Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea Magistrale in Informatica

Proof-Of-Work e Impatto Ambientale: Problemi e Potenziali Soluzioni

Relatore:
Chiar.mo Prof.
Ugo Dal Lago

Presentata da:
Francesca Grillo

Sessione III
Anno Accademico 2019/2020

Alla mia famiglia ...

Agli amici, ma quelli veri ...

... e soprattutto a me stessa, gli sforzi fatti a volte ripagano!

Introduzione

Il progresso tecnologico attuale sarebbe stato impensabile per gli individui che hanno vissuto nell'era in cui si utilizzava il baratto di merci o animali come mezzo di scambio. Nessuno in quegli anni avrebbe mai immaginato che il capitale di una persona si potesse portare in giro custodito in una semplice tessera elettronica o che, addirittura, si potessero fare acquisti comodamente da casa, sfruttando un computer o un telefono cellulare di ultima generazione, senza la necessità di dover comunicare direttamente con gli intermediari. Quello del pagamento elettronico è sicuramente un bel salto in avanti, ma non privo di rischi.

Pagamento elettronico vuol dire anche fidarsi del sistema, fidarsi del fatto che i dati personali non verranno divulgati o intercettati, fidarsi del fatto che la carta non venga clonata, fidarsi della controparte sperando che non cerchi di commettere una frode. Tutto ciò non sempre è garantito, purtroppo, ma col tempo sono anche migliorate le tecniche per prevenire problemi di questo genere. Esistono, tuttavia, gli scettici, come per ogni cosa, che preferiscono i metodi tradizionali, i pagamenti effettuati di persona. Questo non significa essere protetti dai rischi, si può lo stesso incorrere in truffe o in furti da parte di mal intenzionati. In ogni circostanza serve adottare le giuste misure di sicurezza nel modo migliore possibile.

In questa premessa si è parlato di fiducia verso le parti coinvolte, fiducia che non serve nel contesto delle criptovalute, ovvero, delle forme di pagamento note per essere *trustless* (letteralemente "senza fiducia"). La prima tra tutte è Bitcoin che ha portato, nel giro di poco tempo, innovazione nel mondo del mercato finanziario.

La sua innovazione è motivata, principalmente, dal fatto che non necessita di alcun ente amministrativo (es. le banche) e, soprattutto, non richiede l'uso dei dati personali degli utenti, garantendo così il perfetto anonimato. Si tratta di un sistema del tutto decentralizzato, in cui gli utenti hanno il pieno controllo delle loro finanze e la convalida delle transazioni avviene tramite dei meccanismi di consenso distribuito, che coinvolgono tutti i nodi della rete. Il sistema è stato pensato per essere sicuro e per rendere questo possibile si sfrutta la crittografia che garantisce l'integrità dei dati (ecco a cosa si deve il nome criptovaluta). Questo lo rende resistente, quasi completamente, ad ogni tipo di attacco ma, come già detto, in ogni circostanza si possono presentare delle problematiche.

Da quando è stato messo in produzione, nel lontano 2009, Bitcoin è diventato ben presto di dominio pubblico. Sempre più persone hanno iniziato ad utilizzarlo, chi per necessità chi per la curiosità di provare. Sta di fatto che l'uso sproporzionato di questo sistema ha cominciato a gravare in maniera preoccupante sull'ambiente. La motivazione è legata alle risorse energetiche e sistematiche di cui ha bisogno per poter funzionare.

Bitcoin utilizza un grande registro distribuito, noto come "*Blockchain*", per tener traccia di tutte le transazioni che circolano in rete. Una volta inserite al suo interno non possono più essere cancellate, a meno di casi straordinari, dunque, se si considera l'anno in cui è stato inventato, al momento la Blockchain contiene al suo interno un numero molto elevato di transazioni. Il problema, però, non è tanto il numero quanto il processo che c'è dietro alla loro convalida e alla conseguente registrazione. Tale attività si riferisce metaforicamente al processo di estrazione dell'oro nelle miniere, ed è per questo motivo che prende il nome di "*mining*" (in italiano "minare") e i nodi che se ne occupano sono noti come "*miner*" (in italiano "minatori).

Per poter aggiungere le transazioni alla Blockchain i miner devono fornire una prova di lavoro, nel gergo "*proof-of-work (PoW)*", la prova consiste nel risolvere complessi problemi crittografici, vale a dire calcolare delle funzioni hash (nel contesto definite "puzzle") e per fare ciò necessitano di un'elevata potenza di calcolo. Più i nodi diventano bravi nella risoluzione di questi puzzle e più la difficoltà viene aumentata.

Lo scopo di questo elaborato è quello di fornire un'analisi sull'impatto ambientale del PoW di Bitcoin, sui problemi di scalabilità che presenta e sulle soluzioni che sono state proposte nel corso degli anni per fronteggiare queste situazioni. Alla fine verrà fornito un riassunto di quella che è la situazione attuale e delle considerazioni personali sul possibile futuro di questa criptovaluta.

Nello specifico il resto di questa tesi è organizzato come segue:

- Il primo capitolo sarà un viaggio nella storia per illustrare il percorso che ha portato dall'uso del baratto allo sviluppo delle criptovalute;
- Il secondo capitolo si concentrerà sulla tecnologia Blockchain, sulle sue principali caratteristiche, in modo da capire come essa sia utile allo scopo di Bitcoin;
- Il terzo capitolo analizzerà il protocollo Bitcoin, dunque, le informazioni sulla sua architettura e sul suo processo di funzionamento, i possibili attacchi e le soluzioni adottate per fronteggiarli, i vantaggi e gli svantaggi. La parte finale del capitolo riguarderà il confronto con altre criptovalute nate in seguito;
- Il quarto capitolo sarà interamente dedicato all'analisi degli effetti del PoW sull'ambiente, con riferimenti alle ricerche che sono state condotte negli anni in merito a questo argomento e una lista delle possibili soluzioni proposte/adottate per migliorare la scalabilità di Bitcoin;
- Il quinto capitolo introdurrà il concetto di Proof of Useful Work (PoUW), ovvero una prova di lavoro utile, da sfruttare in alternativa alla classica PoW, per migliorare le prestazioni e ridurre lo spreco di risorse. Nello specifico, si parlerà di alcuni progetti che sono stati realizzati/teorizzati e che potrebbero essere fonte di ispirazione futura per gli ideatori di Bitcoin;
- Nel capitolo conclusivo, come già detto, verrà fatto un quadro generale della situazione con l'aggiunta di considerazioni personali sugli argomenti trattati.

Indice

Elenco delle figure

Capitolo 1

Dal Baratto alle Criptovalute

Il termine "*evoluzione*" può essere utilizzato in diversi contesti per identificare un processo di trasformazione graduale di una determinata realtà che attraverso cambiamenti successivi può portare al miglioramento o al peggioramento della stessa. Si consideri, ad esempio, l'evoluzione della specie umana, della medicina, dell'elettronica, della cultura, dell'industria e via dicendo.

Nel contesto di questo documento, per introdurre la nascita di Bitcoin come moneta elettronica, si fa riferimento all'evoluzione che c'è stata in ambito economico/monetario. Nello specifico, nelle prossime sezioni verrà inizialmente descritto il progresso evolutivo che ha portato dalle origini, con l'utilizzo del baratto come primo mezzo di scambio, al giorno d'oggi, con l'avvento delle criptovalute come alternativa alla moneta tradizionale.

In seguito, verranno forniti dei concetti teorici di crittografia, utili alla comprensione della struttura di Bitcoin e del suo funzionamento, basato sull'utilizzo di tecniche crittografiche che consentono di garantire la riservatezza dei dati ed impedire a terzi non autorizzati di accedere o alterare informazioni a proprio vantaggio o a danno di altri.

1.1 Le Origini della Moneta

Tra le citazioni più famose di Paul Anthony Samuelson[1], premio Nobel per l'economia nel 1970, si ricorda "*La moneta, in quanto moneta e non in quanto merce, è voluta non per il suo valore intrinseco, ma per le cose che consente di acquistare*". Questo per dire che una moneta è tutto ciò che si può utilizzare come mezzo di pagamento, a prescindere dal suo valore.

1.1.1 Baratto

In un tempo in cui le monete non esistevano le transazioni economiche avvenivano tramite il **baratto**, la forma più semplice e naturale di scambio di un bene o di una risorsa con un altro bene o un'altra risorsa.

L'idea alla base del baratto era che i soggetti coinvolti dovevano possedere dei beni diversi, in modo da ricavare vantaggi acquisendo il bene posseduto dalla controparte. Sì sta parlando, però, di una forma primitiva di commercio e come tale presentava delle limitazioni, tra le principali vi sono:

- **Numerosi atti di scambio:** non sempre si riusciva ad ottenere subito quanto desiderato. A volte poteva succedere che il venditore non avesse bisogno del bene che gli veniva proposto, quindi poteva decidere se rifiutare lo scambio oppure accettare lo stesso per poi scambiare nuovamente la merce con altre persone, al fine di ottenere il bene gradito. Questo riclico di beni poteva rendersi necessario più di una volta, ciò significa che il venditore riusciva ad arrivare al fine ultimo solo dopo una serie di scambi (baratto multiplo);

- **Valore dei beni non divisibile:** non c'era alcuna garanzia sulla qualità delle merci, quindi si poteva incorrere nello scambio di merci di qualità con altre di qualità inferiore. Ad esempio, il venditore che scambiava delle mele per delle pere non aveva modo di stabilire se fossero davvero dei prodotti di qualità;

[1] https://it.wikipedia.org/wiki/Paul_Samuelson

- **Deperibilità dei beni:** un contadino che produceva un bene aveva la necessità di scambiarlo prima che questo deperisse. In altri termini, trattandosi di generi alimentari si deve far fronte ad una data di scadenza, quindi non tutti i beni prodotti potevano essere conservati per troppo tempo;

- **Rallentamenti tra gli scambi:** un individuo che aveva la necessità di scambiare un bene per riceverne un altro, doveva trovare un individuo che avesse contemporaneamente come esigenza il bene che egli offriva. Questo comportava delle criticità che portavano spesso a situazioni di stallo, creando problematiche non indifferenti soprattutto in presenza di merce di natura deperibile.

Per far fronte a queste problematiche, sorge l'esigenza di avere a disposizione uno strumento che possa ottimizzare le transazioni mercantili e gli scambi. Tale strumento deve essere però accettato come termine di pagamento da tutti gli operatori economici presenti all'interno di una comunità. Nasce con questo scopo la moneta naturale, descritta nella prossima sezione.

1.1.2 Moneta Naturale

Per risolvere le difficoltà causate dall'utilizzo del baratto era necessario introdurre un bene di accettabilità diffusa che permettesse di stabilire il valore degli altri beni. La prima tipologia di pagamento adibita a questo scopo fu la cosiddetta **moneta naturale (o moneta-merce)**, considerata dagli studiosi come la **pre-moneta**. Sì definisce naturale perché la moneta era rappresentata da beni presenti in natura, diversi in base alle comunità, cioè ogni popolo forniva come pagamento la merce di cui disponeva in abbondanza (bestiame, sale, utensili, conghiglie, grano, spezie, ecc.).

All'utilizzo delle monete naturali si deve la nascita di alcune terminologie comunemente usate al giorno d'oggi. Nelle zone dove era diffusa la pastorizia si utilizzava il bestiame come mezzo di pagamento, da qui il termine *pecunia* che viene dal latino *pecus* e significa "**gregge**". Altri popoli disponevano in abbondanza di sale, ecco perché viene utilizzata la parola *salario* quando ci si riferisce allo stipendio.

Affinché un bene potesse fungere da moneta doveva presentare delle caratteristiche precise che risolvessero i limiti legati al baratto, nello specifico doveva fornire:

- **Conservazione nel tempo:** i beni non dovevano risultare deperibili, ovvero dovevano conservarsi nel tempo in modo da poter essere scambiati in tempi futuri desiderati ma incerti;
- **Larga diffusione e trasferibilità:** questo doveva essere garantito per generare un'ampia accettazione e incentivare gli scambi anche a grandi distanze;
- **Verificabilità:** una caratterista che consentisse di stabilire il valore del bene proposto e che riducesse le incertezze legate al pagamento;
- **Divisibilità:** un bene doveva essere frazionabile senza perdita di valore.

Questa moneta venne ben presto adottata da molti popoli, ma come per il baratto cominciò a presentare dei problemi, legati soprattutto alla divisibilità. Infatti, facendo riferimento allo scambio di animali non è possibile mantenere questa caratteristica senza perdita di valore. Ad esempio, due mezze pecore valgono chiaramente meno di una intera. Inoltre, in quanto esseri viventi gli animali sono soggetti a malattie e quindi non è possibile sempre garantire la conservazione nel tempo degli stessi. Per ovviare a questi inconvenienti si fece ricorso all'uso della moneta metallica, descritta di seguito.

1.1.3 Moneta Metallica

Quando gli uomini iniziarono a lavorare i metalli per farne utensili e armi si accorsero che rispetto al bestiame presentavano notevoli vantaggi: erano più facili da trasportare, si potevano ridurre in frammenti senza che perdessero valore; inoltre, erano inalterabili e non richiedevano manutenzione e, quindi, non si deterioravano in seguito ad un lungo immagazzinamento. Una volta scelto il materiale si cercò la forma che ne rendesse più comodo l'utilizzo. La forma più antica è quella dell'anello, successivamente vennero creati i lingotti a forma rettangolare. Entrambi andarono scomparendo verso la prima metà del VII secolo per lasciar spazio a piccoli pezzi di metallo prezioso di forma circolare. Così nacque la **moneta metallica**.

In principio si utilizzava come *moneta privata*, cioè una moneta sulla quale veniva apportato un particolare sigillo che ne garantiva il peso e la qualità della lega, essa veniva amministrata da alcuni mercanti dell'epoca che fungevano da banche. In quanto esercenti privati avevano il diritto di accettare o meno la garanzia rappresentata dal marchio e qualora lo ritenessero necessario, ad ogni pagamento, potevano ricorrere alla verifica del titolo o del peso. In seguito, venne utilizzata come *moneta pubblica* e in questo caso l'esercente diviene lo stato che si appropria del diritto di battere moneta, apponendo il proprio timbro su di essa, e vieta le emissioni da parte dei privati.

La moneta vera e propria compare in Asia Minore, attorno alla metà del VII secolo a.C., e la sua creazione è stata attribuita a Creso, re di Lidia, il quale, coniò l'**elettro**, una moneta fatta con una lega naturale di oro e di argento che si trovava nei fiumi della zona. La novità era che peso e titolo erano garantiti da un'autorità pubblica e questo ne facilitava l'uso nel commercio. Da lì a poco l'uso di coniare le monete si diffuse piano piano in tutto il mondo. L'impiego di monete metalliche d'oro o d'argento consentiva di regolare facilmente gli scambi internazionali perché i metalli preziosi venivano accettati ovunque. Infatti, chi riceveva come pagamento la moneta di un paese straniero poteva usarla nel proprio, se invece la moneta straniera non era accettata era possibile fondere il metallo prezioso e usarlo per coniare nuove monete.

Anche questa moneta, però, così come la moneta naturale presentava degli svantaggi. Nello specifico, si è scoperto che era difficile trasportarla in grandi quantità da un luogo all'altro e inoltre risultava a tratti rischioso, perché si poteva incorrere in rapine da parte dei briganti. Si introdusse l'uso della moneta cartacea, meglio descritta di seguito.

1.1.4 La Moneta Cartacea

La **moneta cartacea**, meglio nota con il nome di **banconota**, fu introdotta nel IX secolo d.C. dai Cinesi, mentre in Europa si diffuse solamente a partire dal XVII secolo.

Erano i banchieri a rilasciare, a coloro che depositavano monete metalliche e metalli preziosi, dei biglietti convertibili in oro. Chiunque fosse in possesso di tali biglietti poteva recarsi presso la banca emittente e chiedere l'equivalente in oro o in monete metalliche. Inoltre, per evitare falsificazioni le banconote vennero realizzate in carta filigrana, un materiale che consente la visione, in controluce, di particolari immagini o scritte. Questo nuovo sistema basato sulla moneta cartacea risultò molto più funzionale rispetto a quelli che lo hanno preceduto. In pratica l'oro e l'argento venivano custoditi nei forzieri delle banche e sostituiti con questi biglietti intercambiabili.

Fino ai primi anni del '900 le monete cartacee potevano essere convertite in oro presso gli istituti bancari. Questa possibilità oggi non esiste più quindi ci si riferisce alla moneta cartacea come **moneta fiduciaria**, in quanto la sua circolazione si fonda sulla fiducia dei cittadini nello Stato e nel valore che esso ha assegnato alla moneta. Nella prossima sezione verrà meglio descritto cosa si intende per *valore della moneta*.

1.1.5 Valore della Moneta

Sì è parlato, riferendosi al baratto, del non riuscire ad attribuire il giusto valore alla merce scambiata. Con l'avvento della moneta è stato possibile farlo, definendo così il potere di acquisto, cioè la quantità di beni che è possibile acquistare con essa. Quando si parla di valore della moneta ci si riferisce a:

- **Valore intrinseco:** da attribuire alla moneta coniata con metalli preziosi (oro o argento) poiché il valore intrinseco della moneta rappresenta il valore del metallo in essa contenuto. Volendo fare il paragone con la moneta cartacea, il valore intrinseco si può attribuire ad esempio ai costi dell'inchiostro e della stampa. In ogni caso è un valore molto basso che non assume più importanza, considerando anche che attualmente le monete vengono coniate con metalli non preziosi (bronzo o nichel);
- **Valore nominale:** ci si riferisce al valore impresso sulla moneta in forma numerica, che viene dunque attribuito ad essa. Tale valore viene stabilito dallo Stato;
- **Valore legale:** con questo termine si intende semplicemente che le monete devono essere accettate come pagamento per legge, questo valore è dunque indipendente dal materiale con cui è coniata la moneta.

In questo contesto è possibile incorrere nel problema della **svalutazione** della moneta, cioè nella perdita di valore. In passato, quando le monete venivano coniate con metalli preziosi, il valore nominale corrispondeva al valore del metallo prezioso contenuto. Se il metallo veniva sostituito con metallo comune o mischiato ad esso, allo scopo di emettere una maggiore quantità di denaro, la moneta veniva svalutata. A seguito della fusione era possibile confermare questo aspetto.

Su questo principio si basa la *Legge di Gresham*[2], teorizzata da un inglese mercante e banchiere nel XVI secolo, la quale afferma: "*La moneta cattiva scaccia quella buona*". Per non incorrere nel problema della svalutazione, che rende più costose le merci importate e può avere conseguenze sull'inflazione (aumento dei prezzi di beni e servizi) del paese, in alcune civiltà veniva utilizzato solo uno dei due metalli preziosi per coniare le monete. Ad esempio: in Cina, India, Russia, Persia si usavano solo monete d'argento, nel Mediterraneo prevalse l'oro, mentre il rame si usava per le monete di minor valore.

La ragione per la quale queste monete vengono accettate in pagamento risiede nella **fiducia** di chi le riceve che altri faranno altrettanto, accettando in pagamento monete, banconote, depositi bancari o titoli di stato. Senza tale fiducia difficilmente una moneta sarebbe accettata in pagamento. Ad esempio, l'oro era accettato ovunque perché tutti ritenevano che altri avrebbero accettato di essere pagati in oro. La stessa caratteristica è oggi posseduta dal dollaro e da altre monete.

Nel tempo si affermarono le tre funzioni principali della moneta:

1. **Mezzo di scambio:** agevola lo scambio di beni e servizi superando gli ostacoli riscontrati nell'uso del baratto, in quanto ogni cosa viene misurata ed acquisisce un prezzo;

2. **Mezzo di pagamento:** permette di estinguere ogni tipo di debito, di natura finanziaria o legato allo scambio di beni;

3. **Riserva di valore:** in quanto non deperibile può essere conservata nel tempo e riutilizzata in futuro senza che perda di valore.

[2]https://it.wikipedia.org/wiki/Legge_di_Gresham

Dopo questo breve excursus utile per conoscere la storia legata alla nascita della moneta e per comprendere alcuni concetti di base, nella prossima sezione verranno descritti, più nel dettaglio, i sistemi monetari che si sono susseguiti negli anni.

