In tale sistema non si hanno più minatori che competono tra di loro ma validatori, i quali in base alle leggi dei vari protocolli blockchain hanno regole diverse.

La prova di skin in the game è data dallo stake allocato dal nodo validatore (capitale "in gioco"). La quota di Ether messo in stake funge da incentivo a comportarsi in modo benevolo da parte del validatore, altrimenti, se dovesse modificare a proprio vantaggio la blockchain , essendo quest'ultima pubblica, gli altri partecipanti al network accorgendosene potrebbero dubitare il buon funzionamento del protocollo e perdere interesse nel suo utilizzo, con conseguente perdita di valore del token e quindi perdita di valore anche per l'attore malevolo, dato che il decremento di valore del token impatterebbe anche sul prezzo del proprio stake. Inoltre vi sono alcuni meccanismi che fungono da deterrente per comportamenti malevoli:

- **Slashing**: viene requisito parte dello stake in caso di comportamento scorretto, parte delle coin in stake vengono prese e trattenute dal protocollo ("slashing" = tagliare, squarciare).

- **Jailing**: blacklist dal ruolo di validatore ("jailing" = mettere in prigione), danno economico non indifferente per il nodo validatore.

[15] Con l'aggiornamento "The Merge" è avvenuta l'unione tra la rete principale di Ethereum e la Beacon Chain, rete sviluppata in parallelo basata sul consenso Proof of Stake, e primo passo per il passaggio ad esso. Questo processo verrà concluso con l'aggiornamento "Sharding", atto a migliorare la scalabilità del network. Vedrà anche ridurre i requisiti di hardware, tramite un sistema che eviterà di dover archiviare tutti i dati contenuti nel database distribuito. Lo "Sharding" faciliterà quindi l'esecuzione da parte dei client.

Ogni nodo validatore vincola un tot di token (32 ETH) e ottiene la possibilità di essere eleggibile per poter validare un blocco sulla blockchain e ottenere la coinbase transaction (attualmente 2 ETH) più le commissioni dei partecipanti in quel blocco.

3.4 Centralizzazione

La principale critica che viene mossa nei confronti di Ethereum è la tendenza ad essere un sistema centralizzato, a differenza di Bitcoin che presenta come punto di forza la totale distribuzione, impedendo a chiunque di poterne decidere le sorti. Dietro Ethereum si cela una fondazione no profit (Ethereum Foundation) che lavora al progetto in maniera attiva, con individui capaci di influenzarne il percorso. Lo stesso Vitalik è una figura di spicco all'interno della comunità, di conseguenza la sua opinione è molto importante e ne condiziona inevitabilmente gli sviluppi.
Inoltre tramite i sistemi di slashing e jailing è possibile attuare politiche di censura nei confronti degli utenti che vanno contro il pensiero della massa (o della Ethereum Foundation). Questo rappresenta si un punto di forza per arginare i tentativi di attacco al protocollo, ma va contro gli ideali per cui è stato sviluppato Bitcoin, che è un sistema trustless, che non necessita del controllo di un ente centrale, che ha il potere decisionale all'interno del protocollo. Bitcoin a differenza di qualsiasi altra blockchain non ha bisogno di qualcuno per poter funzionare, perché il codice rappresenta la legge ("code is law") e grazie a questo non è necessario dover porre la fiducia in mano di una persona o un ente.

Stablecoins

Ad oggi uno dei principali limiti delle criptovalute è la volatilità rispetto alle valute FIAT[16]. Convenzionalmente la valuta di riferimento con cui si comparano i prezzi delle criptovalute è il dollaro statunitense, dal momento che rappresenta lo standard anche nell'economia mondiale.
Prima dell'avvento delle stablecoin, gli scambi di crypto avvenivano solo attraverso il dollaro, costringendo quindi gli utenti a dover uscire dal circuito della blockchain e rientrare nel circuito delle banche centrali, come riparo dalla volatilità che le caratterizza. La volatilità del mercato crypto è strettamente collegata tra le altre cose alla bassa capitalizzazione del settore, se confrontato con i mercati tradizionali, che ne risentono comunque ma in misura più moderata.

Le stablecoin nascono sia come strumento che permette di potersi riparare dalla volatilità di un mercato ancora troppo giovane, rimanendo comunque onchain, che come moneta spendibile, pur mantenendosi all'interno del mondo crypto.

A tal proposito vale la pena aprire una parentesi sul perché si abbia difficoltà ad oggi ad attribuire a Bitcoin lo status di moneta spendibile, e del perché sia utile avere una alternativa per questo utilizzo. In primis per la sua caratteristica deflattiva, a contrario delle valute FIAT, che si trasforma in un incentivo ad accumulare l'asset piuttosto che spenderlo. Contrapposto a ciò le valute FIAT come Euro e Dollaro subendo un inflazione sempre più accentuata, spingono chi le detiene a spendere piuttosto che accumulare, con il rischio di perdere sempre più potere d'acquisto.

[16] Con valuta FIAT si intende uno strumento di pagamento non coperto da riserve, e quindi privo di valore intrinseco. La valuta FIAT ha un valore grazie al fatto che esiste un'autorità che agisce da garante. Il sistema basato sull'oro come sottostante a garanzia del valore della moneta (gold backed currency) è stato definitivamente abbandonato dagli Stati Uniti nel 1971 con Nixon, e di conseguenza anche dal resto delle valute nel resto del mondo.