1.2 I Sistemi Monetari

Per sistema monetario si intende l'insieme delle monete che circolano in un dato paese e delle norme che ne regolano la circolazione. Si dividono in 3 categorie:

- **Metallici:** sono caratterizzati dalla circolazione di monete metalliche e a loro volta si suddividono in 2 macro-categorie: i sistemi *mono-metallici* e i sistemi *bimetallici*. Come si può facilmente intuire il termine mono-metallico identifica le monete coniate con un solo metallo. Al contrario, nel sistema bimetallico circolano sia monete coniate in oro sia in argento. In entrambi i sistemi vi è piena libertà di *coniazione* e *fusione*. Ovvero, il cittadino è libero di portare alla Zecca[3] dello Stato del metallo e chiedere di coniare nuove monete o, viceversa, può portare delle monete e chiedere di fonderle per ottenere del metallo;

- **A cambio aureo:** consente l'immediata convertibilità di ogni banconota nel suo corrispettivo in oro e viceversa. Nel Paese in cui è in vigore tale sistema la banca centrale si impegna a convertire in oro qualunque ammontare di valuta nazionale (conversione totale), o ne ammette la conversione solo in modo ridotto (conversione parziale) poiché la banca centrale emette una quantità di monete il cui valore in oro è multiplo rispetto al valore dell'oro da essa custodito;

- **Con moneta cartacea inconvertibile:** il questo sistema la moneta non può essere cambiata in oro poiché mancano le necessarie riserve auree. Ciò avviene in tutti i paesi, dopo la prima guerra mondiale, quando lo Stato si trova a dovere effettuare pagamenti superiori alle sue possibilità perciò viene impedito il cambio dei biglietti in oro. Ciò significa che la moneta cartacea non può più essere convertita in oro, ma il cittadino è obbligato ad accettarla in cambio di beni e servizi. Questo è ciò che accade al giorno d'oggi.

[3] https://it.wikipedia.org/wiki/Zecca_(moneta)

Con l'avvento del sistema aureo e della cartamoneta convertibile si assicurò una certa stabilità nei cambi e l'equilibrio nel sistema internazionale dei pagamenti.
Nelle prossime sezioni verranno meglio descritte le fasi che hanno portato dal regime aureo internazionale all'età contemporanea.

1.2.1 Gold Standard

Il sistema monometallico a base aurea è detto **Gold Standard**. La prima nazione ad adottarlo fu la Gran Bretagna. A partire dal 1815 conservò uno standard bimetallico (oro e argento), ma le monete d'oro, le famose "ghinee" che portavano il nome della regione africana da cui proveniva il metallo (Guinea), rimpiazzarono largamente quelle d'argento nell'uso. Durante le guerre napoleoniche, la Banca d'Inghilterra, con l'autorizzazione del governo si rifiutò di pagare oro e argento in cambio delle proprie banconote, dunque, il paese rimase sprovvisto di uno standard monetario. Dopo le guerre il governo decise di ritornare ad uno standard metallico, ma scelse l'oro invece dell'argento. Secondo la legge relativa a questo standard bisognava osservate tre condizioni:

1. La Zecca reale era obbligata a comprare e a vendere quantità illimitate di oro a prezzo fisso;

2. La Banca d'Inghilterra, e per estensione tutte le banche, era tenuta a convertire a richiesta banconote e depositi in oro;

3. Non si potevano imporre restrizioni sull'importazione o sull'esportazione di oro.

Ciò significava che l'oro serviva da bene ultimo o riserva dell'intera provvista monetaria della nazione. Di conseguenza il movimento di entrata e uscita dell'oro dal paese impattava direttamente sui prezzi delle monete. Per i primi tempi la maggior parte degli altri paesi cercò di adottare un regime argenteo o bimetallico; alcuni paesi non ebbero alcun regime metallico. Tuttavia, a causa della posizione di politica, economica e finanziaria della Gran Bretagna, quasi tutti i paesi alla fine aderirono al Gold Standard. L'inizio della prima guerra mondiale segnò la fine del sistema aureo, poiché c'era la necessità da parte dei governi di sostenere e finanziare le spese belliche senza acquistare oro, ma emettendo moneta di cui non era più garantita la conversione in oro.

Al termine del conflitto non si riuscì a ricreare la situazione dell'anteguerra, sia perché questo aveva sconvolto lo scenario internazionale (bloccando i flussi commerciali e finanziari), sia perché molte nazioni trovarono difficoltà a garantire una diretta corrispondenza tra la quantità di oro detenuta e la quantità di banconote in circolazione. Per questi motivi tale sistema monetario fu abbandonato e sostituito dal Gold Exchange Standard, meglio descritto nella prossima sezione.

1.2.2 Gold Exchange Standard

La crisi del 1929 e la successiva grande depressione degli anni '30 sancirono la fine del Gold Standard. Dopo la seconda guerra mondiale, a seguito degli accordi di Bretton Woods[4], animati dall'esigenza di definire un sistema di regole e procedure per controllare la politica monetaria internazionale, nel 1944, questo sistema venne sostituito dal **Gold Exchange Standard**, basato sulla conversione della valuta cartacea nazionale non più in oro ma in una valuta straniera (il dollaro), a sua volta convertibile in oro.

Durante la conferenza di Bretton Woods venne sancito il passaggio di consegne dalla Gran Bretagna agli Stati Uniti. Lo scopo degli accordi era soprattutto quello di favorire la ripresa dell'Europa sopraffatta e provata dalla guerra. Con questo obiettivo si decise di creare un sistema basato su due istituzioni fondamentali: il Fondo Monetario Internazionale e la Banca Internazionale per la Ricostruzione e lo Sviluppo (BIRS). Queste istituzioni avevano lo scopo di incoraggiare la cooperazione monetaria tra gli stati e di incentivare il commercio internazionale attraverso la stabilità dei cambi, cioè lo scopo era quello di ottenere una parità fissa tra le valute dei vari paesi. Fu stabilito che fosse il dollaro la moneta ad essere legata come riferimento all'oro, e fu questa valuta a diventare la base diretta per ogni operazione. Venne fissato il prezzo dell'oro a 35 dollari all'oncia, prezzo a cui gli USA si impegnarono ad acquistarlo da chiunque e a venderlo solo alle banche centrali. Ogni Paese partecipante fu obbligato ad adottare il dollaro americano come valuta di riserva e consentire la convertibilità della propria moneta esclusivamente in valuta di riserva alla parità determinata dai contenuti aurei.

[4] https://it.wikipedia.org/wiki/Accordi_di_Bretton_Woods

Il nuovo sistema monetario funzionò fino alla prima metà degli anni '60, quando i paesi che partecipavano all'accordo cominciarono a presentare livelli di inflazione molto diversi. Infatti, i prezzi statunitensi salivano determinando una perdita di competitività, mentre paesi come il Giappone e la Germania registravano un attivo dei loro scambi con l'estero accumulando dollari. Questo portò ad una profonda sfiducia nel dollaro e molte banche centrali cominciarono a convertire i dollari in loro possesso in oro. Di fronte a questa situazione, nell'agosto del 1971, l'allora presidente USA, Richard Nixon, dichiarò l'inconvertibilità del dollaro in oro, decretando ufficialmente la fine del sistema a cambi fissi, per dare spazio ad un sistema con cambi flessibili, descritto nella sezione successiva.

1.2.3 Sistema a Cambi Flessibili

Dopo l'abbandono del Gold Exchange Standard, nel 1971, si passò ad un **sistema di cambi flessibili**, un regime in cui i tassi di cambio possono variare e sono determinati dalle forze della domanda e dell'offerta del mercato. Non vi è alcun intervento ufficiale nel mercato dei cambi. La banca centrale consente al tasso di cambio di adeguarsi in modo da equiparare l'offerta e la domanda di valuta estera. Ciò non vuol dire che non effettui degli interventi per ritoccare la flessibilità del cambio (**fluttuazione sporca**).

I **vantaggi** di questo sistema sono:

- Il deficit o l'eccedenza viene automaticamente corretto, tramite la svalutazione;
- Non è necessario che il governo detenga alcuna riserva di cambio;
- Aiuta a ottimizzare l'allocazione delle risorse.

Gli **svantaggi** di questo sistema sono:

- Incoraggia la speculazione che porta a fluttuazioni del tasso di cambio;
- L'ampia fluttuazione del tasso di cambio ostacola il commercio estero e il movimento di capitali tra Paesi;
- Genera pressione inflazionistica quando i prezzi delle importazioni aumentano a causa del deprezzamento della valuta.

L'introduzione del sistema a cambi flessibili non riscosse grandi consensi in Europa, poiché molti paesi desideravano maggiore sicurezza contro possibili svalutazioni attuate dai paesi a forte inflazione. Nacque così il sistema monetario europeo, descritto nella prossima sezione.

1.2.4 Sistema Monetario Europeo (SME)

Creato nel 1978 ed entrato in vigore nel marzo del 1979, il **Sistema Monetario Europeo (SME)**[5], è stato un accordo monetario europeo nato per il mantenimento di una parità di cambio prefissata tra le monete dei Paesi membri della CEE[6] (Comunità Economica Europea). Comprendeva tutte le valute degli Stati membri, ad eccezione in un primo tempo della sterlina britannica che aveva scelto di rimanere fuori dal sistema, il SME era fondato sul concetto di tassi di cambio stabili e soggetti a revisione. Il suo aspetto più innovativo fu l'introduzione dell'ECU[7] (European Currency Unit o unità di conto europea): un paniere di monete, che fluttuavano entro il 2,25% (6% per la lira, a causa dell'elevato tasso di inflazione). I governi avevano dunque il compito di controllare che le valute rientrassero in questo intervallo e di intervenire in caso contrario, al fine di ristabilire l'equilibrio.

Tra il 1992 e il 1993 ci furono delle turbolenze che portarono il SME ad attraversare un periodo di profonda crisi, gli episodi di rilievo furono i seguenti:

- Il ritiro della lira e della sterlina britannica dal SME, questo perché l'Italia e la Gran Bretagna non furono più in grado di mantenere le rispettive monete entro i limiti di oscillazione previsti; solo nel novembre del 1996 la lira poté rientrare;
- L'ampliamento della banda di oscillazione al 15% avvenuto nell'agosto del 1993, per evitare che altre monete dovessero abbandonare il meccanismo.

Il SME cessò di esistere il 31 dicembre 1998 con la nascita dell'Unione economica e monetaria, meglio descritta nella prossima sezione.

[5] https://it.wikipedia.org/wiki/Sistema_monetario_europeo
[6] https://it.wikipedia.org/wiki/Comunità_economica_europea
[7] https://it.wikipedia.org/wiki/Unità_di_conto_europea

1.2.5 L'Unione Economica e Monetaria (UEM)

A partire dal 1986 si susseguirono una serie di iniziative dirette in un'unica direzione: la realizzazione dell'Unione Europa. Con l'Atto Unico Europeo[8] (Single European Act), predisposto in quell'anno, si confermò dunque la volontà di unione, che era stata già ribadita in diversi referendum nazionali condotti nei singoli paesi. Successivamente nel 1989, il *Rapporto Delors*, che prende il nome dall'allora Presidente della Commissione, rappresentò il vero punto di svolta nel processo di integrazione economica e monetaria.

La prima tappa verso questo processo di integrazione fu quella prevista dal Rapporto e realizzata nel 1990, la quale prevedeva la libera circolazione dei capitali. Nel 1991, invece, con lo storico **trattato di Maastricht**[9] (Trattato sull'Unione Europea) si stabilirono i criteri di convergenza cui dovevano uniformarsi i paesi che volevano prendere parte all'unione monetaria. Nello specifico gli accordi riguardavano:

- La stabilità dei prezzi, con un'inflazione intorno al 2%;
- La crescita sostenibile;
- Il rispetto dell'ambiente.

Nel 1993 il Mercato Unico divenne una realtà, vennero eliminate tutte le barriere non tariffarie ancora vigenti e venne liberalizzato il movimento delle merci, dei capitali e delle persone. Inoltre, particolari accordi predisponevano la creazione della **Banca Centrale Europea (BCE)** che avrebbe avuto il compito di gestire la nuova moneta (l'**Euro**), mantenere i prezzi stabili e guidare la politica economica e monetaria dell'UE. L'introduzione della nuova moneta ebbe inizio nel gennaio del 1999 e si concluse nel gennaio del 2002, quando iniziò materialmente l'emissione di monete in Euro, che per alcuni mesi circolarono contemporaneamente insieme alle valute nazionali. Il primo marzo 2002 l'Euro diverrà l'unica moneta in circolazione.

Nelle prossime sezioni verranno descritte quelle che si possono definire *monete alternative*, le quali caratterizzato l'attuale sistema monetario.

[8] https://it.wikipedia.org/wiki/Atto_unico_europeo
[9] https://it.wikipedia.org/wiki/Trattato_di_Maastricht

1.3 Le Monete Alternative

Come ampiamente descritto nelle sezioni precedenti, ciò che caratterizza il sistema monetario odierno è l'uso della moneta tradizionale (banconote o monete metalliche). Negli anni quest'ultima è stata definita moneta legale, in quanto per legge deve essere accettata come metodo di pagamento. Nell'era moderna si sono sviluppati dei mezzi di pagamento alternativi: la moneta bancaria e la moneta elettronica. Queste non hanno però corso legale poiché il pagamento elettronico o bancario può essere rifiutato, qualora il debitore non avesse a disposizione la somma richiesta.

Un'altra alternativa riguarda le criptovalute (o valute virtuali) da non confondere con le precedenti. Infatti, in questo caso manca la presenza di un terzo soggetto (es. la Banca), oltre al pagatore ed al beneficiario del pagamento, che funga da intermediario nella transazione; dunque, il trasferimento del denaro avviene in maniera diretta tra le parti. Maggiori dettagli in merito a queste tipologie di pagamento verranno forniti nelle prossime sezioni.

1.3.1 Le Monete Bancarie

Le **monete bancarie**, come suggerisce il nome stesso, fanno riferimento a tutti i mezzi di pagamento che dipendono dalle banche. Come ad esempio:

- L'**assegno bancario**: è un titolo di credito mediante il quale, il soggetto che ha un deposito presso una banca, ordina alla banca stessa di pagare una certa somma di denaro a favore della persona indicata sull'assegno. Mediante la **girata**[10] l'assegno può circolare, in modo che il beneficiario indicato sullo stesso possa consegnare quest'ultimo ad altri, i quali avranno il diritto di ricevere dalla banca tale somma;

- Le **carte di credito**: sono delle tessere di plastica rigida, dotate di una banda magnetica di riconoscimento. Esse vengono emesse da società specializzate che si impegnano a garantire il pagamento degli importi che vengono addebitati sul conto del cliente a date fisse, in un'unica soluzione o a rate;

[10] https://it.wikipedia.org/wiki/Girata

- Le **carte prepagate**: vengono rilasciate direttamente dalle banche e possono essere di due tipologie:

  1. **Usa e getta**: sono rilasciate per un dato importo e sono valide fino ad esaurimento di tale somma;
  2. **Ricaricabili**: al contrario delle precedenti, quando l'importo disponibile si è esaurito consentono la ricarica e il conseguente riutilizzo della carta.

Le carte di credito e le carte prepagate sono anche considerate monete elettroniche, ma questa tipologia di moneta verrà descritta nella prossima sezione.

1.3.2 Le Monete Elettroniche

La **moneta elettronica** per essere considerata tale deve possedere un valore monetario che soddisfi una serie di requisiti. Ovvero, il valore deve:

- Essere memorizzato elettronicamente;
- Rappresentare un credito verso l'emittente, ad esempio una Banca o IMEL (Istituto di Moneta Elettronica);
- Esser emesso per consentire operazioni di pagamento (versamento, trasferimento o prelievo di fondi);
- Essere accettato quale mezzo di pagamento da persone diverse dall'emittente.

Esistono 3 principali tipologie di monete elettroniche:

1. **Card-based**: il valore monetario viene immagazzinato nel microchip che si trova sulla carta;
2. **Software-based**: la liquidità dell'acquirente è memorizzata in locale su di un file. Tramite il POS virtuale, fruibile online, viene stabilito un collegamento con il computer dell'utilizzatore, sul quale è stato memorizzato tale file;
3. **Computer-based o Network-based**: un esempio è il noto sistema PayPal, nel quale l'utente si registra ed apre un conto precaricato, dal quale viene prelevato l'ammontare della transazione.

Ciò che accomuna i sistemi di pagamento elettronici riguarda l'uso di strumenti diversi dal contante. Tra i principali sistemi, attualmente in circolazione, ci sono le carte di credito (Mastercard, Visa e American Express), le carte di debito (esempio PagoBancomat, un circuito nato in Italia), le carte prepagate e le carte a spendibilità limitata (di recente emissione).

Ci sono vari vantaggi nell'utilizzo di questo metodo di pagamento, come ad esempio: la riduzione del costo del contante e la tracciabilità delle transazioni, con riflessi positivi alla lotta contro il riciclaggio e l'evasione fiscale, anche se, riguardo quest'ultimo punto la garanzia non è totale. Le monete elettroniche si definiscono anche **valute digitali**, da non confondere con le criptovalute (o valute virtuali) descritte nella prossima sezione.

1.4 Le Criptovalute

Le **criptovalute** (o *valute virtuali*) sono delle monete virtuali il cui funzionamento si basa su una complessa rete di calcoli crittografici che ne garantiscono la sicurezza. La più nota criptovaluta esistente è **Bitcoin**, di cui si parlerà ampiamente nei prossimi capitoli. In questa sezione, invece, ci si soffermerà principalmente sulle caratteristiche principali di una criptovaluta per capire in che modo essa si differenzia dalla moneta elettronica.

Partendo dal nome, si può notare che è composto da due parole: "*cripto*" (dal greco kryptós = nascosto) e "*valuta*". Volendo quindi fornire una definizione più semplice la criptovaluta si può considerare come una "*valuta nascosta*" che si rende visibile/utilizzabile solo conoscendo una determinata chiave di accesso. Il termine "*virtuale*", invece, indica che non esiste in forma fisica ma si genera e si scambia per acquistare beni e servizi, previo consenso tra i partecipanti alla transazione, esclusivamente per via telematica in modalità *peer-to-peer*[11] (ovvero tra due dispositivi direttamente, senza necessità di intermediari). Non è pertanto possibile trovare in circolazione dei Bitcoin in formato cartaceo o metallico. Trattandosi di una valuta virtuale non ha valore legale.

[11] https://it.wikipedia.org/wiki/Peer-to-peer

Si distinguono 3 tipologie di moneta virtuale: chiusa, unidirezionale e bidirezionale. Si riporta uno schema in Figura 1.1.

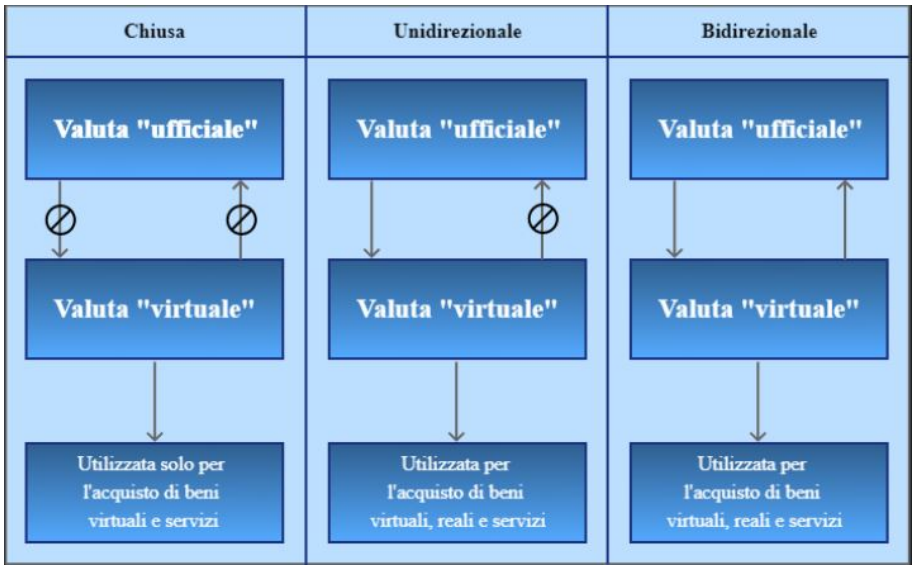

Figura 1.1: Le tre tipologie di moneta virtuale

Nel 2012, la BCE pubblica una relazione in cui spiega ampiamente le caratteristiche di questi 3 modelli, le quali verranno riassunte di seguito.