Entrando nell'aspetto tecnico, ad oggi esistono tre categorie di stablecoin, con diversi meccanismi che permettono l'ancoraggio (in gergo "peg") alla valuta FIAT (ma non solo, esistono stablecoin ancorate a commodities), ognuna delle quali presenta vantaggi e svantaggi, in relazione all'utilizzo finale:
- **Stablecoin collateralizzate** con sottostante in FIAT (o commodities)
- **Stablecoin overcollateralizzate** da asset volatili
- **Stablecoin parzialmente collateralizzate**
- **Stablecoin algoritmiche** regolate da smart contracts

4.1 Stablecoin collateralizzate

Regolate da un sistema totalmente centralizzato, sono caratterizzate da un sottostante in valutaFIAT parialvaloredellestesse.Prendiamoadesempiolastablecoinpereccellenza del mercato crypto, Theter (USDT), gestita da un azienda a tutti gli effetti, che ne garantisce il sottostante. Per ogni Tether in circolazione quindi, l'azienda detiene un dollaro nelle proprie riserve. Quando si palesa una richiesta di Tether nel mercato crypto, l'azienda crea token USDT pari alla richiesta ed è tenuta a conservare il controvalore in Dollari nei propri fondi. Con l'operazione inversa i token verranno "bruciati" e verrà restituito il controvalore in Dollari. Il meccanismo è abbastanza semplice, ma non perfetto. Essendo un'azienda, Tether deve sostenere dei costi di gestione non indifferenti, basti pensare che nel 2022 la capitalizzazione di mercato di Theter ha superato i 75 Miliardi di dollari.
Per questo motivo una parte del controvalore detenuto viene investita in asset e fondi, in ottica speculativa. Una grossa fetta invece deve essere disponibile per liquidare i token bruciati. Viene da sé che in caso estremo di bank run il rischio principale sia quello di non riuscire a soddisfare la richiesta di liquidità, innescando una perdita del "peg" al Dollaro. Tralasciando gli scenari estremi (l'azienda garantisce sempre la disponibilità istantanea della maggior parte della liquidità), può succedere che in alcuni momenti il controvalore del token scenda sotto il Dollaro (ad ogni modo uno scostamento contenuto, nell'ordine dell'1%). Di conseguenza si azionano operazioni di arbitraggio,

applicate dalla stessa azienda, o da grossi player esterni, che approfittano del momento per applicare strategie di speculazione, comprando quindi grandi quantità di token, aumentando così la domanda, con conseguente recupero del peg.

I limiti ovvi di queste stablecoin sono il fatto di essere completamente centralizzate, la sicurezza è quindi legata alla fiducia posta nell'azienda stessa. Esistono organi di controllo per assicurare la trasparenza dei fondi detenuti come controvalore, inoltre l'azienda è obbligata periodicamente a pubblicare i report relativamente alle quantità di liquidità e asset gestiti.
Sotto la pressione dei governi è capitato che l'azienda Theter congelasse indirizzi ritenuti in possesso di utenti malevoli.

Altra stablecoin completamente collateralizzata molto utilizzata è USD Coin (USDC). Segue Binance USD (BUSD), che rappresenta la stablecoin di riferimento dell'exchange Binance, ma che è emessa dall'azienda Paxos.

4.2 Stablecoin overcollateralizzate da asset volatili

Qui il meccanismo è simile alle stablecoin collateralizzate da sottostante in FIAT, con la differenza che il sottostante in questo caso è rappresentato da asset volatili, tipicamente altre crypto, e il meccanismo è gestito non più da un ente centrale ma tramite smart contracts, pertanto ci addentriamo in un ambiente decentralizzato. Per ripararsi dalla volatilità intrinseca delle crypto che garantiscono il controvalore è necessario che il collaterale sia molto maggiore della capitalizzazione del token di queste stablecoin. Ad ogni modo vengono selezionate quelle crypto che subiscono meno la volatilità nei momenti di recessione del mercato (Bitcoin, Ethereum in primis).
Il meccanismo è gestito dagli utenti della community, che tramite protocolli (chiamate Dapp, Decentralized application) hanno la possibilità di depositare i propri asset a collaterale per creare una determinata quantità di token della stablecoin, quindi avere in cambio quello che è a tutti gli effetti un

prestito nella stablecoin del protocollo. La quantità di stablecoin creata è a discrezione dell'utente che deposita il collaterale. Il rischio associato è che se il valore del collaterale messo a garanzia diminuisce arrivando quasi a pareggiare il valore del prestito in stablecoin, si attiva lo smart contract che venderà il collaterale per conto del protocollo con l'intento di ripagare il prestito contratto dall'utente. L'utente si ritrova così a detenere la quantità di stablecoin presa a prestito, ma non potrà più riscattare il collaterale, perché venduto dalla piattaforma.
Per evitare che la piattaforma diventi insolvente (nel caso che il collaterale viene liquidato per un valore minore del prestito), la soglia di liquidazione è fissata a priori dal protocollo, in maniera totalmente trasparente, e il collaterale liquidato viene venduto nel mercato a sconto per avere la garanzia di un realizzo istantaneo. Sta quindi all'utente ponderare la quantità di prestito in base al rischio associato.

In questo caso non è necessario porre la fiducia nelle mani di un ente centrale, perché la piattaforma è gestita dal codice (code is law). È necessario potersi però fidare di chi ha sviluppato lo smart contract. In casi di bug o problemi di sicurezza, utenti più esperti potrebbero approfittarne a loro vantaggio, trovando il modo di sottrarre liquidità alla piattaforma.
Il peg al dollaro è quindi garantito finché è presente del collaterale con cui si possa scambiare liberamente con i token della stablecoin.

Esempi di stablecoin overcollateralizzate sono Dai (DAI), e Magic Internet Money (MIM), con valori di capitalizzazione di mercato inferiori ai 10 miliardi di Dollari.

4.3 Stablecoin parzialmente collateralizzate

Questa categoria è caratterizzata da stablecoin che presentano una parte di collaterale rappresentato da altre crypto, e una parte algoritmica, legato al suo token. Tutto il collaterale è messo a rendita per creare utile che verrà

distribuito ai detentori del token collegato alla stablecoin.
La prerogativa di funzionamento è strettamente legata alla domanda della stablecoin perché il meccanismo regga è necessario contenere le fughe di capitale, creando dei casi d'uso reali che siano di incentivo per l'utente a possederla.
I momenti di maggiore stress di queste stablecoin sono legati ai crolli di mercato, che potrebbero innescare una vendita massiccia del token con conseguente perdita del peg. Come per le precedenti, anche qui navighiamo in ambiente decentralizzato, il meccanismo è regolato da smart contracts, quindi con i rischi descritti in precedenza.

4.4 Stablecoin algoritmiche

Basate su un sistema di signoraggio, rappresentano la frontiera più sperimentale di questi strumenti. Per capirne il funzionamento vale la pena analizzare l'esempio più noto, relativo all'ecosistema Terra, con il suo token Luna e la sua stablecoin UST.

UST è un token, come tutti i token il suo prezzo è governato dalla domanda e dall'offerta. Più c'è richiesta del token e più il prezzo tende a salire, al contrario più offerta c'è e più si svaluta. L'obiettivo di una stablecoin è però quello di mantenere il prezzo stabile al valore di 1$, per far si che questo accada, ogni volta che c'è richiesta del token, viene aumentata la quantità di token disponibili (total supply), in modo da diluire la capitalizzazione di mercato e mantenere così fisso il prezzo del singolo (prezzo unitario = market cap / total supply). Ma da dove arrivano questi nuovi token e come è possibile crearli? A questo punto entra in gioco il token LUNA, che a differenza di UST è esposto a volatilità. Per come è strutturato l'algoritmo, è possibile convertire il valore di LUNA in UST, bruciando l'equivalente in Dollari di token LUNA pari a una quantità di UST uguale al controvalore di LUNA bruciati. Così facendo aumenta la supply di UST e diminuisce quella di LUNA. Il valore di quest'ultimo quindi si apprezza. Il meccanismo funziona anche al contrario,

se quindi si contrae la domanda per UST vengono bruciati token e vengono restituiti tanti LUNA pari al controvalore in Dollari degli UST bruciati. Vengono aggiunti LUNA alla supply con conseguente diluizione del prezzo. In questo modo il prezzo di UST rimane stabile a 1$. la blockchain di Terra è regolata dal sistema di consenso Proof of Stake, è possibile quindi detenere LUNA (token di governance del protocollo) per partecipare in maniera attiva alla sicurezza della chain, mettendo i propri LUNA in stake, bloccandoli quindi a disposizione del protocollo per convalidare le transazioni, ricevendo reward in LUNA, derivato dalle commissioni.
Si può vedere questo meccanismo come un sistema di arbitraggio, dal momento che il cambio tra UST e LUNA è fissato indipendentemente dal prezzo di UST. Per assurdo, se UST dovesse valere 0.7$, è comunque possibile scambiare 1 UST con 1$ di LUNA, anche se 1 UST vale 0.7$, guadagnando così 0.3$. Questo incentiva l'utente a sfruttare il meccanismo a proprio vantaggio, comprando UST e convertendoli in LUNA, contribuendo a ripristinare il peg al Dollaro. Vale ugualmente il percorso inverso, nel caso in cui UST arrivi a valere più di 1$, è possibile scambiare 1$ di luna per 1 UST, che varrà quindi di più, per poi rivenderlo a mercato e incassare la differenza.
Il meccanismo è gestito totalmente da smart contract, con rischi e benefici descritti nei paragrafi precedenti.

Il sistema rimane sostenibile se c'è una domanda costante su UST, per mantenere questa condizione è indispensabile creare un use case per il token, per avere un incentivo a possederlo e utilizzarlo. L'incentivo principale era rappresentato dalla possibilità di mettere a rendita i propri UST a fronte di un interesse del 20% circa, sulla piattaforma Anchor Protocol, protocollo di lending e borrowing su alcune cryptovalute.

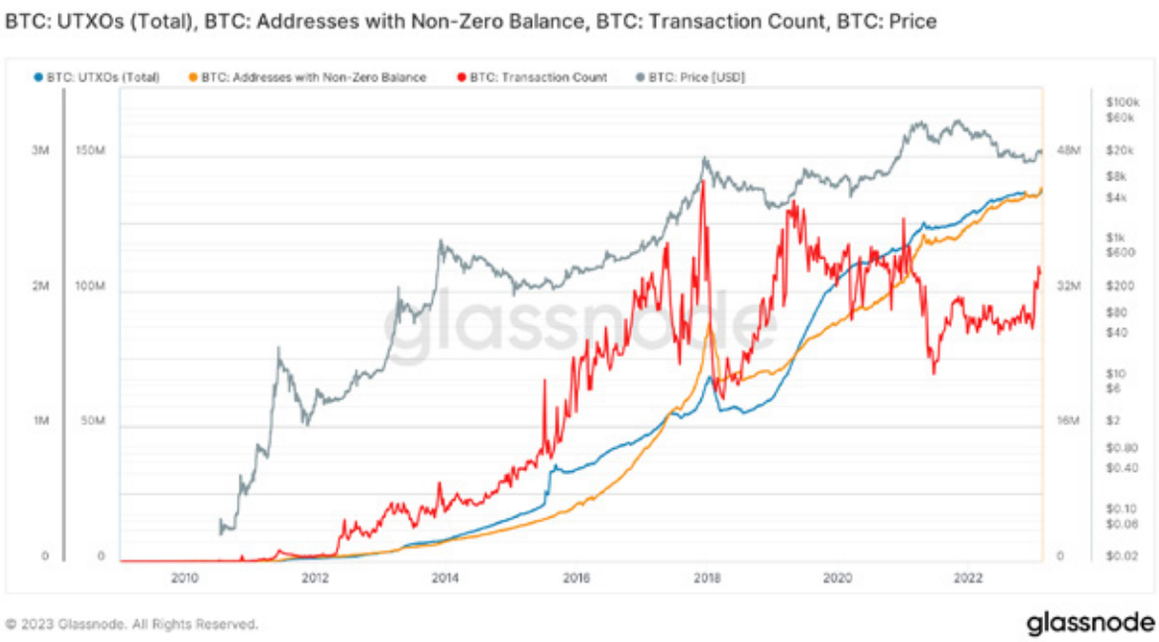
Il protocollo non ha avuto problemi fino al 9 maggio 2022, in cui grossi player hanno messo alla prova il sistema mettendo in atto un attacco con lo spostamento di enormi capitali, atto a realizzare un grosso profitto ai danni della piattaforma. Questo ha innescato la perdita del peg di UST che è arri-