- **Moneta virtuale chiusa**: non esiste un collegamento tra la moneta digitale e l'economia reale. Ne sono un esempio le valute dei giochi online: i giocatori pagano e ottengono in cambio moneta che potrà essere utilizzata unicamente all'interno del gioco stesso;

- **Moneta virtuale unidirezionale**: la moneta virtuale può essere comprata con denaro reale, ad un certo tasso di cambio, ma non può essere scambiata di nuovo in valuta reale. Un esempio sono stati i famosi *Facebook Credits*[12]: quest'ultimi permettevano al suo proprietario di comprare beni e servizi offerti dalla comunità;

- **Moneta virtuale bidirezionale**: le criptovalute possono essere facilmente scambiate con la moneta reale e viceversa.

[12]https://en.wikipedia.org/wiki/Facebook_Credits

La differenza sostanziale, dunque, risiede nella possibilità o meno di poter scambiare la criptovaluta con una moneta a corso legale e nella tipologia di beni/servizi acquistabili. Il Bitcoin, ad esempio, è una moneta virtuale bidirezionale in quanto può essere facilmente convertita con le principali valute ufficiali e viceversa.

Le criptovalute hanno caratteristiche peculiari che le contraddistinguono e differenziano dalle monete digitali. Di seguito se ne riporta un elenco:

- Un insieme di regole (detto "**protocollo**") che stabilisce le modalità per cui i partecipanti possono effettuare le transazioni;
- Una sorta di "libro mastro" meglio noto come **blockchain** (o distributed ledger) la cui struttura, organizzata a blocchi, permette di costruire un'architettura condivisa e immutabile su cui sussistono le varie transazioni;
- Una **rete decentralizzata** di **miners** che aggiornano, conservano e consultano la blockchain delle transazioni, secondo le regole del protocollo;
- I programmi su cui si sviluppano sono completamente **open-source**, ossia modificabili e ri-programmabili.

Tali caratteristiche rendono le criptovalute di difficile inquadramento sistematico-giuridico, favorendone l'elevata esposizione allo scetticismo e alla sfiducia da parte delle istituzioni. Nel prossimo capitolo verrà descritta nel dettaglio la tecnologia Blockchain che è l'organo portante di tutti i sistemi basati sulle criptovalute, ma nello specifico si farà riferimento al suo utilizzo nel contesto Bitcoin.

Capitolo 2

Blockchain

La **blockchain** è una raccolta digitale condivisa di dati all'interno della quale viene registrata cronologicamente ogni unità di criptovaluta. Inoltre, consente il tracciamento dei vari trasferimenti da un utente all'altro. Le transazioni vengono mantenute all'interno di "*blocchi*" di dati e ogni nuovo blocco viene inserito all'inizio della catena di dati. Esistono tre diverse categorie di Blockchain e identificarle correttamente è molto importante, per comprendere quale sia la più adatta a ogni ambito di applicazione.

1. **Blockchain Pubblica:** viene definita così perché è completamente priva di autorizzazioni e restrizioni. Gli utenti che ne fanno parte non hanno privilegi sugli altri e i dati memorizzati su di essa non possono essere modificati o eliminati. In sostanza, nessuno può alterare il protocollo che ne determina il funzionamento. Bitcoin fa parte di questa categoria. Questo tipo di tecnologia soffre di una limitazione, **non è scalabile**, ovvero non ha la capacità di migliorarsi all'aumentare del numero di partecipanti. Al crescere della quantità di nodi, la velocità delle transazioni rimane invariata ma aumenta la stabilità del sistema che diventa così più sicuro;

2. **Blockchain Autorizzata:** è comunque una blockchain pubblica ma è soggetta ad un'autorità centrale che determina chi può accedervi e quali sono i ruoli che un utente può ricoprire all'interno della stessa, definendo anche regole sulla visibilità dei dati registrati. Viene, dunque, introdotto il concetto di governance e centralizzazione in una rete che nasce con lo scopo di essere del tutto decentralizzata e distribuita.

Per le sue caratteristiche viene ritenuta dalle istituzioni più sicura rispetto a quella pubblica, poiché permette di avere il livello di segretezza richiesto, controllando chi può accedervi e chi può visualizzare i dati. Inoltre, è considerata più performante, scalabile e meno costosa, merito delle piccole dimensioni e del fatto che le transazioni vengano verificate da un limitato numero di utenti. Una blockchain di questo tipo non è necessariamente anche privata;

3. **Blockchain Privata:** condivide molte caratteristiche con quella autorizzata. Si tratta di una rete privata e, in quanto tale, non visibile quindi per accedervi bisogna essere invitati e autorizzati. Chiaramente questo garantisce un maggiore livello di privacy agli utenti e determina la segretezza dei dati. Viene controllata da un'organizzazione, ritenuta attendibile dagli utenti, che determina chi possa accedere o meno alla rete e alla lettura dei dati in essa registrati. L'organizzazione proprietaria della rete inoltre, ha il potere di modificare le regole di funzionamento della blockchain stessa, rifiutando ad esempio delle transazioni. Anche questa è considerata più veloce, economica, sicura e scalabile rispetto alle blockchain pubbliche.

Per garantire la sicurezza dei dati le blockchain fanno affidamento a dei sistemi di protezione che i file dei computer tradizionali non hanno, vale a dire sfruttano alcune note tecniche crittografiche, quali: funzioni e puntatori hash, firma digitale a crittografia asimmetrica. Una descrizione più precisa verrà fornita nelle prossime sezioni.

2.1 Funzioni Hash

Una **funzione hash**, se considerata all'interno di un contesto matematico, presenta le seguenti tre proprietà:

1. Il suo input può essere qualsiasi stringa di qualsiasi dimensione;

2. Il suo output ha dimensioni prefissate (relativamente piccole) e di norma viene definito *hash* o *message digest*, letteralmente riassunto del messaggio, proprio perché da un input di lunghezza variabile si ottiene una versione sintetica che rappresenta lo stesso contenuto;

3. È calcolabile in modo efficiente. Intuitivamente significa che data una stringa di input si può ottenere l'output della funzione hash in un ragionevole lasso di tempo. In linea teorica il calcolo dell'hash di una stringa di n bit dovrebbe avere un tempo di esecuzione pari a $O(n)$.

In questo contesto è necessario andare più nello specifico e riferirsi alle **funzioni hash crittografiche**. Affinché una funzione hash sia crittograficamente sicura deve soddisfare ulteriori tre proprietà:

1. **Resistenza alle collisioni**
   Si verifica una collisione quando due input distinti producono lo stesso output. Dunque, una funzione hash è resistente alle collisioni se nessuno riesce a trovare una collisione. Formalmente: una funzione hash H si dice *resistente alle collisioni* se non è possibile trovare due valori, x ed y, tali che

   $$x \neq y, \text{ ma } H(x) = H(y).$$

   Da notare che la premessa è che nessuno riesca a trovare una collisione ma ciò non vuol dire che non ne esistano. Chiaramente le collisioni esistono, basti pensare che lo spazio di input per la funzione hash contiene tutte le stringhe di tutte le lunghezze ma lo spazio di output contiene solo stringhe di una lunghezza fissa specifica. Dal momento che lo spazio di input (potenzialmente infinito) è maggiore dello spazio di output devono essere presenti stringhe di input che mappano la stessa stringa di output. Ad oggi trovare delle collisioni richiede ancora moltissimo tempo, quindi semplicemente ci si fida del fatto che le funzioni hash siano **collision free** ovvero resistenti alle collisioni.

2. **Resistenza alla preimmagine (o Hiding)**
   La proprietà hiding afferma che dato l'output della funzione hash $y = H(x)$, non esiste un modo per capire quale sia l'input, x. Il problema è che questa proprietà non può essere vera in questa forma. Si consideri il seguente esperimento come dimostrazione: viene lanciata una moneta, se il risultato del lancio è testa, viene annunciato l'hash della stringa "testa", altrimenti, l'hash della stringa "croce".

Si chiede, dunque, ad un avversario, che non ha visto il lancio della moneta ma conosce solo l'output, di provare ad indovinare la stringa corrispondente all'hash generato. Farlo risulta molto semplice, perché basta calcolare l'hash di entrambe le stringhe per trovare una corrispondenza, quindi poiché esistono soltanto due valori di x, in un paio di passaggi, l'avversario sarà in grado di risalire all'input della funzione hash. Per poter ottenere la proprietà nascosta, è necessario che non vi sia alcun valore di x che è particolarmente probabile. Cioè, x deve essere scelto da un insieme che è, in un certo senso, molto esteso. Così facendo, questo metodo non funzionerà. Fortunatamente, però, anche per questa particolare casistica esiste un modo per nascondere i valori di x. Basta concatenare quest'ultimo input non distribuito con un altro input distribuito. Viene fornita una definizione più precisa:

Una funzione hash H si dice **Hiding** quando un valore segreto r viene scelto da una distribuzione di probabilità che ha un'entropia minima (**min-entropy**) elevata, quindi dato $H(r\|x)$[1] non è possibile trovare x.

Nella teoria dell'informazione, l'entropia minima è una misura di quanto sia prevedibile un risultato. Quindi, per un esempio concreto, se r è scelto uniformemente tra tutte le stringhe lunghe 256 bit, allora una stringa particolare è stata scelta con probabilità $1/2^{256}$ che è un valore infinitamente piccolo. Le funzioni hash con questa proprietà sono componenti essenziali dei cosiddetti **commitment schemes**[2].

Uno schema di impegno è una primitiva crittografica che consente di "impegnarsi" in un valore scelto mantenendolo nascosto agli altri, con la possibilità di rivelarlo in un secondo momento. Questi schemi sono vincolanti, poiché sono progettati in modo tale che il valore scelto non possa essere modificato una volta impegnato. Per capire facilmente il funzionamento si può pensare ad un mittente che inserisce un messaggio in una scatola chiusa a chiave, la scatola viene consegnata ad un destinatario, che però non può aprire la serratura da solo.

[1] La doppia barra verticale indica la concatenazione

[2] https://en.wikipedia.org/wiki/Commitment_scheme

Poiché il destinatario ha la scatola, il messaggio al suo interno non può essere cambiato, ma solo rivelato se il mittente decide di fornire la chiave in un secondo momento. Le interazioni in uno schema di impegno si svolgono in due fasi:

- La fase di commit (*commit phase*) durante la quale un valore viene scelto e specificato;
- La fase di rivelazione (*reveal phase*) durante la quale il valore viene rivelato e verificato.

Affinché il processo funzioni devono essere rispettate due proprietà di sicurezza:

- **Hiding:** nei protocolli semplici, la fase di commit consiste in un singolo messaggio dal mittente al destinatario. Questo messaggio si chiama impegno ed è essenziale che il valore specifico scelto non possa essere conosciuto dal destinatario in quel momento;
- **Binding:** una fase di rivelazione consiste in un messaggio dal mittente al destinatario, seguito da un controllo effettuato dal destinatario. Il valore scelto durante la fase di commit deve essere l'unico che il mittente può calcolare e in seguito convalidare durante la fase di rivelazione.

3. **Resistenza alla seconda preimmagine (o Puzzle-friendliness)**
   Si dice che una funzione hash H sia **puzzle-friendliness** se per ogni possibile valore di output y, costituito da n-bit, se k viene scelto da una distribuzione con un'entropia minima elevata, allora è impossibile trovare x tale che $H(k\|x) = y$ in tempo significativamente inferiore a 2^n.
   Un'applicazione consiste nella costruzione di *puzzle di ricerca*, costituiti da:

   - Una funzione hash H;
   - Un valore *id* (chiamato **puzzle-ID**), scelto da una distribuzione con min-entropia elevata;
   - Un insieme di target Y.

   Per risolvere il puzzle è necessario trovare un input in modo che l'output rientri nell'insieme Y, che in genere è molto più piccolo dell'insieme di tutti gli output.

La dimensione di Y determina quanto è difficile il puzzle. Se $Y = \{0,1\}^n$ il puzzle è banale, mentre se Y ha solo 1 elemento il puzzle è estremamente difficile. Il fatto che l'ID puzzle abbia una min-entropia elevata garantisce che non ci siano scorciatoie. Al contrario, se l'ID fosse probabile, qualcuno potrebbe imbrogliare, ad esempio pre-calcolando una soluzione al puzzle con quell'ID.

Quindi, questa è una buona strategia da usare per ottenere un puzzle difficile da risolvere, purché l'ID sia generato in maniera opportunamente casuale. Questa è l'idea alla base del mining di Bitcoin, che è una sorta di puzzle computazionale e verrà meglio descritto in seguito.

Le funzioni hash presenti in letteratura sono molteplici ma nel contesto Bitcoin quella utilizzata per la blockchain è la funzione hash SHA-256, descritta nella prossima sezione.

2.1.1 SHA-256

Con il termine SHA dall'acronimo di **Secure Hash Algorithm**[3], dal quale cui si può intuire che si tratta di un algoritmo di hashing molto sicuro, si vuole indicare una famiglia di funzioni crittografiche hash, sviluppate a partire dal 1993 dalla National Security Agency (NSA).

Esse si possono catalogare in 4 standard, quali:

1. SHA-0: fu il nome dato alla versione originale della funzione hash a 160 bit pubblicata nel 1993. È stata ritirato poco dopo la pubblicazione a causa di un "difetto significativo" non rivelato e sostituito dalla versione leggermente rivista SHA-1;

2. SHA-1: è una funzione hash a 160 bit molto simile alla precedente, dalla quale differisce per una sola rotazione di bit. A seguito della scoperta di alcuni punti deboli questo standard non è più stato approvato per la maggior parte degli usi crittografici dopo il 2010;

[3] https://en.wikipedia.org/wiki/Secure_Hash_Algorithms

3. SHA-2: è l'insieme di due funzioni hash simili, con dimensioni di blocco diverse, note come SHA-256 e SHA-512. Differiscono nella dimensione delle stringhe; SHA-256 utilizza stringhe da 32 byte, mentre, SHA-512 utilizza stringhe da 64 byte. Esistono, inoltre, delle versioni troncate di ogni standard, note come SHA-224, SHA-384, SHA-512/224 e SHA-512/256;

4. SHA-3: è una funzione hash, precedentemente chiamata Keccak, scelta nel 2012 dopo un concorso pubblico tra designer non facenti parte della NSA. Supporta le stesse lunghezze del gruppo SHA-2 ma la sua struttura interna differisce in modo significativo.

Nel contesto Bitcoin la funzione presa in considerazione è la **SHA-256** che si utilizza in diversi scenari, quali: la creazione dell'address, il calcolo dell'ID di una transazione, la generazione dell'identificativo del blocco. Ma questi argomenti verranno discussi meglio in seguito.

Teoricamente la SHA-256 si ottiene tramite la cosiddetta *trasformazione di Merkle-Damgård*[4], la quale venne descritta nella tesi di dottorato di Ralph Merkle nel 1979. La trasformazione consiste nel costruire una funzione hash a partire da una funzione di compressione a senso unico[5], resistente alle collisioni. In crittografia una funzione di compressione a senso unico è una funzione che trasforma 2 valori in ingresso di lunghezza fissa in un valore in uscita, della stessa dimensione di quella dei valori passati. Con il termine a "senso unico" (o One-Way) si intende che risulta particolarmente difficile calcolare i valori in ingresso avendo a disposizione solo il risultato compresso.

Questo metodo rende possibile la conversione di una qualsiasi funzione hash di lunghezza fissa in una funzione hash delle stesse dimensioni ma resistente alle collisioni. Dunque, lo scopo della funzione hash è quello di prendere in ingresso una stringa di una lunghezza arbitraria e restituire in output un'altra stringa della stessa lunghezza (detta *digest*), in questo caso specifico, dato che si parla di SHA-256 la stringa sarà lunga 256 bit.

[4]https://it.wikipedia.org/wiki/Costruzione_di_Merkle-Damgård
[5]https://it.wikipedia.org/wiki/Funzione_di_compressione_a_senso_unico

Per dimostrare la proprietà di resistenza alle collisioni di queste praticolari funzioni hash si fornisce un esempio pratico [Act20]. Si consideri come messaggio in chiaro la stringa "bitcoininaction", il cui digest cifrato corrispondente è il seguente, in esadecimale:

`b76b7041106a75de9fa4fbf880b3886cc114cbfd570e1a17adb58b937afee351`

Non è difficile intuire che da questo è impossibile risalire alla stringa originale. Provando ad applicare nuovamente la funzione crittografica si otterrà il seguente risultato:

`b76b7041106a75de9fa4fbf880b3886cc114cbfd570e1a17adb58b937afee351`

Il risultato è esattamente lo stesso del precedente, ma provando a cambiare leggermente la stringa il suo hash corrispondente sarà diverso. Ad esempio, si consideri la stringa "bitcoininaction.com", applicando la funzione SHA-256 il digest risulterà:

`41dbcc447756ddd2c32ac99c76ef6f090fa0a63da5a6ecfda3311936f85daa85`

Come si può notare il risultato è completamente diverso. Ogni messaggio in chiaro su cui è applicato l'algoritmo SHA256 produce un digest unico e, dunque, è possibile affermare che questa funzione hash è resistente alle collisioni. Non sarebbe così se due messaggi diversi producessero lo stesso digest.

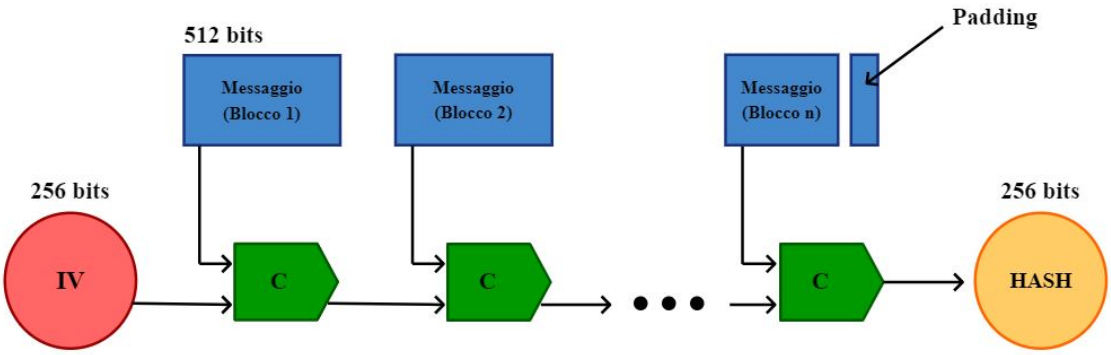

Figura 2.1: Schema di lavoro di una funzione hash SHA-256

Viene fornito adesso un esempio più tecnico di come avviene questa cifratura, facendo riferimento allo schema riportato in Figura 2.1.

Fondamentalmente, funziona nel modo seguente:

- Prende in input un messaggio e lo suddivide in blocchi di 512 bit. Se la lunghezza del messaggio non è un multiplo di 512 si ricorre ad una sorta di riempimento cioè si aggiunge all'ultimo blocco un ulteriore blocco di bit, detto *Padding*. Nello specifico questo è composto dal primo bit inizializzato ad 1 seguito da un certo numero di bit inizializzati a 0;
- L'algoritmo parte da un vettore di inizializzazione (chiamato IV) di 512 bit che viene associato al primo blocco del messaggio. Questa sequenza di 768 bit diventa l'input di una *funzione di compressione c* che emette una stringa di 256 bit;
- La funzione di compressione viene applicata alla concatenazione del primo output e del secondo blocco, ottenendo un nuovo output compresso di lunghezza 256 bit;
- Il processo viene ripetuto per tutte le sequenze di 768 bit, finché non si ottiene in output l'hash finale (*message digest*) a 256 bit.

Nella prossima sezione verrà descritto il modo in cui le funzioni hash possono essere sfruttate per costruire strutture dati più complicate che vengono utilizzate in sistemi distribuiti come Bitcoin, nello specifico verrà introdotto il concetto di puntatore Hash.