vato a valere 0.75$ nel giro di appena 12 ore. A questo punto si è scatenato il panico e si è innescata la bank run che ha portato a una grande fuga di capitali. Il punto di non ritorno si è verificato nel momento in cui la capitalizzazione di mercato di LUNA è scesa al di sotto di quella di UST. Ci si è ritrovati nella condizione in cui non c'era sufficiente liquidità per ripristinare il peg, che diminuiva in maniera più rapida rispetto al meccanismo di recupero. Il meccanismo ha diluito così tanto la supply di LUNA che nei 4 giorni successivi è passata ad essere scambiata sugli exchange da 60$ a meno di 0.0001$. In una situazione del genere in cui c'è solo offerta per entrambi i token, anche il prezzo di UST è crollato fino ad arrivare a valere meno di un decimo del valore iniziale.

Analisi esplorativa di metriche

In questo capitolo affrontiamo un'analisi esplorativa di metriche, al fine di fare considerazioni riguardo all'adozione di Bitcoin, all'hash power utilizzato nel meccanismo di consenso e come questi vanno ad incidere sul prezzo.
I grafici sono stati creati tramite Glassnode, una società di analisi che, tramite un aggregatore, ti permette di confrontare e personalizzare metriche di diversa natura, attingendo da una banca dati riguardante Bitcoin e altre criptovalute.

Iniziamo considerando l'adozione di Bitcoin, quindi se effettivamente vi è un incremento dell'utilizzo reale in rapporto al prezzo.
Il seguente grafico riporta il totale di UTXO presenti nel network, il numero di addresses con un bilancio positivo di bitcoin e il numero di transazioni effettuate sul network (dati settimanali), il tutto confrontato con il prezzo in scala logaritmica.

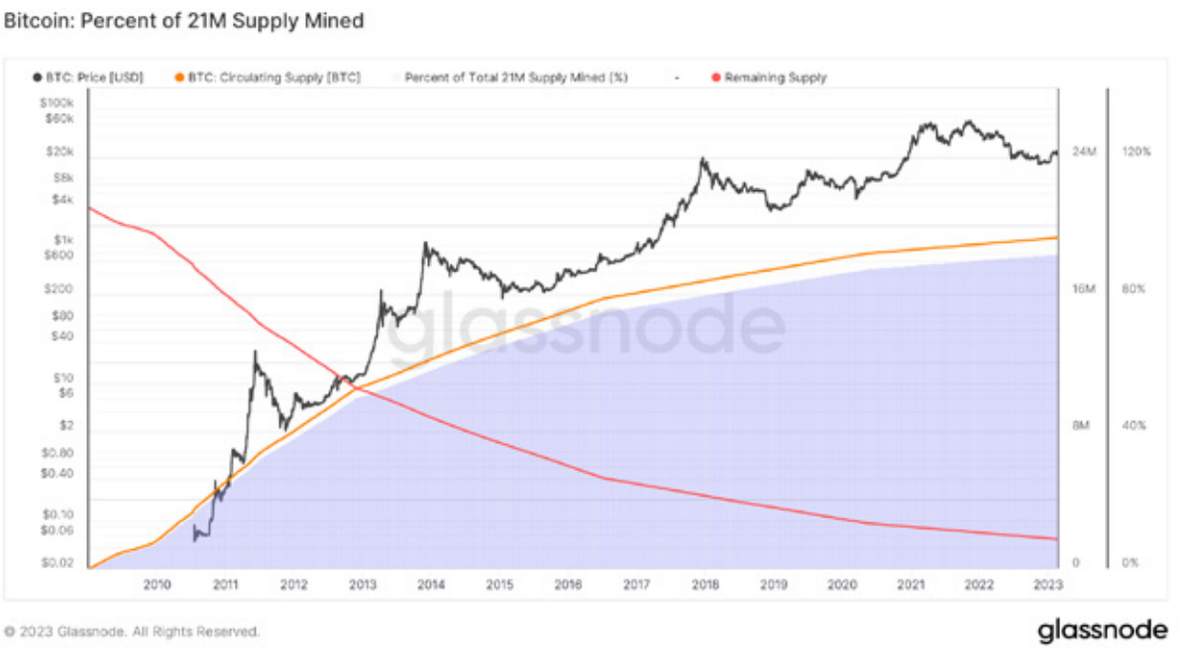


Il trend degli addresses è chiaramente positivo, il numero di transazioni ha avuto il suo massimo con il picco di prezzo di fine 2017, quando un bitcoin