2.2 Puntatori Hash

Un **puntatore hash**, la cui rappresentazione è visibile in Figura 2.2, è una struttura dati che contiene al suo interno l'indirizzo del blocco precedente in cui vengono memorizzate alcune informazioni e un hash crittografico delle informazioni che esso stesso contiene.

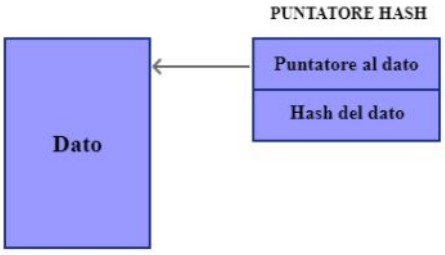

Figura 2.2: Puntatore Hash

Come un puntatore normale dà modo di recuperare le informazioni, ma in più offre anche la possibilità di verificare che tali informazioni non siano state cambiate, poiché al suo interno è contenuto un riassunto di ciò che rappresenta il dato.

In Figura 2.3 viene riportato l'esempio di come si possa costruire una blockchain utilizzando dei puntatori hash. L'inizio dell'elenco è un normale puntatore hash che punta al blocco di dati più recente e così via, fino ad arrivare al blocco dati meno recente.

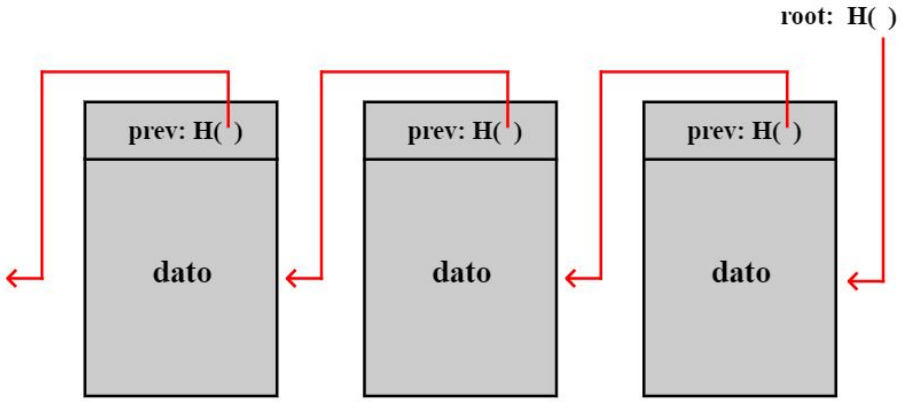

Figura 2.3: Struttura di una blockchain con puntatori hash

Questo tipo di costruzione rende la blockchain resistente alle manomissioni. Se qualcuno prova ad alterare i dati è facile risalire al registro che è stato compromesso. Per capire come sia possibile che questa proprietà antimanomissione funzioni, bisogna chiedersi cosa succederebbe se un avversario provasse a manomettere i dati che si trovano nel mezzo della catena.

Si consideri la seguente situazione: l'avversario tenta la manomissione del registro modificando i dati di un blocco k. A seguito della modifica, l'hash nel blocco $k+1$ cambierà e non corrisponderà con l'hash del blocco k. Il fatto che non corrisponderà è garantito dalla proprietà di resistenza alle collisioni della funzione hash. Dunque, in questo modo viene rivelata l'incongruenza tra i nuovi dati nel blocco k e il puntatore hash nel blocco $k+1$. Ovviamente l'avversario potrebbe provare a mascherare questa modifica cambiando anche l'hash del blocco successivo, continuando con questa strategia per tutta la catena di blocchi, ma la strategia è destinata a fallire una volta raggiunta la cima della lista.

Il puntatore hash all'inizio della lista non può essere cambiato, dunque, l'avversario non sarà in grado di cambiare alcun blocco senza essere rilevato. Il risultato è che per manomettere i dati in qualsiasi punto della catena dovrà manomettere i puntatori hash fino all'inizio, ma arriverà in un vicolo cieco poiché non sarà in grado di manomettere il capo della lista (la radice). Mantenendo in un luogo sicuro la radice la struttura risulterà essere a prova di manomissione. Un'alternativa a questa struttura è una blockchain basata sulla costruzione di Merkle-Damgard, da cui il nome *Merkle tree (alberi di Merkle)*, in cui la lista viene rimpiazzata dagli alberi. Questa soluzione viene descritta di seguito.

2.2.1 Alberi di Merkle

Gli **alberi di Merkle** [Nar+16], che devono il nome al loro inventore Ralph Merkle, sono degli alberi binari che utilizzano i puntatori hash. Basandosi sulla Figura 2.4 che ne ritrae lo schema, per spiegare il funzionamento si procede dal basso verso l'alto.

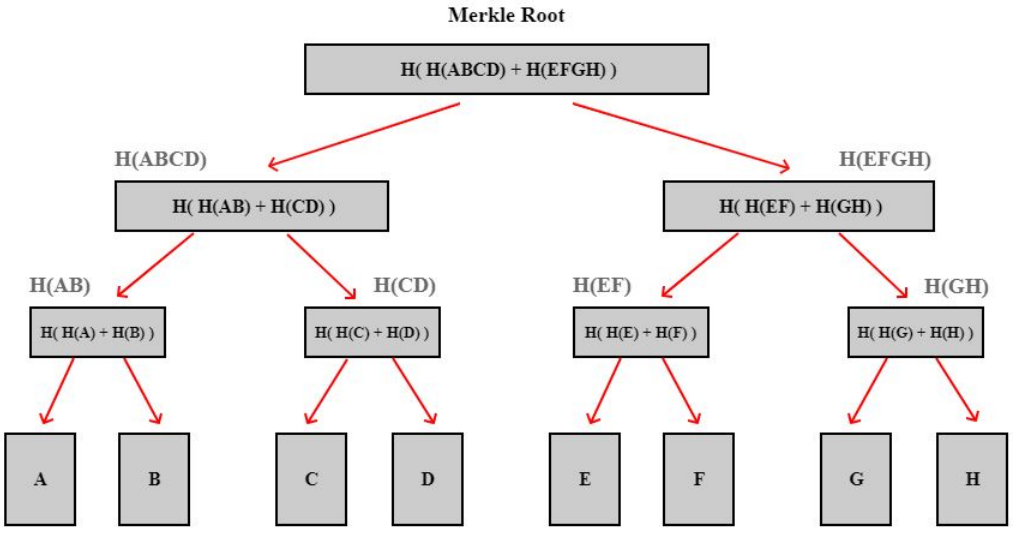

Figura 2.4: Merkle tree

I dati veri e propri sono contenuti nei nodi foglia i quali vengono organizzati a coppie (se l'insieme dei blocchi di dati è un numero dispari, l'ultimo blocco sarà in coppia con una copia di se stesso). Il livello superiore di ogni coppia di nodi foglia, è costituito da due puntatori hash, uno per ciascuna foglia.

Queste coppie di puntatori verranno raggruppate a due a due e nel livello superiore ci saranno dei nuovi blocchi, contenenti i puntatori hash ad esse. Si procede in questo modo verso l'alto fino a raggiungere un singolo blocco, la radice (**Merkle tree root**).

Anche questo tipo di struttura, come quella descritta in precedenza, è resistente alle manomissioni. Infatti, se un avversario manomette l'hash di un blocco di dati nella parte inferiore dell'albero causerà la non corrispondenza del rispettivo hash del livello superiore. Inoltre, se l'avversario fosse in grado di continuare a manomettere tutta la catena di puntatori hash arriverebbe prima o poi in cima dove non sarebbe in grado di manomettere il puntatore hash contenuto nella radice. Quindi di nuovo, ogni tentativo di manomettere qualsiasi dato verrà rilevato semplicemente, come già detto, mantenendo in un luogo sicuro la radice dell'albero.

Per confermare ulteriormente la sicurezza di questo meccanismo e dimostrare che a livello computazionale risulti più efficiente del precedente caso d'uso, è possibile fornire delle nuove prove. Nello specifico:

- **Prova di appartenenza:**
  Supponendo che qualcuno voglia dimostrare che un determinato blocco di dati faccia parte del Merkle Tree, rappresentazione in Figura 2.5, sarà necessario conoscere solo la radice dell'albero ed un certo numero di blocchi. È possibile ignorare il resto dell'albero, poiché i blocchi lungo questo percorso sono sufficienti ad effettuare la verifica degli hash, dal nodo desiderato fino alla radice dell'albero.

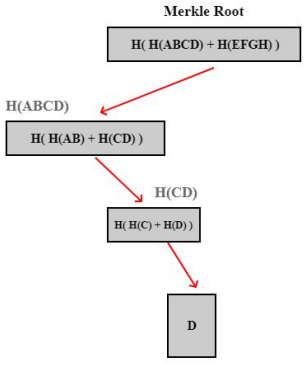

Figura 2.5: Appartenza ad un Merkle Tree

  Poiché ogni passaggio richiede solo il calcolo dell'hash del blocco figlio, con un numero di blocchi pari ad n (con n molto grande), il tempo di verifica sarebbe dell'ordine di $O(log\ n)$. Dunque è possibile dimostrare l'appartenenza in un tempo relativamente breve.

Nel caso descritto in precedenza, con i blocchi organizzati a lista il tempo richiesto sarebbe di $O(n)$ nel caso pessimo, poiché se il blocco da ricercare fosse alla fine bisognerebbe scorrere tutta la lista per accertare l'appartenenza.

- **Prova di non appartenza:**
  Per provare la non appartenenza di un blocco è necessario partire da un albero di Merkle ordinato, che si definisce tale se partendo dalle foglie si ordinano i blocchi tramite una qualsiasi funzione di ordinamento (alfabetica, numerica o un qualsiasi ordine concordato). Fatto questo, diventa possibile dimostrare che un particolare blocco non è presente all'interno dell'albero, in tempo e spazio logaritmici.

  La logica è molto semplice: posto X come il blocco non presente, basterà mostrare un percorso fino all'elemento che si trova appena prima a dove X dovrebbe stare e un percorso fino all'elemento che si trova subito dopo a dove X dovrebbe stare. Se questi due elementi sono consecutivi nell'albero, ciò diventa una prova del fatto che il blocco in questione non è incluso nell'albero. Poiché se fosse incluso, dovrebbe trovarsi tra i due elementi in questione, ma essendo consecutivi non c'è spazio tra di loro.

Le tecniche discusse fino a questo momento, che fanno uso di puntatori hash in elenchi collegati e alberi binari, hanno validità in contesti in cui le strutture dati non presentino dei cicli. In presenza di cicli non sarà possibile trovare corrispondenza tra i vari hash. Ad esempio, in una struttura dati aciclica basata sugli alberi binari, è possibile partire dalle foglie, calcolare gli hash e risalire fino alla radice. Al contrario, in una struttura dati con cicli non ci sarebbe un punto finito da cui partire per calcolare gli hash a ritroso.

Nella prossima sezione verrà introdotto il concetto di firma digita e di crittografia asimmetrica, anch'esse utilizzate nell'ambito dello sviluppo di una blockchain.

2.3 Firma Digitale

Nel contesto di Bitcoin, quello che realmente interessa non è tanto la riservatezza dei dati in sé, quanto il rispetto di 3 proprietà fondamentali:

1. **Autenticazione:** chi riceve un messaggio deve poterne identificare con certezza la provenienza, ossia verificare l'identità del mittente;

2. **Integrità:** i dati e le informazioni memorizzate in un sistema o scambiate tra due entità devono essere protette da modifiche non autorizzate (alterazione, cancellazione o aggiunta);

3. **Non-Ripudiabilità:** chi genera un messaggio non deve poter negare di averlo generato, né deve poter negare il contenuto. Allo stesso modo, chi riceve un messaggio non deve poter negare di averlo ricevuto, né deve poter negare il contenuto.

La sicurezza della blockchain deriva dal tipo di crittografia che utilizza. Ogni transazione viene criptata e solo il suo destinatario è in grado di decriptarla. Così facendo non sono necessari particolari sistemi di sicurezza per difendere un dato, in quanto questo viene reso indecifrabile per tutti coloro che non sono autorizzati a leggerlo. Per ottenere questo livello di sicurezza si frutta la **firma digitale**, cioè un metodo matematico teso a dimostrare l'autenticità di un messaggio o di un documento digitale inviato attraverso un canale di comunicazione non sicuro, che garantisce il rispetto delle proprietà sopra citate. Le firme digitali, infatti, sono utili per rivelare la falsificazione o l'alterazione dei dati in circolazione e si basano su schemi o protocolli crittografici. Nello specifico, sfruttano le caratteristiche della crittografia asimmetrica che sarà descritta in modo dettagliato nella prossima sezione.

2.3.1 Crittografia Asimmetrica

Gli algoritmi di cifratura sono spesso divisi in due categorie: *cifratura simmetrica e asimmetrica*. Gli algoritmi di cifratura simmetrica utilizzano una chiave singola per cifrare e decifrare i messaggi, la quale viene scambiata tra mittente e destinatario, mentre, la cifratura asimmetrica utilizza due chiavi differenti ma correlate. Entrambe le tipologie di cifratura presentano vantaggi e svantaggi. Gli algoritmi di cifratura simmetrica sono molto più veloci e richiedono una potenza di calcolo minore, ma il loro punto debole è la distribuzione della chiave. In genere le chiavi simmetriche sono lunghe 128 o 256 bit e questo comporta dei rischi a livello di sicurezza perché sono più soggette ad attacchi.

In confronto, la cifratura asimmetrica risolve il problema di sicurezza, utilizzando chiavi più lunghe di 2048 bit, e il problema della distribuzione della chiave, usando chiavi pubbliche per la codifica e chiavi private per la decodifica. Lo svantaggio, però, sta nel fatto che i sistemi a cifratura asimmetrica sono molto più lenti e richiedono una potenza di calcolo maggiore a causa delle chiavi più lunghe. Questo breve confronto è utile a comprendere perché la creazione e la verifica di firme digitali si basi sulla crittografia asimmetrica. Di seguito verrà approfondita la logica che si nasconde dietro il funzionamento di uno schema di firma digitale. Partendo da una definizione teorica uno schema di firma digitale consiste di 3 algoritmi:

1. $(sk, pk) := generateKeys(keySize)$: il metodo *generateKeys* accetta in input una dimensione della chiave e genera una coppia di chiavi. La chiave segreta *sk* viene mantenuta privata ed utilizzata per firmare i messaggi. La chiave pubblica *pk* funge da chiave di verifica e viene resa nota a tutti. Chiunque possegga questa chiave può verificare la firma.

2. $sig := sign(sk, message)$: il metodo *sign* accetta in input una chiave segreta *sk* e un messaggio, e restituisce in output una firma del messaggio tramite *sk*.

3. $isValid := verify(pk, message, sig)$: il metodo *verify* accetta in input una chiave pubblica *pk*, un messaggio e una firma, e restituisce in output un valore booleano *isValid*, che sarà TRUE se *sig* è una firma valida per il messaggio con chiave pubblica *pk*, altrimenti FALSE.

È necessario, inoltre, che le seguenti 2 proprietà siano valide:

- Le firme valide devono essere verificate:

$$verify(pk, message, sign(sk, message)) == true$$

- Le firme sono **existentially unforgeable**, cioè deve essere impossibile per l'avversario falsificare la firma.

Per rendere più chiara l'idea viene fornito di seguito un esempio pratico di applicazione di queste proprietà, considerando lo scambio di messaggi tra due persone A e B.

Come già detto in precedenza, la crittografia asimmetrica si basa sull'utilizzo di una coppia di chiavi: *pubblica e privata*. Tale coppia è legata matematicamente da un algoritmo crittografico, che assicura che un messaggio criptato con una delle due chiavi possa essere decifrato solo dall'altra. Si consideri l'esempio in Figura 2.6

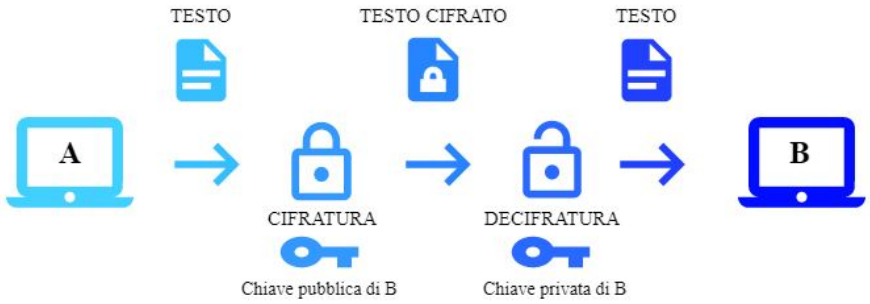

Figura 2.6: A manda un messaggio a B

A intende mandare un messaggio a B e per essere sicuro che solo B sia in grado di leggerne il contenuto, prima di procedere con l'invio, A utilizza la chiave pubblica di B per cifrare il messaggio (A conosce la chiave pubblica di B poiché, in quanto tale, B l'ha messa a disposizione di A). Così facendo il documento criptato risulta indecifrabile per A, in quanto non è in possesso della chiave privata di B (questa essendo appunto privata è in possesso solo di B). Dunque, il messaggio viene inviato e una volta ricevuto, B è in grado di decifrarlo utilizzando la sua chiave privata.

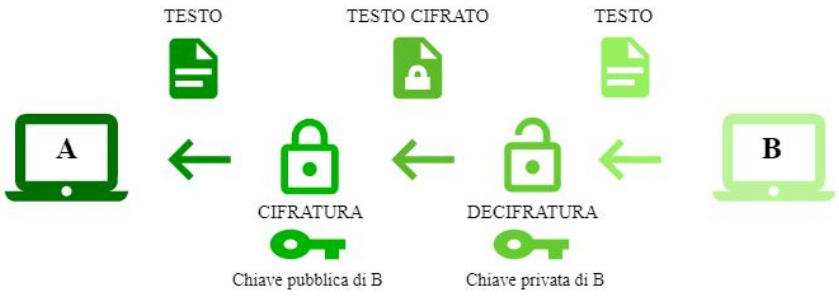

Figura 2.7: B decrifa il messaggio ricevuto e risponde ad A

B, a questo punto, decide di rispondere ad A utilizzando lo stesso metodo di crittografia, così da essere sicuro che solo lui possa leggere il contenuto del messaggio.

Facendo riferimento alla Figura 2.7, è facile intuire che la logica è la stessa di quella appena descritta, cioè B cripta il documento utilizzando la chiave pubblica di A, lo invia, A riceve il documento e lo decripta utilizzando la sua chiave privata. Questo esempio dimostra che il funzionamento della crittografia asimmetrica è piuttosto semplice quanto efficace. Non sarebbe efficace solo nel caso in cui venisse utilizzata la chiave privata per criptare il messaggio, questo perché chiunque fosse in possesso della chiave pubblica associata sarebbe in grado di decifrarlo. Arrivati a questo punto, è interessante comprendere come il tutto si applichi all'interno della blockchain, fulcro del sistema Bitcoin.

La blockchain utilizza la crittografia asimmetrica per permettere lo scambio di beni (es. criptovalute) tra due persone. Ogni persona che detiene un bene è in possesso di una chiave pubblica, nota in questo contesto come **address** (indirizzo), e di una chiave privata. Per rendere più semplice il tutto si consideri la presenza di 2 identità, quali:

- Enzo, con address: 0x1234567890
- Stefano, con address: 0x5678901234

Enzo e Stefano sono identificati all'interno della blockchain con un address, reso pubblico, tramite il quale è possibile inviare loro dei beni. Inoltre, ognuno di loro possiede una chiave privata, la quale, garantisce che l'invio di eventuali beni sia realmente voluto dal proprietario di essi, in quanto, solo chi è in possesso della chiave privata è in grado di effettuare il trasferimento. Chiunque in possesso della chiave privata sarà in grado di effettuare qualsiasi operazione, dunque, è buona norma custodire le proprie chiavi private in luoghi sicuri, così da limitare il rischio di essere derubati.

Figura 2.8: Crittografia asimmetrica all'interno di una blockchain

In Figura 2.8 viene riportato un esempio di quello che succederebbe se Enzo volesse inviare 1 Bitcoin (BTC) a Stefano. Enzo accede ai suoi beni utilizzando la sua chiave privata, la transazione viene criptata utilizzando la chiave pubblica di Stefano e successivamente il Bitcoin viene spedito verso l'address 0x5678901234 di Stefano. La transazione avviene in maniera sicura e legittima, poiché essa viene autorizzata dalla chiave privata di Enzo verso l'address di Stefano, che è l'unico in grado di decriptare la transazione, utilizzando la sua chiave privata.

Per cifratura dei messaggi si intende che il messaggio viene firmato digitalmente dal mittente con la sua chiave privata e sarà poi il destinatario a poterlo decifrare, il tutto viene reso possibile dalla crittografia asimmetrica. In generale, l'utilizzo della firma digitale all'interno della tecnologia Blockchain, si può riassumere in due fasi:

1. **Creazione della firma**
   Quando un nodo crea una transazione, calcola l'hash di tutte le informazioni contenute al suo interno e lo cifra attraverso la sua chiave privata ottenendo così la firma digitale. Infine, invia le informazioni in chiaro della transazione e la firma a tutti i nodi della rete.

2. **Verifica della firma**
   Ogni nodo per verificare l'integrità delle informazioni ricevute calcola l'hash delle informazioni in chiaro. Applica la chiave pubblica alla firma digitale in modo da ottenere l'hash calcolato in precedenza dal nodo mittente. Se i due hash coincidono, allora le informazioni non hanno subito variazioni e la firma applicata risulta valida.

L'algoritmo utilizzato all'interno della Blockchain per la creazione e validazione della firma digitale è l'ECDSA, descritto di seguito.

2.3.2 ECDSA

Bitcoin utilizza uno schema di firma digitale chiamato **Elliptic Curve Digital Signature Algorithm (ECDSA)**. ECDSA è uno standard del governo degli Stati Uniti, nonché una variante del precedente algoritmo DSA adattato per utilizzare curve ellittiche, ed è generalmente ritenuto un algoritmo molto sicuro.

Nello specifico, Bitcoin utilizza ECDSA sulla curva ellittica standard "*secp256k1*" che si stima fornisca 128 bit di sicurezza, la quale, non è stata quasi mai utilizzata prima dell'avvento di Bitcoin, ma adesso pare stia acquisendo maggiore popolarità grazie alle sue proprietà interessanti. Le curve più comunemente usate hanno una struttura casuale, ma *secp256k1* è stata costruita in modo non casuale e questo consente un calcolo particolarmente efficiente. Di conseguenza, è spesso più del 30% più veloce di altre curve, se l'implementazione è sufficientemente ottimizzata.

Non è necessario conoscere tutti i dettagli relativi al suo funzionamento poiché dipendono da alcuni calcoli complicati ma potrebbe essere utile avere un'idea delle dimensioni dei vari oggetti coinvolti, se ne fornisce un elenco di seguito:

1. Chiave privata: 256 bit;
2. Chiave pubblica, non compressa: 512 bit;
3. Chiave pubblica, compressa: 257 bit;
4. Messaggio da firmare: 256 bit;
5. Firma: 512 bit.

Da notare che ECDSA può tecnicamente firmare solo messaggi di 256 bit, ma questo non rappresenta un problema poiché i messaggi vengono sempre sottoposti ad hashing, quindi è possibile firmare efficacemente messaggi di qualsiasi dimensione. Una cosa importante, invece, riguarda il concetto di **randomness**, cioè serve una buona dose di casualità nella generazione delle chiavi, poiché se non ci fosse queste non sarebbero sicure e potrebbero essere falsificate.

Fino a questo momento si è parlato spesso di transazioni e blocchi all'interno della blockchain, ma più che sulla struttura ci si è soffermati sulla parte legata alla sicurezza. Dunque, è arrivato il momento di capire quale sia la struttura fisica di blocchi e transazioni, proseguendo nelle sezioni successive.

2.4 Blocchi

Come già accennato in precedenza una blockchain, anche nota come **ledger**, è un registro di archiviazione distribuito che tiene traccia delle transazioni effettuate e non necessita di un'autorità centrale per essere gestita, ma, viene amministrata da un insieme di nodi che appartengono alla rete Bitcoin. Le transazioni vengono memorizzate in un elenco composto da blocchi sequenziali e man mano che vengono eseguite il numero dei blocchi aumenta. Il compito della blockchain è di tenere costantemente aggiornato il registro dei blocchi criptati e, nel contempo, eseguire gli algoritmi necessari a garantire la sicurezza dell'utente.

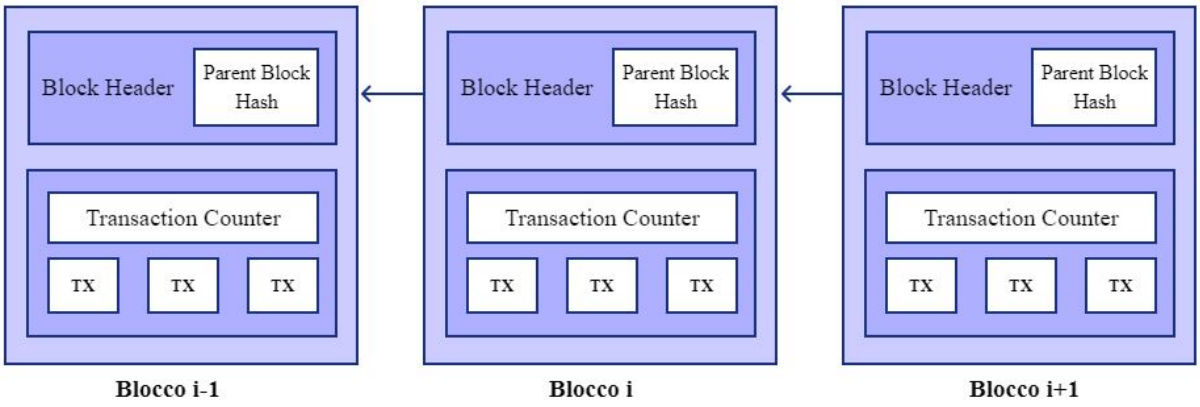

Figura 2.9: Struttura interna dei blocchi

In Figura 2.9 viene mostrata una versione più dettagliata, rispetto a quella già vista, della struttura dei blocchi che compongono una blockchain. In generale, ogni blocco consiste dell'intestazione (**Block Header**) e del corpo del blocco.

Il corpo del blocco è composto da un contatore di transazioni (**Transaction Counter**) e dalla lista di transazioni (**TX**). Il numero massimo di transazioni che può contenere il blocco dipende dalla sua dimensione e da quella di ogni transazione. Attualmente, la dimensione massima di un blocco è di 1 MB e ciò significa che è possibile processare al massimo 7 transazioni al secondo, questo è un limite tecnologico pensato per evitare che la rete venga saturata da transazioni di scarso valore.

Come si può notare in Figura 2.10, nell'intestazione di un blocco sono presenti 7 campi di gestione del blocco stesso.

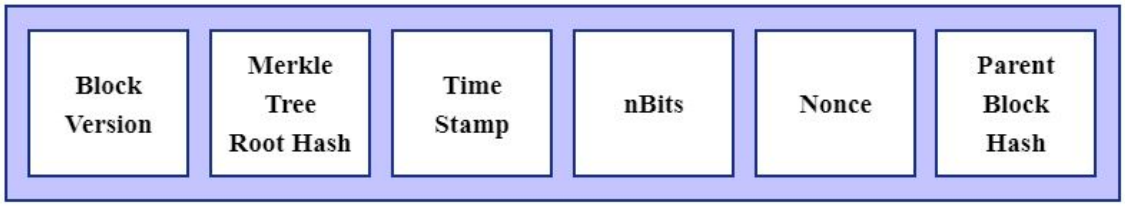

Figura 2.10: Struttura del blocco header

Da sinistra verso destra si può osservare:

1. **Block Version - 4 Byte**: è un valore intero che indica la versione del software usato e quindi l'insieme di regole da seguire per la validazione del blocco;
2. **Merkle Tree Root Hash - 32 Byte**: è l'hash della radice del Merkle Tree di questo blocco, quindi è complessivamente l'hash di tutte le transazioni nel blocco;
3. **Timestamp - 4 Byte**: è l'orario di creazione del blocco;
4. **nBits (o Target) - 4 Byte**: è la soglia che l'hash del blocco non deve superare affinché il blocco sia ritenuto valido;
5. **Nonce - 4 Byte**: è un numero di 32 bit, che normalmente inizia con 0 e aumenta ad ogni calcolo di un hash, e viene utilizzato per risolvere la Proof-of-Work dei miners;
6. **Parent Block Hash - 32 Byte**: è un valore hash a 256 bit che punta al blocco precedente. L'unico blocco che non possiede questo puntatore è il primo aggiunto alla catena, conosciuto come *Genesis Block*.

Il numero di transazioni presenti in un blocco di norma è superiore a 500 e ciascuna occupa in media 225 Byte. Considerando che la dimensione dell'header è di 80 Byte si può concludere che un blocco completo di tutte le transazioni è più di 1000 volte superiore al proprio header. Di seguito verrà descritta la struttura interna di una transazione.

2.5 Transazioni

Ogni transazione possiede un identificativo chiamato **Transaction ID** che rappresenta l'hash della transazione stessa. Gli elementi che caratterizzano le transazioni Bitcoin sono gli output non spesi, o **UTXO** (*Unspent Transaction Outputs*). In Figura 2.11[6] viene riportata la struttura interna di una transazione.

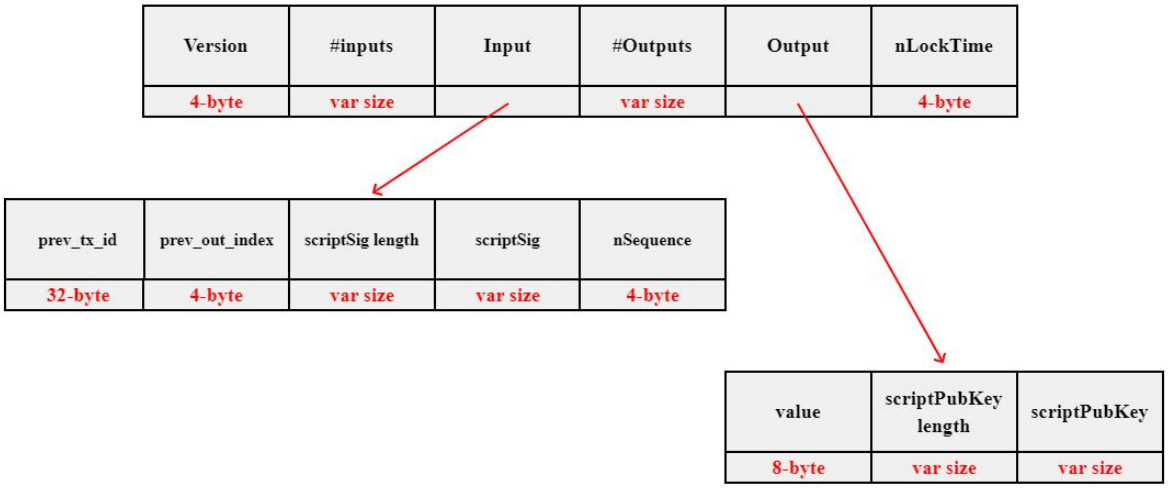

Figura 2.11: Struttura di una transazione

Andando più nel dettaglio, una transazione è composta da 6 campi principali:

1. **Version**: indica la versione del protocollo e l'insieme di regole da seguire per la validazione della transazione;
2. #**Inputs**: è il contatore degli input inclusi nella transazione;
3. **Input**: è la lista di input della transazione;
4. #**Outputs**: è il contatore degli output inclusi nella transazione;
5. **Outputs**: è la lista di output della transazione;
6. **nLockTime**: è il tempo che deve trascorrere prima che la transazione possa essere aggiunta alla blockchain.

[6]Per *var size* si intende che quel particolare elemento ha dimensione variabile (1-9 Byte)

Secondo la definizione data in precedenza di UTXO, una transazione può essere vista come una raccolta di input e output. Gli input si riferiscono agli UTXO creati in precedenza, mentre gli output ne generano di nuovi. Pertanto, quando si crea una transazione, ogni input spende un UTXO e ogni output ne crea uno nuovo. In particolare, la struttura di un input è così composta:

- **prev_tx_id**: è il puntatore alla transazione precedente che contiene l'UTXO da consumare;
- **prev_out_index**: è l'indice del suddetto UTXO;
- **scriptSig length**: contiene informazioni sulla lunghezza di scriptSig;
- **scriptSig**: è uno script, conosciuto anche come *Signature Script (stript di firma*, utilizzato per verificare il rispetto delle condizioni di spesa definite nell'UTXO da consumare;
- **nSequence**: è un numero utilizzato per la verifica del LockTime.

L'output, invece, è così composto:

- **value (o amount)**: rappresenta la quantità di Bitcoin da inviare agli altri nodi della rete;
- **scriptPubKey length**: contiene informazioni sulla lunghezza di scriptPubKey;
- **scriptPubKey**: è lo script utilizzato per stabilire quali sono le condizioni da rispettare per spendere l'output.

Di seguito, viene mostrato un esempio del processo che porta all'accettazione di una transazione.

2.5.1 Accettazione di una Transazione

Sì consideri come esempio una transazione di Bitcoin che Alice (pagante) fa verso Bob (ricevente). In Figura 2.12 viene mostrato il processo che porterà all'accettazione della transazione.

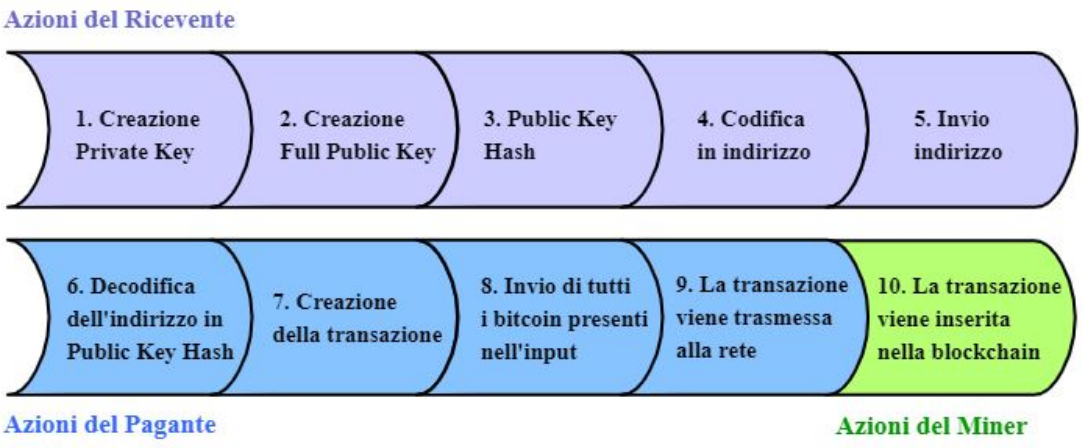

Figura 2.12: Processo di accettazione di una transazione

Tale processo si può suddividere in 10 fasi[7]:

1. Bob genera una chiave privata (*Private Key*), rappresentata da una sequenza del tutto casuale di cifre, e la salva sul suo computer;

2. La chiave privata viene convertita in chiave pubblica (*Full Public Key*) tramite l'algoritmo ECDSA, precedentemente descritto, basato sulle curve ellittiche. Da notare che si tratta di un processo unidirezionale, ovvero è possibile generare una chiave pubblica a partire da quella privata ma non il contrario. Il processo inverso richiederebbe una quantità di tentativi e una potenza di calcolo talmente enorme da essere al di là di ogni possibilità. Se esistesse un supercomputer in grado di effettuare quest'operazione allora probabilmente qualsiasi password nel mondo sarebbe vulnerabile, anche all'esterno del contesto Bitcoin;

3. La chiave pubblica viene crittografata tramite una funzione hash e dunque la sua lunghezza viene ridotta (*Public Key Hash*);

4. L'hash della chiave pubblica viene codificato in un indirizzo, cioè una stringa che per comodità è lunga al più 35 caratteri. Questa codifica altro non è che l'indirizzo del portafoglio (*o wallet*) di Bob;

[7]Le prime 4 fasi avvengono istantaneamente

5. L'indirizzo codificato viene spedito al pagante (Alice);

6. Il software di Alice decodifica l'indirizzo in hash della chiave pubblica;

7. A questo punto il pagante è in grado di creare la transazione. Stando alle definizioni date in precedenza riguardanti la struttura interna di una transazione, in questo esempio essa dovrà contenere principalmente:

   - *L'input*: uno o più output di una transazione precedente fatta nei confronti di Alice, da cui attinge i Bitcoin da spedire nel nuovo output;
   - *L'output*: la quantità di Bitcoin spediti. Possono esserci più output per ogni transazione, ciascuno identificato con un ID specifico;
   - *Il signature script*: le istruzioni che Bob dovrà fornire per convalidare la transazione, dimostrando di essere il possessore del nuovo output. Per la creazione di questo script il software di Alice ha bisogno della Public Key Hash fornita da Bob. Le informazioni necessarie per validare la firma sono due, entrambe già in possesso di Bob: la full Public Key e la Private Key, che dovranno coincidere con la Public Key Hash specificata da Alice nello script;
   - *La versione del software*: quest'informazione permette di modificare il protocollo senza invalidare le passate transazioni, poiché queste risulteranno registrate nella blockchain come valide pur non rispettando più le nuove regole.

   Queste informazioni vengono processate insieme per creare un unico hash chiamato *Transaction ID* (o txID).

8. Il pagante conferma la transazione e tutti i Bitcoin che Alice ha a disposizione nell'input vengono spediti nella transazione in uno o più output. Inoltre, è importante ricordare che nella transazione viene coinvolta sempre l'intera quantità di Bitcoin presenti nell'input anche se il ricevente ne richiede un numero inferiore. Ad esempio, se Alice possiede un input di 100 Bitcoin e ne vuole inviare 20 a Bob, l'input viene trasferito nella sua interezza ma, in questo caso, avrà due output diversi. Un output sarà di 80 Bitcoin che torneranno al portafoglio di Alice (*change output*),

l'altro sarà di 20 Bitcoin che andranno all'indirizzo di Bob. L'unico caso di transazione che abbia un solo input e un solo output è quello in cui l'input corrisponde esattamente all'ammontare richiesto;

9. Alice trasmette online la transazione a tutti gli altri nodi della rete;

10. I miner inseriscono nella blockchain la transazione, che viene riconosciuta da tutti i nodi della rete. Per inserire le transazioni all'interno della blockchain il miner deve creare un nuovo blocco. Questo processo richiede una quantità di calcolo molto elevata e una spesa in energia elettrica e strumenti. Un miner ha interesse ad inserire quante più transazioni nel blocco che vuole creare poiché guadagnerà le commissioni pagate per ciascuna. Se una transazione non include alcuna commissione non vi è interesse economico nell'inserirla nel blocco.

    Per fare ciò, i miner partono dagli id delle transazioni (txId), i quali rappresentano l'hash delle informazioni inerenti alle stesse. Viene costruito il cosiddetto Merkle tree, descritto nelle sezioni precedenti. Le foglie rappresentano le transazioni, i rami gli hash intermedi e la radice (la Merke root) l'hash finale, cioè il prodotto di tutti gli altri hash. Grazie a questa struttura ad albero, non è necessario conoscere tutte le transazioni incluse in un blocco per verificare che una specifica transazione ne faccia parte, è invece sufficiente seguire un particolare ramo che collega una foglia alla Merkle root.

Si consideri a questo punto una nuova fase, riportata in Figura 2.13, in cui Bob può decidere di spendere i Bitcoin appena ricevuti. Quindi l'output della prima transazione diventerà l'input di una nuova transazione creata da Bob.

Figura 2.13: L'output della TX #1 come input della TX #2

Dunque, la fase 11 avviene solamente durante la seconda transazione, nella quale il ricevente firma il Signature script con la propria chiave privata e pubblica, dimostrando così di essere il proprietario dell'output della transazione precedente. Fatto questo, avrà la possibilità di spendere quell'output come input di una nuova transazione, della quale diventerà il pagante. Il procedimento è esattamente lo stesso di quello appena descritto e comprensivo delle 10 fasi.