veniva scambiato per $20.000, per poi trovare un equilibrio.
Ci sono diverse considerazioni da fare a tal proposito: ricordiamo infatti che fino ad inizio 2017 Bitcoin rappresentava l'85% di capitalizzazione di mercato dell'intero settore crypto, valore che è calato drasticamente durante tutto il 2017 a causa della bolla speculativa delle altcoins, quando i capitali si sono spostati su di esse, per poi rientrare in Bitcoin in maniera progressiva dal 2018 in poi. Questo fenomeno ha tolto interesse su Bitcoin, facendo calare drasticamente anche le transazioni sul network, durante il periodo descritto; successivamente si è stabilizzato, perchè ricordiamo che c'è un limite fisico al numero di transazioni che possono essere inserite nei blocchi, creati ogni 10 minuti circa, dato dallo spazio massimo di essi. Il peso di ogni transazione è dettato dal numero di UTXO che questa utilizza. A riguardo, notiamo chiaramente come anche gli UTXO siano in costante aumento, e questo è un fenomeno inevitabile, dal momento che, all'aumentare del prezzo di Bitcoin, per trasferire lo stesso controvalore in dollari, è necessario frammentare questi in parti sempre più piccole. Inoltre, ad ogni Halving gli UTXO creati tramite Coinbase Transaction rappresentano quantità di bitcoin sempre minori, quindi 1000 bitcoin minati nel prossimo halving corrisponderanno al doppio degli UTXO rispetto a 1000 bitcoin minati oggi.

Passiamo ora ad analizzare l'impatto che ha il metodo di consenso del network sul prezzo. Per fare questo è necessaria una piccola premessa.

Come spiegato in precedenza nel capitolo sul mining, l'attività di mining di Bitcoin è responsabile della creazione di nuova moneta ottenuta come premio dal soggetto che è stato in grado, tramite potenza computazionale, di risolvere il puzzle matematico necessario a validare un nuovo blocco della blockchain. Il fatto che questa ricompensa venga dimezzata ogni 210.000 blocchi, evento che come già detto prende il nome di halving, rende Bitcoin un asset sempre meno inflattivo, con una produzione che disegna una funzione asintotica con asintoto a 21 milioni di bitcoin.



Durante il primo ciclo halving, durato circa 4 anni, la coinbase transaction era pari a 50 bitcoin per blocco, per un totale di 10.500.000 bitcoin minati, esattamente il 50% dell'intera supply. Nel momento in cui scrivo ci troviamo all'interno del quarto ciclo halving, con 6,25 bitcoin per blocco, al termine del quale ci sarà in circolazione già il 96,875% dell'intera offerta prevista.
Tramite semplici calcoli si può risalire al numero del blocco che minerà l'ultimo satoshi, sarà il blocco 6.930.000, al 34 esimo ciclo di halving. Ricordiamo infatti che l'unità di bitcoin può essere scomposta in centomilionesime sottounità, quindi, nonostante a livello teorico non si raggiunge mai la cifra esatta di 21 milioni di unità tramite continuo dimezzamento, a livello pratico il dimezzamento (approssimato per difetto ove necessario) termina con l'halving che corrisponde ad una ricompensa pari a 0,00000001 bitcoin, ovvero 1 satoshi. La produzione termina perché il dimezzamento di questa ricompensa ha un valore approssimato per difetto a zero, non potendo scomporre ulteriormente la moneta.
A quel punto il guadagno dei miner sarà rappresentato dalle sole commissioni delle singole transazioni incluse nel blocco.

Il meccanismo di mining è fondamentale per l'economia del protocollo; i miners sono imprenditori che hanno importanti costi di gestione da sostenere per avere una produzione efficiente e continuativa, tra costi energetici e di attrezzatura specifica, unito all'applicazione di economie di scala. Risulta quindi fondamentale dover vendere i bitcoin minati.

Questa azione impatta sul mercato creando una sell pressure più o meno pronunciata, in base alle esigenze di dover far cassa.
Alle condizioni attuali (coinbase transaction pari a 6,25 btc), vengono minati circa 900 bitcoin al giorno, con un controvalore ai prezzi attuali di circa 20 milioni di dollari.

Il prezzo rimane stabile se chiaramente c'è abbastanza domanda per assorbire questa offerta, al pari di tutte le altre variabili. Chiaramente questa è una situazione ideale, in primo luogo perché i miners non scaricano i propri bitcoin subito dopo averli ottenuti, ma prediligono farlo in momenti in cui il prezzo è più alto, cercando di accumularli fino a quel momento, salvo imprevisti (come il dover sostenere costi improvvisi). Oltre a questo, il prezzo è influenzato dalla domanda e dall'offerta presente sui vari mercati secondari e dalle notizie e vicende all'interno del settore ma anche di natura politico-economica a livello mondiale.

La presenza di più o meno players che si dedicano al mining impatta direttamente sull'hashrate, ovvero la potenza computazionale totale dei miners connessi al network e come visto nel capitolo sulla Proof of Work, questo va a modificare la difficoltà di mining. L'attività di mining va in qualche modo ad impattare sulla price action di Bitcoin?
Durante i trend rialzisti del prezzo, il mining diventa un'attività molto attraente dal punto di vista della redditività, ci saranno quindi più individui attratti dai possibili profitti; è tipico in questi periodi notare un aumento dell'hashrate del network, causato dai nuovi entranti. Quando il trend inverte la tendenza e il prezzo inizia a calare, molti miners saranno costretti a ven-

dere sempre più bitcoin ottenuti dall'attività, perché a parità di controvalore, corrispondono ora più bitcoin.