Con il bagaglio di informazioni raccolto sino a questo momento, relativo ai sistemi di sicurezza e alla particolarità della blockchain, è possibile comprendere il funzionamento del protocollo Bitcoin. Nei prossimi capitoli, infatti, verrà fornita prima di tutto una panoramica sulle motivazioni che hanno portato alla nascita di Bitcoin, verrà descritta la sua struttura e i processi che ne caratterizzano il funzionamento e, in seguito, verranno elencati i pro e i contro di tale architettura.

Capitolo 3

Il Funzionamento della Rete Bitcoin

Il **Bitcoin (o BTC)** è una criptovaluta che definisce un sistema di pagamento elettronico e fu ideata nel 2009. Il suo creatore è conosciuto con lo pseudonimo di Satoshi Nakamoto [Nak08], ma ad oggi non è ancora possibile sapere con certezza se dietro questo nome si nasconda una persona o gruppo o un gruppo di persone.

Nakamoto ha continuato a collaborare con altri sviluppatori del protocollo fino a metà del 2010, per poi lasciare il controllo del codice sorgente a Gavin Andresen, il suo collaboratore più fidato fino a quel mostrano che i portafogli di Nakamoto contengono circa 1 milione di Bitcoin.

Come si legge nell'articolo pubblicato dallo stesso Nakamoto, l'idea era quella di creare un sistema che fosse una soluzione per problemi legati ai sistemi di commercio presenti su internet, i quali fanno affidamento quasi esclusivamente ad istituti finanziari, che fungono da terze parti, per elaborare i pagamenti elettronici. Ad esempio, trattandosi di modelli basati sulla fiducia, operazioni irreversibili non sono possibili poiché le istituzioni finanziarie non possono fare a meno di mediare le controversie e il costo della mediazione aumenta i costi di transazione.

Inoltre, i commercianti devono chiedere ai loro clienti più informazioni di quante ne avrebbero altrimenti bisogno. Infine, una certa percentuale di frode è accettata come inevitabile. Tutti questi costi e incertezze sui pagamenti si potrebbero evitare di persona utilizzando valuta fisica, ma in quel momento non esisteva alcun meccanismo per effettuare pagamenti su un canale di comunicazione senza una parte fidata.

Partendo da questi presupposti, Nakamoto, ebbe l'intuizione di creare un sistema di pagamento elettronico basato su *prove crittografiche* anziché sulla fiducia, che consentisse la comunicazione tra due parti disponibili senza la necessità di una terza parte fidata (*decentralizzazione e consenso distribuito*). Così facendo, le transazioni irreversibili proteggerebbero i venditori dalle frodi. Il tutto viene reso possibile in gran parte dalle firme digitali, ma Nakamoto, precisa che si avrebbe uno svantaggio se fosse necessaria una terza parte fidata in grado di evitare il problema della doppia spesa, descritto in seguito. La soluzione proposta in merito, riguarda l'utilizzo di un server di timestamp distribuito peer-to-peer che consente di mantenere l'ordine cronologico delle transazioni. Anche questa parte verrà approfondita in seguito, ma in generale l'idea è quella di segnalare le transazioni tramite hashing in una continua prova di lavoro (nota come *proof-of-work*) che rende impossibile la modifica dei blocchi, senza ripetere l'intera prova.

Dunque, il 3 gennaio 2009 fu creato il primo blocco Bitcoin (già citato in precedenza come *genesis block*) e vennero generati 50 BTC. Procedendo, però, per gradi la prima cosa da comprendere è il concetto di sistema decentralizzato. Un approfondimento a riguardo verrà fornito nella prossima sezione, per capire come la decentralizzazione funzioni all'interno della rete Bitcoin.

3.1 Decentralizzazione

Nel mondo delle criptovalute si parla spesso di decentralizzazione, senza però quasi mai esaminarne il vero significato e le possibili implicazioni. Innanzitutto bisogna precisare che esistono 3 tipologie fondamentali di struttura di una rete, infatti, questa può essere: centralizzata, decentralizzata, distribuita.

Nel gergo informatico le reti, come ad esempio internet, utilizzano strutture di comunicazione che vengono classificate in base ai ruoli e alle funzioni dei diversi utenti. I partecipanti alla rete sono tecnicamente definiti **nodi**. Nell'ecosistema di Facebook, per esempio, gli amministratori (o admin) scelgono le modifiche, gli aggiornamenti e le funzionalità del sito, mentre il ruolo degli utenti (o user) è quello di aggiungere i contenuti. Si crea così un ecosistema che dà valore agli utenti e all'azienda.

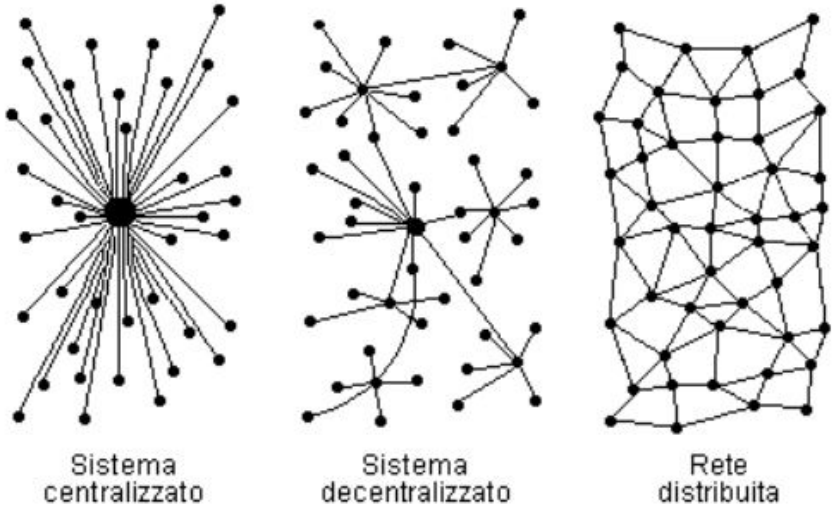

Figura 3.1: Rappresentazione di network centralizzati, decentralizzati e distribuiti

La Figura 3.1 può dare un'idea iniziale delle differenze strutturali relative ai 3 sistemi menzionati, analizzati di seguito:

- **Sistema Centralizzato**: tutti i nodi esterni sono detti **client**, mentre, il nodo centrale è detto **server**. Il server ha il compito di assolvere tutte le richieste dei client connessi alla rete. Un esempio può essere quello di una piccola realtà aziendale, dove i computer, in dotazione ai dipendenti, rappresentano i client che sono connessi ad unico server centrale sul quale è installato un software per la gestione delle attività commerciali quotidiane, come la contabilità;

- **Sistema Decentralizzato**: non esiste un server centrale ma ogni nodo può essere sia client sia server, realizzando così una nuova logica di elaborazione delle richieste.

I nodi attivi sulla rete collaborano tra di loro per elaborare i dati necessari alla risoluzione delle richieste fatte dai client. Con un'organizzazione del genere si riduce il rischio di dipendenza da un solo server. Infatti, quando un server è inaccessibile è possibile rivolgersi agli altri. La posta elettronica o le reti di chat sono esempi di sistemi decentralizzati;

- **Sistema Distribuito**: si può definire un sistema decentralizzato particolare, poiché anche in questo caso non esiste un server centrale. La differenza con il precedente sistema è che in questo caso, tutti i nodi hanno gli stessi privilegi e nessuno può essere isolato dal servizio. Ciò significa che ogni nodo è autosufficiente, non ci sono server dedicati a particolari servizi, al contrario, ogni nodo della rete possiede le stesse informazioni o dati. Internet è un esempio di rete distribuita poiché tutti i nodi sono uguali tra loro e posseggono la stessa copia dei dati in circolo sulla rete.

Tenendo a mente questi concetti, si può affermare che non esiste al mondo un sistema totalmente decentralizzato. La rete Bitcoin ne è l'esempio perfetto. Dal punto di vista architetturale la si può considerare come un sistema decentralizzato, poiché non è controllata da nessuno, ma al tempo stesso è anche logicamente centralizzata per quanto riguarda i dati che i blocchi contengono: un'unica catena di blocchi viene univocamente riconosciuta come valida e funge da riferimento per tutti i nodi partecipanti alla rete, che ne detengono una copia (completa o soltanto parziale). Inoltre, si può dire, che sia anche distribuita da un punto di vista informatico, perché funziona senza server, tutti gli utenti sono uguali e possiedono le stesse copie di dati.

Trattandosi complessivamente di una rete decentralizzata, come detto prima, Bitcoin soffre di alcuni svantaggi, il più noto è sicuramente il problema della doppia spesa (o *double-spending*). Nella prossima sezione verrà spiegato in che modo esso si può verificare e quali sono state le soluzioni adottate per prevenirlo.

3.2 Il Problema del Double-Spending

Il modo migliore per comprendere il problema è quello partire da un esempio.

Il mezzo di pagamento più comune al giorno d'oggi è la banconota, dunque, si potrebbe pensare di duplicarla prima di spenderla, in modo da poterla utilizzare più volte. Questa falsificazione di denaro è chiaramente un reato, ma per fortuna non è possibile semplicemente creare una copia di una banconota fisica identica all'originale. La stessa cosa non è scontata quando ci si riferisce al denaro digitale, infatti, dal momento che in informatica tutto è informazione e le informazioni sono costituite da bit, è facile che queste possano essere replicate e rese perfettamente identiche alle originali. Pertanto, duplicare denaro digitale risulta più semplice rispetto a duplicare una banconota fisica.

Tornando al problema, il **Double-Spending** o doppia spesa, altro non è che una frode digitale nella quale un utente cerca di spendere il proprio denaro, o meglio i propri bitcoin. Un bitcoin non può essere duplicato e quindi non è falsificabile, ma bisogna impedire che venga speso due (o più) volte, poiché se si potesse spendere più volte lo stesso bitcoin sarebbe come crearne delle copie. Per queste ragioni, il protocollo è stato ideato in modo che sia impossibile spendere due volte lo stesso token senza violarlo. In altre parole, se si rispetta il protocollo questo fenomeno non si può verificare, al contrario, non rispettandolo diventerebbe impossibile utilizzare Bitcoin.

Come già accennato in precedenza, la soluzione proposta, riguarda l'utilizzo di un server di timestamp distribuito utilizzato in una rete peer-to-peer (cioè in poche parole una rete di nodi paritari con a disposizione le stesse informazioni) che consenta di mantenere l'ordine cronologico delle transazioni. Si sta parlando della blockchain, cioè una catena di blocchi progettata in modo tale che non si possa incorrere nella duplicazione dei dati. Affinché questo sia possibile si sfruttano i timestamp, cioè dei marcatori temporali presenti in ogni blocco, i quali identificano l'orario di creazione del blocco stesso e ne garantiscono la tracciabilità. Inoltre, la verifica dell'hash permette di stabilire l'ordine cronologico dei blocchi inseriti nella catena.

Riassumendo, quello che il protocollo Bitcoin fa per evitare la doppia spesa dei token è verificare che questi non siano già stati inviati in passato, poiché così è impossibile che vengano inviati nuovamente.

Per evitare che i dati passati possano essere alterati bisognerebbe poter modificare a ritroso tutti i blocchi della catena dall'ultimo fino a quello in cui sono memorizzati i dati del precedente invio. Un'azione di questo tipo richiederebbe una tale potenza di calcolo che nessuno sarebbe realisticamente in grado di farlo. Ma questo aspetto verrà meglio analizzato in seguito quando si parlerà del ruolo della Proof-of-Work (PoW), che di fatto rende inattaccabile la blockchain. Fino a questo punto si può affermare che un'architettura di questo tipo è resistente agli attacchi Double-Spending e a molti altri noti (es. *Denail of Service* o DoS[1]), tuttavia, come spesso accade si possono creare delle falle nel sistema. Nel caso di Bitcoin l'unico modo che consentirebbe la compromissione del dati sarebbe quello di provare a falsificare la blockchain, con un attacco noto come *Attacco 51%* e descritto di seguito.

3.2.1 Attacco 51%

L'**Attacco 51%** è sicuramente tra i più conosciuti e potenti attacchi nel contesto delle criptovalute, anche se fino ad oggi non risulta che si sia mai verificato nei sistemi più noti. Un attacco di questo tipo può avvenire se un utente malevolo è in possesso del 51% della potenza di calcolo distribuita nel sistema. Questa potenza è meglio conosciuta come **Hashrate**, e rappresenta l'unità di misura della potenza di elaborazione della rete Bitcoin. In parole povere, quantifica la velocità con cui un calcolatore completa un'operazione, cioè quanto tempo è necessario per inserire delle nuove transazioni nella blockchain e quanta probabilità si ha di produrre dei blocchi validi.

Se l'utente malevolo, di cui sopra, controllasse la blockchain sarebbe in grado di trasferire bitcoin al suo portafoglio numerose volte invertendo il registro della blockchain, come se le transazioni iniziali non fossero mai avvenute. La validità di un blocco dipende dal consenso della rete, la quale decide quali sono i blocchi da accettare. Se durante questa fase un attaccante riuscisse a generare dei blocchi più velocemente sfruttando una maggiore potenza di calcolo, riuscirebbe a creare delle catene di blocchi più lunghe in minore tempo rispetto ai nodi onesti.

[1] https://it.wikipedia.org/wiki/Denial_of_service

Questo gli gioverebbe vantaggio poiché nel contesto Bitcoin si tende a considerare più affidabili le catene di blocchi più lunghe. Dunque, se un attacco 51% si verificasse sicuramente ci sarebbe una perdita di fiducia nei confronti del sistema e la moneta verrebbe rapidamente svalutata, ma come già detto in precedenza, non sono stati confermati attualmente, almeno per Bitcoin, attacchi di questo tipo.

Come si è visto fino a questo momento l'architettura decentralizzata di Bitcoin e l'utilizzo di algoritmi crittografici rendono il sistema sicuro, ma tutto ciò è possibile anche perché ci si affida alla politica del consenso distribuito. Questo argomento verrà ampiamente descritto nella prossima sezione.

3.3 Consenso Distribuito

Il consenso distribuito ha varie applicazioni ed è stato studiato per decenni nel campo dell'informatica. Le motivazioni che spingono al suo utilizzo sono legate all'affidabilità nei sistemi distribuiti. Tipicamente i sistemi di questo tipo posseggono migliaia o addirittura milioni di server, che insieme formano un enorme database distribuito dove si registrano tutte le azioni che avvengono nel sistema. Ogni informazione deve essere mantenuta su diversi nodi differenti, i quali devono essere sincronizzati sullo stato generale del sistema. In un contesto come Bitcoin, rispettare queste premesse implica che tutti i nodi coinvolti nella rete devono essere d'accordo su tre punti cardine, ovvero: sulla storia delle transazioni, sulle regole del protocollo e infine sul fatto che la moneta abbia valore. Ottenere tutti e tre i tipi di consenso in modo decentralizzato è molto difficile, ma prima di capire come questo avviene verranno forniti degli esempi e alcune definizioni teoriche, in modo da avere un quadro generale riguardante il concetto del consenso distribuito.

Si considerino n nodi che hanno ciascuno un valore in input, si consideri anche la presenza di possibili nodi difettosi o dannosi. In generale, si dice che un protocollo di consenso distribuito debba rispettare 2 proprietà fondamentali:

1. Deve terminare con tutti i nodi *onesti* in accordo sul valore;
2. Il valore deve essere stato generato da un nodo onesto.

Il rispetto di queste proprietà non è una cosa facile. In primo luogo, il consenso è un problema difficile poiché i nodi potrebbero bloccarsi o essere assolutamente dannosi. In secondo luogo, e in particolare nel contesto Bitcoin, la rete è altamente imperfetta. Si parla di un sistema peer-to-peer e non tutte le coppie di nodi sono collegate tra loro. Potrebbero esserci guasti nella rete, ad esempio a causa della scarsa connettività, e quindi non è possibile eseguire un protocollo di consenso a cui devono partecipare tutti i nodi. Infine, c'è la presenza di latenza nel sistema dovuta alla distribuzione su Internet.

Dunque, il protocollo Bitcoin deve raggiungere il consenso di fronte a due tipi di ostacoli: imperfezioni nella rete, come la latenza e il crash dei nodi, nonché i tentativi deliberati da parte di alcuni nodi di sovvertire il processo. Una conseguenza particolare di questa elevata latenza è che non esiste la nozione di tempo globale. La mancanza di tempo globale limita fortemente l'insieme di algoritmi che possono essere utilizzati nei protocolli di consenso. A causa di questi vincoli gran parte della letteratura sul consenso distribuito è alquanto pessimista e sono stati dimostrati molti risultati di impossibilità. Il più noto riguarda il **problema dei generali bizantini** (o Byzantine Generals Problem), un esempio schematico viene riportato in Figura 3.1.

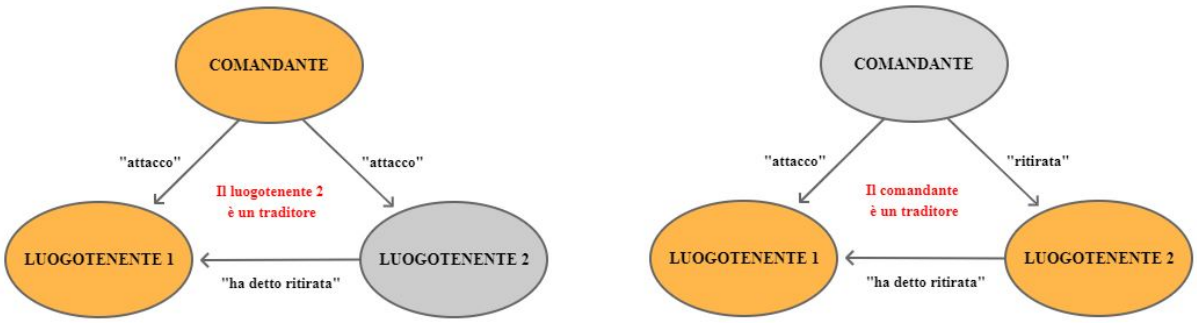

Figura 3.2: Il problema dei Generali Bizantini

Questo problema prevede che un gruppo di generali, ciascuno al comando di una porzione dell'esercito, circondi una città. I generali devono decidere se attaccare o ritirarsi. L'importante non è la decisione finale in sé ma raggiungere un consenso unanime affinché tutti i generali possano dar seguito ad una decisione in modo coordinato.

È stato dimostrato, che se uno o più generali, o uno o più luogotenenti, si dimostrano dei traditori non è possibile raggiungere il consenso all'unanimità, in quanto, verrebbero comunicati ordini contrastanti creando così scompiglio tra le truppe che a quel punto non saprebbero più se attaccare o ritirarsi, o addirittura, alcune potrebbero decidere di attaccare mentre altre di ritirarsi.

Provando ad applicare il problema dei generali bizantini nel contesto Bitcoin, si può affermare che ogni generale rappresenta un nodo della rete dotato di potere decisionale ed il piano di attaccare o ritirarsi rappresenta la singola decisione che i nodi dotati di potere decisionale devono adottare in merito alla validazione o meno del blocco creato. Per risolvere i problemi legati al raggiungimento del consenso Bitcoin fa uso del protocollo "Proof of work" (prova di lavoro), descritto più avanti, e sfrutta anche la nozione di casualità, cioè la scelta dei nodi in maniera casuale con una certa probabilità (non troppo bassa) di selezionare un nodo in buona fede.

Bisogna tener presente che i nodi Bitcoin non hanno identità persistenti a lungo termine. Questa è un'altra differenza rispetto ai tradizionali algoritmi di consenso distribuito. Una delle ragioni di questa mancanza d'identità è che trattandosi di un sistema decentralizzato, Bitcoin, non presenta un'autorità centrale in grado di definire l'identità ai partecipanti e verificare che non stiano creando nuovi nodi a volontà. Per queste ragioni è necessario prevenire gli attacchi di tipo Sybil, le cui peculiarità verranno descritte nella prossima sezione.

3.3.1 Attacco Sybil

Un **Attacco Sybil** è un problema molto comune di informatica, in cui un utente malintenzionato si infiltra nella rete creando più identità false per far sembrare che ci siano molti partecipanti diversi, quando in realtà tutti i falsi nodi sono realmente controllati dallo stesso avversario. Questo è un tipo di attacco da non sottovalutare nel protocollo Bitcoin, poiché tra le sue caratteriste vige la regola dell'anonimato, dunque, la mancanza d'identità introduce un'ulteriore difficoltà per il raggiungimento del consenso.

Si può compensare la mancanza d'identità ricorrendo, come già detto, alla scelta casuale dei nodi. Si supponga per il momento che esista un modo per effettuare questa selezione (in seguito verranno descritte le tecniche utilizzate per questo scopo). L'ipotesi di selezione casuale dei nodi rende possibile ciò che si definisce **consenso implicito**, cioè non esiste alcun algoritmo di consenso e nessuna votazione, semplicemente il nodo scelto propone quale sarà il blocco successivo nella catena. Gli altri nodi accetteranno o rifiuteranno implicitamente quel blocco. In caso di accettazione segnaleranno la cosa aggiungendo quest'ultimo blocco alla catena, altrimenti, estenderanno la catena ignorando quel blocco e partendo da qualunque fosse il precedente ultimo blocco nella catena. Questo è il meccanismo tecnico che consente ai nodi di segnalare quali blocchi sono stati aggiunti e qual è la catena che si sta estendendo.

Questo processo è molto semplificato perché si basa sull'ipotesi che esista un modo per selezionare un nodo in maniera casuale, ma tranne che per questa semplificazione, è abbastanza vicino a come funziona effettivamente Bitcoin. In generale, un blocco viene accettato se tutte le transazioni in esso contenute sono ritenute valide. Affiché una transazione venga considerata valida deve ottenere delle **conferme**, più il numero di conferme è grande maggiore sarà la probabilità che finisca nella catena dei blocchi. Se una transazione ha ricevuto k conferme, la probabilità che si verifichi il fenomeno della doppia spesa scende esponenzialmente in funzione di k. L'euristica più comune utilizzata nell'ecosistema Bitcoin è attendere sei conferme. Non c'è una reale motivazione sulla scelta di questo numero, semplicemente viene considerato un buon compromesso tra il tempo di attesa e la garanzia che la transazione finisca nella catena.

Se un nodo tenta di includere una transazione non valida, l'unica ragione per cui questa non finirà nella catena del consenso è che si considera l'onestà della maggior parte dei nodi, i quali impediranno l'inclusione di una transazione non valida. A questo punto una domanda sorge spontanea: *esiste un modo per garantire l'onestà dei nodi?*. Nel protocollo Bitcoin si è pensato di ricorrere a degli incentivi per indurre i nodi ad essere onesti. Questo argomento verrà discusso nella prossima sezione.

3.4 Incentivi

Lo scopo degli **incentivi** è quello di premiare i nodi che hanno creato i blocchi per motivarli a continuare il loro lavoro e i loro sforzi, utizzando gli stessi bitcoin come premio. Esistono 2 tipi di incentivi:

1. **Block Reward (o ricompensa del blocco)**
   Il nodo che crea un blocco deve includere una transazione speciale all'interno dello stesso, cioè una transazione che conia una nuova moneta. Il nodo può scegliere l'indirizzo del destinatario di questa transazione, ovvero, sceglie sostanzialmente a chi attribuire la moneta (tipicamente a se stesso). Il valore di questa moneta viene dimezzato ad intervalli regolari, per la precisione ogni 210.000 blocchi, che corrispondono all'incirca a 4 anni. Questo processo viene definito **halving** e induce a pensare che la somma delle ricompense abbia un valore finito, infatti, dalla sua nascita Bitcoin andrà incontro a 32 halving, completato l'ultimo dei quali non verranno emessi più nuovi bitcoin poiché sarà raggiunta la quantità massima circolante ammessa e stabilita dall'algoritmo, e cioè 21 milioni di BTC. In Figura 3.3 viene riportato l'andamento della curva di dimezzamento.

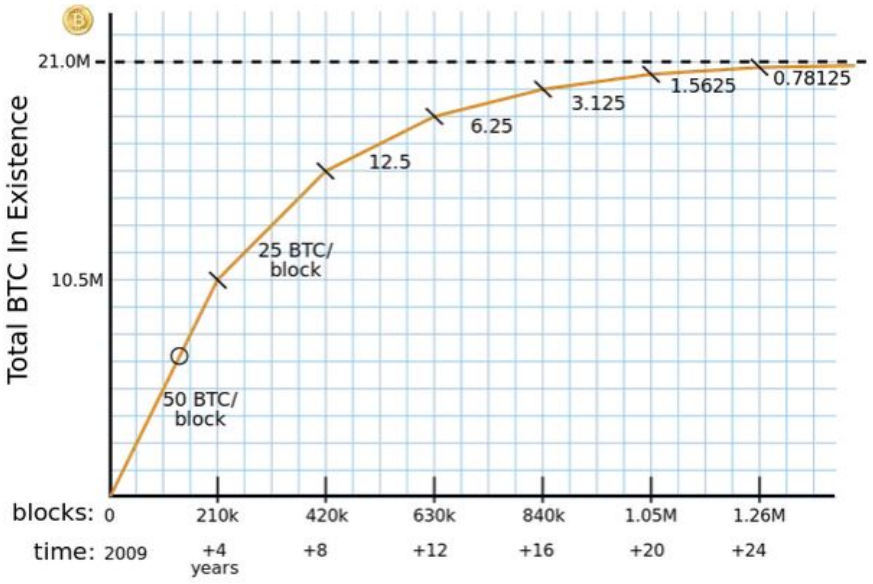

Figura 3.3: Curva di dimezzamento ricompensa dei blocchi Bitcoin

Il primo halving di Bitcoin è avvenuto il 28 novembre del 2012, portando la ricompensa dai 50BTC originari a 25BTC. Il 9 luglio 2016 avviene il secondo halving, con il passaggio da 25BTC a 12,5BTC. Il terzo halving di Bitcoin, considerando il periodo di riferimento della stesura di questo documento, è avvenuto di recente, esattamente l'11 maggio 2020, con il valore della ricompensa che passa da 12,5BTC a 6,25BTC. Convertendolo, il premio stimato si aggira intorno ai 54 mila dollari.

Seguendo questa logica può sembrare che il nodo ottenga la ricompensa indipendentemente dal fatto che proponga un blocco valido o si comporti in modo malizioso, ma non è così. Infatti, il nodo riuscirà ad ottenere la ricompensa solo se il blocco in questione verrà inserito nella catena dei consensi, esattamente come avviene per il resto delle transazioni. Si tratta di un trucco molto sottile ma efficace, poiché incoraggia i nodi a comportarsi in maniera leale seguendo le regole, anche perché in caso contrario non riceverebbero alcuna ricompensa. Questo è il primo meccanismo di incentivazione di Bitcoin.

È importante notare che questo è l'unico modo in cui è consentito creare nuovi bitcoin. Non esiste un altro meccanismo per farlo ed è per questo che 21 milioni è un numero finale e totale di bitcoin che potranno mai esserci. Per come stanno adesso le cose, questa ricompensa si esaurirà nel 2140, ma ciò non vuol dire che il sistema smetterà di funzionare in quell'anno o che diventerà insicuro. Infatti, esiste un altro tipo di incentivo, che è quello descritto di seguito.

2. **Transaction Fees (o Commissioni di transazione)**
   Un nodo che effettua una transazione può destinare parte dell'output al ricevente aggiungendo al suo interno una Transaction Fee. Non si tratta di una commissione fissata dalla rete e il funzionamento del sistema non è condizionato da essa, come invece accade per la Block Reward. Si tratta di una sorta di "mancia" che viene data al nodo per far sì che questo lavori. Il problema è che il blocco da aggiungere alla catena ha dimensione limitata, se quindi la mancia concessa è troppo bassa o addirittura zero, i nodi assegneranno alla transazione una priorità talmente bassa che, in pratica, non verrà mai inserita nella blockchain.

Quindi si può dire che i nodi prenderanno in considerazione solo le transazioni con commissioni elevate. Al momento questo meccanismo è poco utilizzato, ma considerando che la Block Reward diminuisce col tempo, questo incentivo acquisterà sempre più importanza. Se così non fosse i nodi perderebbero interesse nelle loro attività e la rete perderebbe potenza. In poche parole, l'intero sistema collasserebbe.

Gli incentivi sono, dunque, utili per garantire l'onestà dei nodi, lo stesso non si può dire per problemi menzionati all'inizio, riguardanti l'attacco Sybil e la scelta dei nodi in maniera casuale. Questi problemi sono correlati e per capire come sono stati risolti è necessario comprendere il concetto di mining e il funzionamento della prova di lavoro. Approfondimenti in merito verranno fortini nella prossima sezione.

3.5 Mining e Proof of work

L'idea chiave del **Proof-of-work (PoW)** (o prova di lavoro) è che la selezione casuale di un nodo è proporzionale alla quantità di risorse che esso spende, o meglio, alla potenza di calcolo di cui necessita per risolvere complessi algoritmi matematici, conosciuti come **hash-puzzle**. Per creare un blocco, il nodo deve trovare un numero, detto **nonce** (*number once used*, cioè letteralmente "numero usato una volta"), e produrre un hash del blocco tramite un doppio hashing. Detto in modo più semplice, questo numero concatenato con altri componenti dell'header di un blocco sarà l'input di una funzione hash, il valore restituito in output non deve superare un certo target di difficoltà affiché il blocco venga considerato valido. Il tutto si può esprimere mediante la seguente disuguaglianza:

$$H(nonce \| prev\_hash \| tx \| tx \| ... \| tx) < target$$

Il codice hash in output dovrà contenere un certo numero di zeri, consecutivi e iniziali, che sia almeno uguale al grado di difficoltà richiesto. Quest'ultimo è rappresentato dal campo *nBit* presente all'interno dell'header del blocco. Per fare un esempio, se il target è settato a 6, l'hash accettabile per la validazione del nodo dovrebbe essere simile al seguente:

```
0000006c872dc19c4b6dc990b7158ace7d17b4e8ffb75d08493d9656d226fb64e8ecd2
```

Il nonce è l'unico parametro dell'header che può essere modificato e solitamente è inizializzato a 0. Tutte le volte che l'hash del blocco ottenuto si discosta dal valore target il nonce viene incrementato e il procedimento si ripete finché non si trova un valore hash compatibile. Non esiste una tecnica o un calcolo per trovare un nonce valido, l'unico modo logico per farlo è tramite numerosi tentativi casuali, sperando di essere fortunati prima degli altri.

Se un nodo trova una soluzione fornisce il "risultato" agli altri nodi per provare che il lavoro svolto sia corretto (proof-of-work). A questo punto gli altri nodi verificano che la disuguaglianza, sopra citata, sia soddisfatta e in tal caso il blocco viene validato ufficialmente. In seguito, viene inserito nella catena di blocchi e il nodo che ha trovato la soluzione viene ricompensato con l'immissione di nuovi bitcoin e con tutte le commissioni delle transazioni contenute all'interno del blocco validato.

Il tempo necessario per la validazione di un blocco dipende puramente dal grado di difficoltà impostato per la ricerca del nonce. Tale difficoltà è legata al numero di zeri presenti davanti all'hash del blocco ma si può dire che, in media, la verifica avviene ogni 10 minuti. Questa tempistica non è casuale poiché l'algoritmo Bitcoin è stato programmato per fare in modo che, ogni 2 settimane, il grado di difficoltà venga "aggiustato" in funzione della potenza di calcolo di tutti i nodi che stanno partecipando al processo di validazione. Più la potenza di calcolo totale è alta e più viene aumentata la difficoltà, così da mantenere la media di 10 minuti.

Questa nozione di hash-puzzle e proof of work elimina completamente la necessità di scegliere un nodo casuale. I nodi sono costantemente in competizione tra loro, al fine di risolvere questi puzzle. Di tanto in tanto, uno di loro avrà fortuna e troverà un nonce casuale che soddisfi la proprietà. In questo modo, il sistema risulta essere completamente decentralizzato, in quanto, non necessita della presenza di qualcuno che decida chi debba essere a proporre il blocco successivo. Quel qualcuno sarà semplicemente il nodo più fortunato. Questo processo, inoltre, rende moderatamente difficile creare nuove identità e, dunque, rende il sistema resistente agli attacchi Sybil.

Riassumendo gli hash-puzzle, affiché il processo funzioni, devono rispettare 3 proprietà fondamentali:

1. **Difficoltà di calcolo**: più l'hash-puzzle è difficile da calcolare meno probabilità ci sono di subire degli attacchi. Questo, però, rende praticamente impossibile la risoluzione del problema ad una persona che possiede un computer di base, considerando anche il fatto che con l'aumentare della bravura dei nodi viene aumentato anche il livello di difficoltà;

2. **Costo parametrizzabile**: la volontà di avere un costo parametrizzabile è il motivo per il quale il target viene riaggiornato periodicamente, in modo tale che il tempo medio di aggiunta di blocchi alla catena sia di circa 10 minuti;

3. **Banale da verificare**: deve essere banale verificare che un nodo abbia calcolato correttamente la prova di lavoro poiché, questa proprietà, consente di sbarazzarsi della centralizzazione. Infatti, dimostra che non è necessaria alcuna autorità centralizzata che verifichi che i nodi stiano facendo il loro lavoro correttamente. Qualsiasi nodo può verificare istantaneamente che un blocco trovato da un altro nodo soddisfi questa proprietà.

Il processo di verifica e l'aggiunga dei blocchi alla blockchain è conosciuto con il nome di **mining** [MGT18] che letteralmente significa "estrazione", perché viene paragonato a quanto accade nelle miniere con gli estrattori d'oro. Infatti, i nodi che partecipano a questo processo sono definiti **miner**, che significa "minatori", in quanto consentono "l'estrazione" di nuovi bitcoin. I minatori, dunque, svolgono il duplice ruolo di verifica delle transazioni e di emissione dei bitcoin. Se la potenza di calcolo a disposizione di un miner non fosse sufficiente per la risoluzione del puzzle, questo ha la possibilità di unirsi ad una **mining pool**, cioè ad un gruppo di miner, con lo scopo di competere con i nodi più potenti della rete per riuscire a risolvere quanto prima l'enigma dell'hash-puzzle.

Potrebbe capitare che due miner con lo stesso parent block trovino quasi simultaneamente due soluzioni valide, anche se diverse, per l'hash-puzzle. Questo provocherebbe la biforcazione della catena, il cui termine tecnico è **fork**, che verrà discussa nella prossima sezione.

3.6 Fork

Una **fork** è una temporanea inconsistenza della rete Bitcon che si risolve dopo un certo numero di blocchi. Questa è dovuta al fatto che due miner riescono a risolvere quasi contemporaneamente la PoW, cioè la soluzione all'hash-puzzle. Una biforcazione si verifica più o meno nel modo seguente: un nodo riceve un blocco valido e lo aggiunge alla propria blockchain estendendola di un'unità, dopo poco tempo riceve un secondo nodo ma si accorge che è figlio dello stesso padre del nodo precedente, a quel punto aggiunge il nodo ad una catena secondaria. Dunque, la catena di blocchi viene divisa in due rami e per un breve periodo di tempo esisteranno due versioni, valide e parallele, della blockchain.

Quello che succede è che al momento alcuni nodi considerano valida la prima catena e altri la seconda, quindi è necessario sfruttare il meccanismo di consenso per decidere quale delle due sarà la principale e quale dovrà essere scartata. In questo caso, il meccanismo consiste nel creare nuovi blocchi successivi, sfruttando tutta la potenza di calcolo. La catena che si estenderà più velocemente diventerà ufficiale e comune a tutti i nodi, mentre, l'altro ramo sarà lasciato "**orfano**" e tutte le transazioni al suo interno, se considerate valide, torneranno ad essere disponibili nel *memory pool*, altrimenti verranno scartate. Il memory pool è semplicemente una raccolta di transazioni che sono state verificate ma non sono ancora state aggiunte alla blockchain.

Esiste un altro scenario in cui la rete Bitcoin può generare dei fork e verrà descritto nella prossima sezione.

3.6.1 Soft Fork e Hard Fork

Come succede in tutti i sistemi informatici o nelle varie applicazioni mobile presenti in commercio, è necessario talvolta effettuare degli aggiornamenti del sistema, per risolvere alcuni bug o semplicemente aggiungere delle nuove funzionalità. Lo stesso accade nel protocollo Bitcoin, quindi, una fork si può verificare quando è necessario apportare dei cambiamenti alle regole di consenso.

Esistono due tipologie di variazione del protocollo di consenso:

1. **Sorf Fork**
   In Figura 3.4 è riportata la rappresentazione della variazione di tipo Soft Fork.

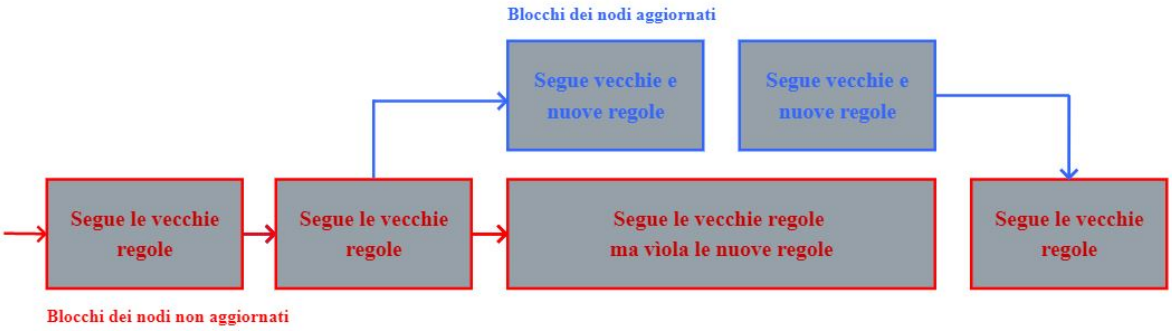

Figura 3.4: Soft Fork

   Un Soft Fork si verifica quando le modifiche al protocollo sono retro-compatibili, vale a dire che non vengono apportati cambiamenti alle regole già esistenti, ma si introducono delle restrizioni.

   Di conseguenza, un blocco che si basa sulle nuove regole viene accettato anche dai nodi non aggiornati, mentre, un blocco che si basa sulle vecchie regole viene rifiutato dai nodi aggiornati. Come per il caso spiegato in precedenza, anche in questo tipo di fork si creano due rami della catena e i nodi devono decidere quale accettare.

   Non c'è nessuna imposizione sul fatto di dover per forza aggiornare la propria versione della Blockchain, infatti, è possibile continuare ad operare come sempre, tenendo a mente, però, che si sta andando contro il nuovo protocollo. Ad ogni modo, se la maggioranza dei nodi deciderà di considerare come catena principale quella con le nuove regole allora il protocollo effettuerà un aggiornamento.

2. **Hard Fork**
   In Figura 3.4 è riportata la rappresentazione della variazione di tipo Hard Fork.

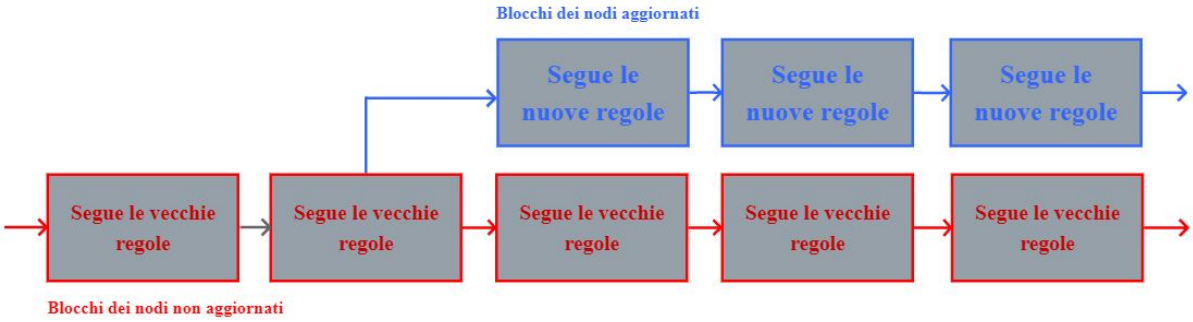

Figura 3.5: Hard Fork

La retro-compatibilità non vale per il caso Hard Fork. Viene comunque creata una diramazione ma in questo caso si formano due catene principali indipendenti. I nodi che accetteranno le nuove regole non potranno più fare riferimento a quelle vecchie.