Quando questo processo perpetua fino a rendere molte attività di mining insostenibili, ovvero quando si deve ricorrere a vendere tutti i bitcoin minati per sopperire alle spese, si innesca un meccanismo di capitolazione degli stessi miners: molti saranno costretti a spegnere le macchine, trovandosi in una situazione in cui i costi superano i guadagni, con un effetto sull'hashrate del network e a dover liquidare le proprie scorte di bitcoin, accentuando la sell pressure. Rimarranno in gioco solo coloro che hanno un'efficienza tale da poter realizzare un profitto, e non dover quindi vendere tutti i bitcoin minati per pagare le spese di gestione, facendo aumentare drasticamente l'offerta di bitcoin.

Questa fase termina quando si ritorna a un equilibrio per cui il mining è meno oneroso, per la presenza di meno player in gioco, che equivale a una difficoltà minore di mining, e pertanto in queste condizioni si è costretti a vendere meno bitcoin, con una diminuzione della sell pressure: i miners saranno quindi nuovamente in grado di accumulare bitcoin.

Di seguito viene riportato un grafico che presenta un fascio di medie mobili di periodi differenti relative alla difficoltà di mining confrontato con il prezzo di Bitcoin, entrambe le metriche in scala logaritmica. Le fasi di compressione delle medie mobili, dove arrivano anche a sovrapporsi, coincidono con i momenti di capitolazione, fino ad arrivare in casi estremi in cui le medie mobili vanno a invertire; è qui che avviene l'epurazione del mercato del mining, in cui restano attivi soltanto i players più efficienti.

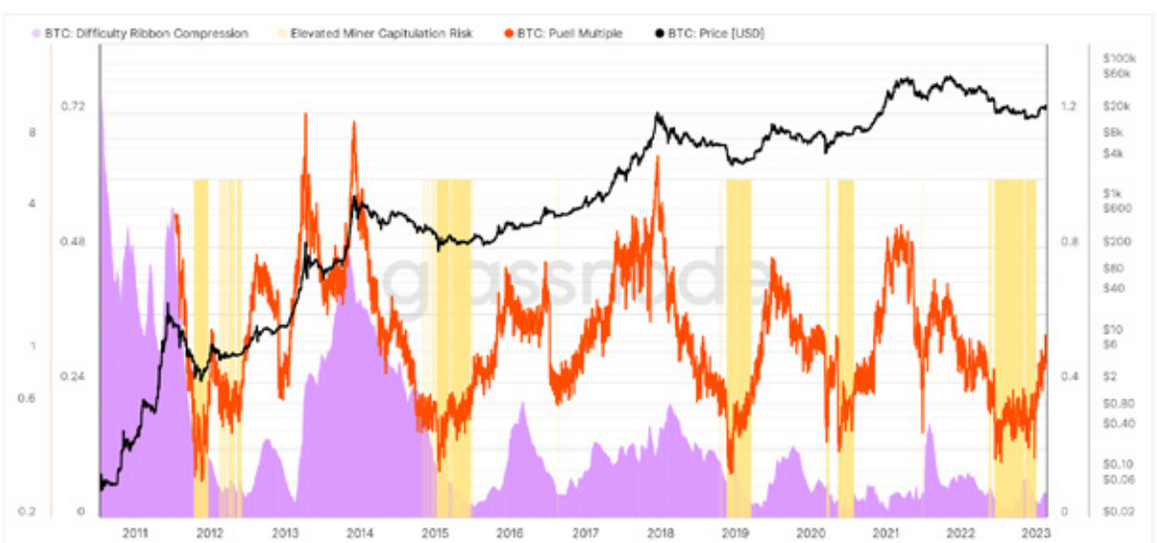
Bitcoin: Difficulty Ribbon

© 2023 Glassnode. All Rights Reserved.

alassnode

Entrando più nello specifico, possiamo utilizzare queste informazioni per un'analisi più approfondita. Combinando due indicatori, il primo riferito alla compressione del fascio di medie mobili qui sopra esaminata, e il secondo al ricavato medio dei miner, possiamo individuare i periodi corrispondenti ad un elevato rischio di capitolazione da parte dei miners.

Bitcoin: Miner Capitulation Risk



© 2023 Glassnode. All Rights Reserved.

glassnode

- **Difficulty Ribbon Compression**: è un indice normalizzato, che assume

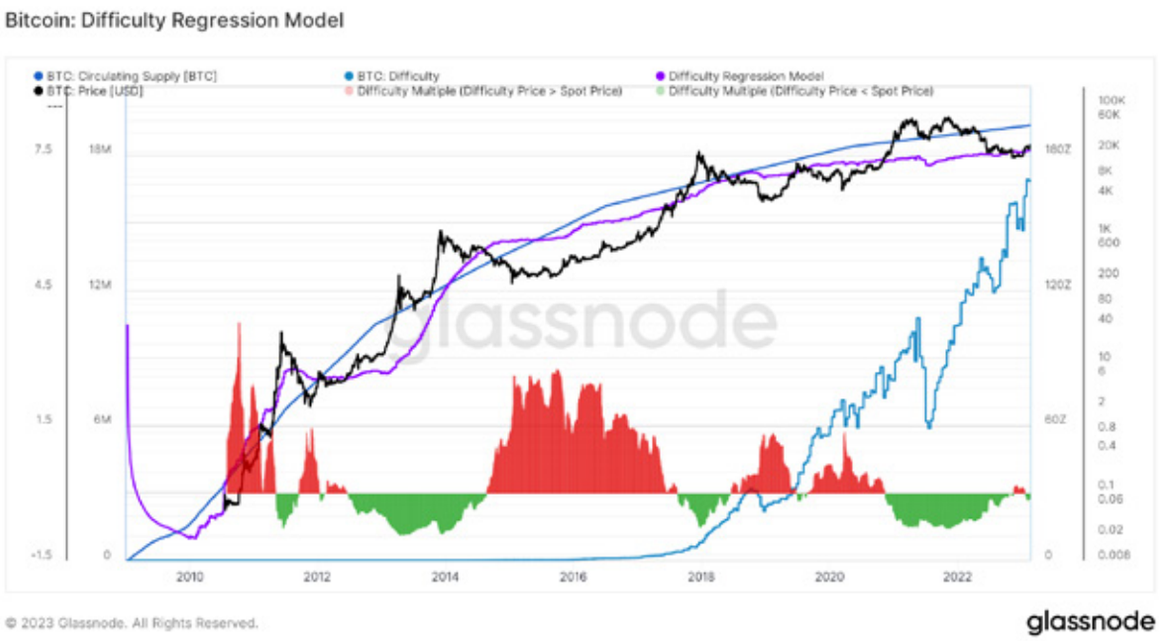
quindi valori compresi tra 0 e 1 e indica quanto sono più o meno compresse le medie mobili relative alla difficoltà di mining: valori prossimi a 0 corrispondono ad elevata compressione. Segnala quindi una diminuzione statisticamente significativa della difficoltà del network, ovvero quando le macchine dei miners vengono spente perché non più profittevoli.

- **Puell Multiple**: rappresenta il ricavato aggregato espresso in dollari dei minatori rispetto alla media annuale: valori inferiori a 1 indicano che i ricavi dei miners sono inferiori alla media annuale.

- **Elevated Miner Capitulation Risk**: le zone corrispondenti evidenziano periodi in cui entrambe le metriche assumono valori minimi e generalmente sono correlate a minimi dei prezzi di Bitcoin, durante i mercati ribassisti, quindi rappresentano un rischio elevato di capitolazione da parte dei miners. La soglia presa in considerazione in questo caso per determinare questi periodi è un valore minore a 0,65 della somma tra il Difficulty Ribbon Compression e il Puell Multiple.

Come abbiamo già visto in precedenza l'attività di mining ha un costo che è direttamente proporzionale alla difficoltà di mining: più la difficoltà è elevata, più sarà oneroso il mining di nuovi blocchi da parte dei miners. Possiamo quindi ottenere una metrica che tenga riferimento di questo, che corrisponda al prezzo medio di produzione (tenendo conto di tutte le variabili in gioco) dei bitcoin.

Confrontando questo valore con il prezzo di Bitcoin possiamo ottenere una stima di quanto sia profittevole il mining in determinati momenti.



- **Difficulty Regression Model**: rappresenta il costo medio di produzione di bitcoin da parte dei miners, al netto di tutte le spese, e viene calcolato come segue:

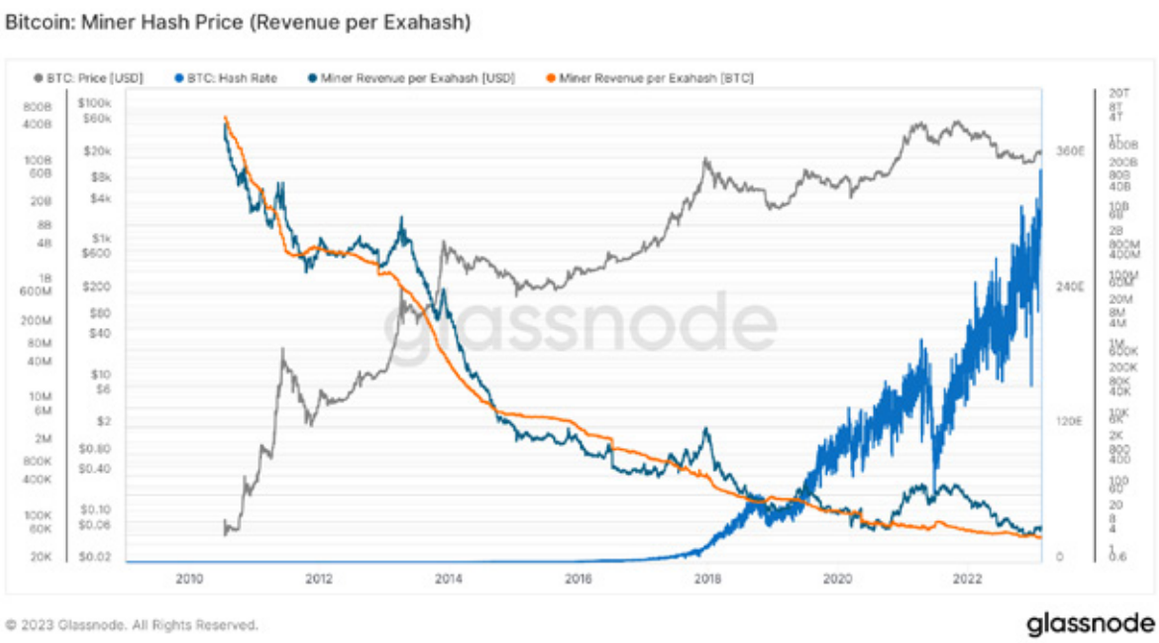
$$\text{Difficulty Regression Price} = \exp(A + B * \log(\text{Difficulty} / C)) / \text{Circulating Supply}$$

con A e B costanti di regressione, e C come fattore di correzione per la difficoltà
A=10,2560
B=0,5250
C=4.294.967.296

- **Difficulty Multiple**: si tratta di un semplice oscillatore che riporta la distanza tra il prezzo di Bitcoin e il Difficulty Regression Model.

Nei periodi in cui l'oscillatore è rosso i miners sono propensi a non vendere, a meno di non essere costretti per sopperire alle spese, come succede dei momenti di capitolazione. Nonostante tutto, però, l'hashrate del network è in costante crescita, indipendentemente dal prezzo di Bitcoin e questo ha un impatto sulla redditività per singola unità di hashpower che un miner genera

tramite le sue macchine. La concorrenza tra miners è in continuo aumento, serve avere una potenza computazionale sempre più grande a parità di bitcoin minati per stare al passo ed avere una farm redditizia. L'avanzamento tecnologico in ambito di ASIC[17] aiuta in tal senso, le macchine sono sempre più potenti e meno costose, ma sempre più players sono interessati all'attività di mining, a causa dell'aumento di interesse e possibili use-case nei confronti di Bitcoin. Il trend generale positivo del prezzo di Bitcoin rende sostenibile la crescita dell'hashrate.



Infatti come mostra il grafico qui sopra, il trend della redditività per ExaHash[18] è inversamente proporzionale alla crescita dell'hashrate del network.

Conclusione

[17] ASIC è l'acronimo di Application Specific Integrated Circuit, si tratta infatti di apparecchiature informatiche basate su circuiti integrati sviluppati per svolgere funzioni molto specifiche, in questo caso il mining di Bitcoin. Prima dell'avvento delle apparecchiature ASIC il mining veniva svolto dai semplici personal computer, tramite CPU o GPU. Una ASIC però è molto più ottimizzata, potente, ed efficiente in termini energetici rispetto alla CPU di un normale pc.

[18] Un ExaHash corrisponde a 10^{18} Hash, secondo il Sistema Internazionale di unità di misura, equivale a un miliardo di miliardi, 1'000'000'000'000'000'000.

Il mining di Bitcoin è colonna portante del protocollo: è necessario che questo sia il più distribuito possibile, e che mantenga un hashrate elevato, per garantire sicurezza e impedire, o comunque scoraggiare, possibili attacchi. Per far in modo che questo avvenga, serve un incentivo importante a questa attività, rappresentato dal profitto che se ne può ricavare, supportando il network in questo modo. Abbiamo constatato in precedenza che il mining è un attività redditizia sotto determinate condizioni, e continuerà a crescere finché queste condizioni verranno rispettate. Le condizioni necessarie affinché questo avvenga sono legate in primis ai costi di gestione, che comprendono il costo energetico, la spesa di infrastrutture e macchinari specifici (ASIC), alla ricompensa per blocco, ed al prezzo di Bitcoin. Di fatto, quindi, la crescita dell'attività di mining è sostenuta dal trend positivo del prezzo di Bitcoin. Ci sono situazioni, tuttavia, in cui il mining va ad influenzare la price action, come nei periodi di capitolazione dei miner, individuati graficamente sulla serie storica dal 2010 ad oggi. In questi momenti i miners, alle strette a causa del mercato sfavorevole, sono costretti ad immettere nel mercato grandi quantità di bitcoin minati in precedenza, per sopperire alle spese di gestione divenute insostenibili, o per ripagare i debiti contratti in precedenza: ricordiamo infatti che, a parte piccole realtà private, la maggior parte delle entità che si occupano di mining sono rappresentate da aziende, che devono registrare utili per poter rimanere in piedi. Tuttavia si tratta di brevi fasi, che terminano non appena si ritrova un nuovo equilibrio.

Il continuo dimezzarsi della ricompensa per blocco aiuta inoltre a regolare la sell pressure creata dal mining, portando ad ottenere scarsità, e quindi rendere il sistema sempre meno inflattivo, fino a che le ricompense dei miners saranno rappresentate dalle sole commissioni di rete. Questo potrebbe portare a un innalzamento di tali commissioni, perché ci si troverà in una situazione in cui si creerà concorrenza per poter ottenere lo spazio nel blocco per la propria transazione. Una soluzione a questo inconveniente è rappresentata ad oggi dai sistemi di layer 2, come Lightning Network, che viene

utilizzato per effettuare micropagamenti a commissioni praticamente nulle e istantanee, con un risparmio di transazioni onchain.
Tutto ciò ha la diretta conseguenza di un apprezzamento lento ma costante dei singoli bitcoin presenti in circolazione, caratteristica che può dare credito a Bitcoin sotto il punto di vista di strumento di Store of Value. L'attività di mining e quindi anche l'hashrate del network, può influire sul prezzo di Bitcoin, ma sul breve periodo, mentre sul lungo periodo è il prezzo che ha un'influenza sul mining.
I valori di hashrate raggiunti ad oggi sono sufficienti per garantire la sicurezza del protocollo: non esiste entità in grado di utilizzare abbastanza risorse per prendere il controllo del sistema di consenso, ma soprattutto il costo di tale operazione non porterebbe a nessun vantaggio economico.
Ecco perché Bitcoin offre una soluzione per il trasferimento di valore in maniera trustless e permissionless in qualsiasi momento e in qualsiasi luogo, senza il bisogno di possedere un conto bancario, ma soprattutto rappresenta un modo di custodia di valore incensurabile, in cui l'utente è a tutti gli effetti proprietario del saldo, e solo esso può gestirne l'utilizzo.
Se ci sarà una continua adozione, si arriverà ad ottenere stabilità anche nel prezzo, rendendo Bitcoin un possibile strumento di pagamento internazionale.

Bibliografia

[1] Schär, Berentsen, Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction; MIT Press, 2020

[2] Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain: Unlocking Digital Cryptocurrencies, 2017

[3] Back, Hashcash - A Denial of Service Counter-Measure, 2002

[4] Nakamoto, A Peer-to-Peer Electronic Cash System, 2008

[5] MIT lecture on Blockchain 2020

[6] Coinmarketcap.com

[7] Binance Academy

[8] Bit2Me Academy

[9] Glassnode

[10] Forbes

[11] Coindesk