A seguito di un Hard Fork la vecchia versione di una Blockchain e la nuova si separano completamente, senza alcuna comunicazione o opzione di transazione tra le due. Solitamente la nuova versione eredita la cronologia delle transazioni della vecchia, dopodiché le due varianti continueranno ad operare in maniera del tutto indipendente.

Bisogna precisare che questo tipo di fork è decisamente meno frequente rispetto al precedente menzionato. Si sceglie questo approccio solo nel caso in cui si vogliano apportare delle modifiche importanti alle regole del consenso. Un esempio molto noto di Hard Fork è **Bitcoin Cash**, che si verificò l'1 agosto 2017. Fu una sorta di scisma tra i team che sviluppavano Bitcoin in quel periodo, ma di questo si discuterà meglio in seguito.

Dopo aver analizzato ampiamente le caratteristiche tecniche di Bitcoin e il funzionamento del suo protocollo è arrivato il momento di fare il punto su quelli che sono i vantaggi e gli svantaggi, derivati dall'uso dello stesso. Il tutto verrà affrontato nella prossima sezione.

3.7 Vantaggi e Svantaggi

L'infrastruttura di Bitcoin, come è ovvio che sia, presenta una serie di vantaggi e svantaggi. Di seguito viene fornita la lista dei **vantaggi** principali:

- **Trasparenza**
  Ogni singola transazione viene registrata ed archiviata all'interno della Blockchain, quindi, chiunque è in grado seguire la crescita della catena di blocco e verificare le transazioni. Ogni transazione è cifrata ma grazie alla presenza delle firme digitali è possibile tracciarle.

- **Velocità delle transazioni**
  Tipicamente una banca impiega un paio di giorni per approvare una transazione, se la somma di denaro è considerevole. Con Bitcoin, invece i pagamenti vengono processati in maniera quasi istantanea. Sono necessari pochi minuti per spedire il proprio denaro ad un altro utente, indipendentemente dalla distanza geografica.

- **Riduzione delle spese di transazione**
  Le commissioni sono molto esigue, rispetto a strumenti di pagamento tradizionali come carte di credito o bonifici, e si aggirano in media intorno a 0,0001 BTC, l'equivalente di pochi centesimi di euro.

- **Non rifiutabilità**
  Una volta che i Bitcoin sono stati spesi, non è più possibile riottenerli, a meno che il destinatario non decida di spedirli nuovamente al mittente. Questo assicura la ricezione del pagamento e l'impossibilità di truffare qualcuno affermando di non aver ricevuto il denaro.

- **Anonimato**
  Al contrario di una banca che conosce ogni singolo dettaglio dei propri clienti (cronologia dei movimenti, indirizzi, numeri di telefono, ecc.), Bitcoin consente agli utenti di rimanere del tutto anonimi. Come detto in precedenza, le transazioni sono tracciabili, in quanto contengono l'indirizzo da cui sono stati inviati i bitcoin e l'indirizzo di destinazione, ma oltre a questi dati non ci sono altre informazioni che potrebbero ricondurre al vero proprietario del denaro.

- **Decentralizzazione**
  La rete è totalmente indipendente da qualsiasi autorità governativa e gli utenti possono comunicare in maniera diretta senza la necessità di intermediari. Vi è una sorta di autogestione in cui i partecipanti alla rete, seguendo le regole del protocollo, possono verificare la correttezza delle transazioni. Il funzionamento è garantito dalla fiducia e dal consenso, raggiunti tramite degli algoritmi informatici ben consolidati e sicuri. In questo modo, anche se parte del network venisse disattivato, il denaro continuerebbe a muoversi.

- **Nessuna contraffazione**
  Grazie al meccanismo del consenso e alla tecnologia Blockchain, Bitcoin, è in grado di contrastare possibili attacchi volti alla contraffazione dei dati. Tra i più noti vi è sicuramente il problema della doppia spesa, cioè del tentativo di spendere due o più volte del denaro già speso.

Nonostante la lista dei vantaggi sia molto ampia vi è, purtroppo, anche la presenza di alcuni **svantaggi**. Di seguito un elenco:

- **Volatilità**
  Il prezzo dei bitcoin è imprevedibile e potrebbe aumentare o diminuire in un breve periodo di tempo, tanto che alcuni lo considerano una semplice bolla finanziaria pronta ad esplodere. Il suo valore è imprevedibile, può cambiare drasticamente e molto velocemente: gli investitori più imprudenti possono andare incontro ad ingenti danni economici.

- **Impatto ambientale dovuto all'attività di mining**
  Il processo di estrazione di bitcoin richiede molta potenza di calcolo, di risorse energetiche e necessita di computer potenti per poter sostenere la prova di lavoro. Lo spreco di così tanta energia può avere impatti notevoli sull'ambiente ma questo specifico argomento verrà ampiamente discusso in seguito. In anticipo si può dire che i principali miner si trovano in paesi come la Cina, dove viene usato il carbone per produrre elettricità, e a seguito del processo di mining si è riscontrato un aumento notevole dell'impronta di carbonio.

- **Uso illecito e riciclaggio**
  Il fatto di garantire l'anonimato rende Bitcoin vulnerabile da un certo punto di vista. Infatti, potrebbe essere utilizzato per scopi illeciti, come attività criminali o riciclaggio di denaro. La condizione giuridica del Bitcoin varia drasticamente da paese in paese e in alcuni stati il suo utilizzo è stato bandito e dichiarato illegale.

- **Perdita delle chiavi**
  Una chiave è un codice alfanumerico necessario per accedere ad un portafoglio Bitcoin e perderla significherebbe perdere il portafoglio stesso. Fortunatamente esistono dei meccanismi di backup o ripristino, a patto che però l'utente li abbia configurati per tempo.

- **Irreversibilità delle transazioni**
  Come già detto, una volta che una transazione viene processata e registrata nella blockchain, non è più possibile annullarla. Se si utilizza Bitcoin come mezzo di pagamento, questo meccanismo tutelerà il commerciante dalla possibilità che il pagamento venga annullato, ma non il consumatore, che potrebbe aver autorizzato per sbaglio una transazione o potrebbe ricevere della merce difettosa, nel caso pessimo, potrebbe addirittura non ricevere nulla.

- **Regolamentazione**
  La situazione legale di Bitcoin non è omogenea e le regole variano da paese in paese. Gran parte delle giurisdizioni del mondo non hanno ancora conferito corso legale a Bitcoin, ma alcune autorità fiscali hanno riconosciuto la sua importanza e proposto alcune normative a riguardo.

- **Sviluppo continuo**
  Il futuro della valuta non è ancora chiaro. La misteriosa entità che ha introdotto i bitcoin ha deciso di lasciare, nel 2010, l'intera rete nelle mani di alcuni membri stimabili della comunità. Questo è il motivo per il quale il software è in fase beta e ci sono funzionalità che devono ancora essere sviluppate.

Dopo avere analizzato i principali aspetti positivi e negativi del protocollo Bitcoin, è interessante fare un confronto con altre famose criptovalute, le quali, vengono definite Altcoins poiché nate dopo la scoperta di Bitcoin. I dettagli nella prossima sezione.

3.8 Bitcoin vs Altcoins

Il nome **altcoin** deriva dall'unione di due parole: "*alt*", che è l'abbreviazione del termine "alternativa", e "*coin*", che si riferisce alle "criptovalute". Per "altcoin" si intendono, dunque, tutte le monete alternative a Bitcoin, nate dopo la sua scoperta con l'intento di provare a sostituirlo o a correggere alcune sue problematiche. Nonostante Bitcoin sia stata la prima criptovaluta ad emergere e sia tuttora la più nota, è solamente una tra le migliaia di criptovalute che esistono attualmente, delle quali molte si basano sulla struttura di Bitcoin. Di seguito verrà fornito un elenco delle principiali altoin in commercio:

- **Ethereum**
  Ethereum è una blockchain programmabile che utilizza un linguaggio programmazione "turing-completo"[2], cioè un modello di calcolo che ha lo stesso potere computazionale di una macchina di Turing. Questo non solo mette a disposizione degli utenti delle funzioni predefinite, come le transazioni Bitcoin, ma permette loro di crearne delle proprie. Ethereum è stato progettato per essere flessibile, versatile e per adattarsi alla creazione di diverse tipologie di applicazioni. Sì tratta di un'applicazione decentralizzata che fa con le applicazioni quello che Bitcoin fa con i soldi, ovvero elimina la necessità di avere intermediari.

  Per regolare le transazioni vengono utilizzati degli **smart contracts**, cioè dei veri e propri contratti, scritti tramite codice di programmazione, che seguono regole ben precise. Si definiscono "contratti intelligenti", in quanto sono in grado di verificare se determinate condizioni, definite nel contratto stesso, sono avvenute realmente, inoltre sono in grado di eseguirsi automaticamente nel momento in cui tali condizioni si sono verificate. La criptovaluta utilizzata prende il nome di **Ether**.

[2]https://en.wikipedia.org/wiki/Turing_completeness

- **Ripple**
  Ripple è un protocollo per transazioni finanziarie e permette a chiunque di trasferire denaro in valuta tradizionale o digitale. Ogni utente può aprire delle linee di credito verso altri utenti e il tutto si basa sulla fiducia che un utente ripone in un altro, la quale viene espressa dalla quantità di denaro che i vari utenti sono disposti a prestare. Ripple permette, dunque, il trasferimento e il ritiro di denaro presso altri utenti che fungono da banche. Inoltre, la sua flessibilità permette di utilizzare ogni tipo di valuta, anche inventata, creando una rete di fiducia tra le persone che l'accettano.

  Ripple possiede anche una propria valuta, chiamata **XRP**, che è stata creata e gestita da un'unica società, ovvero Ripple stessa, pertanto, al contrario di Bitcoin, risulta essere una criptovaluta centralizzata. Il protocollo Ripple nasce per risolvere alcuni problemi collegati alle transazioni, come ad esempio la lentezza e i costi di commissione. XRP è una Criptovaluta pre-minata e viene rilasciata sul mercato secondo la politica monetaria di Ripple. Per fare ciò i bilanci degli utenti vengono gestiti tramite un registro distribuito simile alla blockchain, chiamato ledger, all'interno del quale ogni nodo mantiene una copia dell'ultimo ledger valido.

  Il processo per il raggiungimento del consenso è molto diverso dal proof-of-work di Bitcoin. Ogni client possiede, infatti, una lista di nodi affidabili, chiamata **UNL** (Unique Node List). Ogni nodo propone le modifiche che vuole apportare al registro agli altri nodi, i quali decidono di accettarle solo se provengono da un nodo presente nella propria UNL. Quando la maggioranza dei nodi accetta le modifiche queste vengono incluse nell'ultimo registro valido. Dunque, non essendo presente un processo di mining il tutto è più veloce e meno dispendioso. Non è chiaro come venga garantita la sicurezza delle transazioni, ma trattandosi di un sistema in fase di sviluppo ci sarà modo di testarlo e capire quanto esso sia sicuro.

- **Litecoin**
  Litecoin è una criptovaluta open-source basata su una rete peer-to-peer e nasce con lo scopo di migliorare alcuni aspetti di Bitcoin, pur essendo molto simile.

Tutte le transazioni vengono salvate sulla Blockchain Litecoin e, per garantirne consistenza e sicurezza, si sfruttano le stesse tecniche crittografiche del protocollo Bitcoin. La rete Litecoin prevede l'aggiunta di un blocco alla catena ogni 2,5 minuti, a fronte dei 10 minuti previsti nella rete Bitcoin. In questo modo, viene velocizzato il processo di conferma delle transazioni andando, però, incontro ad un aumento sia della lunghezza della Blockchain sia del numero di blocchi orfani. In questo processo, una transazione viene confermata dopo 15 minuti, a seguito di 6 conferme, e non dopo 1 ora come previsto dal protocollo Bitcoin. D'altra parte l'algoritmo di Proof-of-Work risulta più complesso, poiché il processo di mining dei blocchi richiede molto più tempo e l'utilizzo di hardware più sofisticato, ma il numero complessivo di Litecoin che potranno essere creati è pari a 84.000.000, cioè il quadruplo delle monete messe a disposizione dal protocollo Bitcoin.

- **Bitcoin Cash**

  Bitcoin Cash, già citato in precedenza, nasce l'1 Agosto 2017, a seguito di una fork della Blockchain Bitcoin. Quello che ha portato alla creazione di questa nuova valuta è stata una sorta di scissione all'interno della comunità di Bitcoin, infatti, il 20 luglio 2017 era stato proposto un miglioramento del protocollo per risolvere il problema della scalabilità, ma questo comportava l'aumento della dimensione dei blocchi e dunque la proposta venne rifiutata. Questo gruppo di persone ha quindi espresso l'intenzione di implementare un hard fork della criptovaluta Bitcoin, originando Bitcoin Cash. La blockchain ha ereditato la cronologia delle transazioni del network Bitcoin in quella data, ma le successive transazioni sono registrate su una blockchain diversa. Le novità introdotte sono state dunque:

  - Velocità delle transazioni, con un numero maggiore di transazioni al secondo;
  - Maggiore affidabilità della rete che è meno soggetta a congestioni;
  - Aumento della dimensione dei blocco da 1MB a 8MB;
  - Riduzione del costo delle transaction fee;
  - Introduzione di un nuovo formato di firma digitale per una maggiore sicurezza dei wallet.

Queste sono solo le più note criptovalute alternative che hanno anche sviluppano delle idee per risolvere i problemi di scalabilità di cui soffre Bitcoin, ma di questo si parlerà ampiamente nei prossimi capitoli. Nello specifico, si andranno ad analizzare anche i pericoli che possono essere causati sull'ambiente dalla quantità di risorse energetiche di cui necessita il meccanismo proof-of-work per poter funzionare.

Capitolo 4

Impatto Ambientale del PoW

Dalle analisi fatte nei capitoli precedenti è emerso che il protocollo Bitcoin si è dimostrato essere molto sicuro e resistente agli attacchi, ma come preannunciato, soffre di alcune problematiche. La debolezza principale è legata all'algoritmo proof-of-work che per sua natura comporta un'elevato consumo di risorse energetiche, necessarie al suo funzionamento. Come emerso da alcune discussioni susseguitesi nel corso degli anni ([Shi16], [Ast16], [LS19]), questo rappresenta un punto debole in grado di limitare la scalabilità delle blockchain basate sul PoW. Inoltre, l'impiego di così tante energie causa dei problemi ambientali che, secondo delle stime fatte, a lungo andare potrebbero soltanto peggiorare provocando seri danni all'ambiente. In questo capitolo si parlerà di questi due aspetti, partendo da quelle che sono state le proposte emerse per risolvere il problema della scalabilità di Bitcoin e che verranno descritte nella prossima sezione.

4.1 Scalabilità

Il futuro incerto di Bitcoin è legato in primo luogo ai limiti di scalabilità, ovvero la capacità del sistema di adattarsi ad un aumento del carico di lavoro. In particolare, i problemi di scalabilità di Bitcoin riguardano sostanzialmente il PoW, il cui aspetto negativo è legato ad una quantità molto elevata di energia necessaria al suo funzionamento e alla protezione della rete. Il problema diventa ancora più grande all'aumentare del numero di utenti che effettuano le transazioni sulla blockchain.

Poiché la competizione per risolvere l'algoritmo è maggiore sarà necessaria anche una maggiore potenza di calcolo per vincere la competizione, con il conseguente aumento dell'energia utilizzata. Ciò dipende principalmente da due fattori: il tempo di mining e la dimensione di un blocco.

Ricordando quanto detto in precedenza, il tempo di mining è di 10 minuti e la dimensione massima di un blocco è di 1 MB, ciò significa che la rete può sostenere al massimo circa 7 transazioni al secondo, ma il problema è che con l'aumentare delle transazioni la velocità con cui vengono confermate rimane costante. Abbassando il tempo di mining il processo risulterebbe più veloce ma questo renderebbe il sistema più inconsistente per via dei numerosi fork che si potrebbero creare e, inoltre, aumenterebbero le vulnerabilità aprendo la strada ad eventuali attacchi. Anche l'aumento della dimensione dei blocchi può introdurre delle difficoltà, come l'incremento della dimensione della blockchain. Molti nodi potrebbero non essere in grado di gestirla nella sua totalità e in completa autonomia, ciò significherebbe perdere la decentralizzazione dei nodi. Per queste ragioni gli sviluppatori di Bitcoin non intendono procedere in questo senso.

Nel corso degli anni sono state proposte diverse soluzioni per risolvere questi problemi di scalabilità, la prima che verrà analizzata rappresenta un'alternativa al PoW e prende il nome di Proof of Stake. I dettagli verranno forniti nella prossima sezione.

4.1.1 Proof of Stake

Per risolvere i problemi energetici di cui soffre il PoW è stato sviluppato un metodo alternativo che prende il nome di **Proof-of-Stake (PoS)**, letteralmente "*Prova della posta in gioco*". Il consenso viene raggiunto basandosi sull'ammontare di criptovaluta che i nodi della rete possegono e la presenza dei miner viene sostituita dal concetto di "**validatori**". Questi non usano la potenza di calcolo per confermare i blocchi ma fanno una "scommessa", con i fondi che posseggono, sui blocchi ritenuti validi. Mentre i miner cercavano di accrescere la loro potenza di calcolo per poter risolvere i complessi problemi matematici, i validatori, incrementano la possibilità di essere scelti per la convalida dei blocchi scommettendo più denaro possibile sugli stessi, in pratica, vince chi punta di più.

Nel caso del PoW i miner vengono incentivati con l'emissione di nuove monete, mentre, i validatori ricevono soltanto una percentuale delle commissioni incluse nel blocco, proporzionale all'importo precedentemente investito. L'ammontare di ogni nodo viene "congelato" a titolo di garanzia e in caso di comportamento scorretto il validatore viene punito. A seconda della gravità dell'atto, potrebbe perdere una parte o tutto il proprio ammontare e, inoltre, gli verrebbe precluso il privilegio di future convalide.

Per quanto riguarda l'attacco 51%, citato in precedenza, in questo caso sarebbe ancora più difficile che si verifichi, poiché per farlo un nodo dovrebbe possedere la maggioranza della criptomoneta in circolazione. Infine, si può affermare che la PoS richiede un consumo di energia molto inferiore rispetto alla PoW, poiché non necessita di computer operativi 24 ore su 24 e 7 giorni su 7.

D'altro canto, la PoS presenta anche delle problematiche poiché possiede degli algoritmi molto più complessi in termini di sviluppo e implementazione. Inoltre, un numero eccessivo di validatori potrebbe rallentare la rete, in quanto il tempo necessario per raggiungere il consenso è direttamente proporzionale alla loro quantità.

Proseguendo nell'analisi un'altra soluzione proposta riguarda la *Lightning Network*, che verrà descritta di seguito.

4.1.2 Lightning Network

Una soluzione per la scalabilità basata sulla Lightning Network è stata proposta per la prima volta da Joseph Poon e Thadeus Dryja [PD15] nel 2015. In questo contesto le transazioni non vengono validate dai miners ma lo scambio tra gli utenti avviene su un canale di pagamento, al di fuori della blockchain (off-chain[1]).

[1][ET17] In questo articolo vengono fornite alcune intuizioni per capire come, in un futuro, un maggiore utilizzo di questo approccio consentirebbe di superare i limiti nelle implementazioni blockchain, estendendo le loro funzionalità, e ridurrebbe i costi di utilizzo.

Prima di spiegare il funzionamento di Lightning Network, verrà fatta una piccola digressione per illustrare la differenza fra transazioni on-chain e off-chain [Ken19].

- **Transazione On-Chain**
  Una transazione on-chain, che è semplicemente una normale transazione, deve essere convalidata e autenticata da un numero adeguato di partecipanti alla blockchain. A seguito della registrazione della stessa nel relativo blocco e del processo di validazione, questa si rende irreversibile. Può essere annullata solo dopo che la maggior parte del potere di hashing della rete raggiunge un accordo. In sostanza, ogni passaggio collegato a una transazione on-chain avviene all'interno della blockchain, il cui stato viene modificato per riflettere l'occorrenza e la validità della transazione.

- **Transazione Off-Chain**
  Una transazione off-chain assume valore al di fuori della blockchain, secondo varie modalità. Ad esempio, può esserci un accordo di trasferimento tra le parti che effettuano le transazioni oppure è possibile coinvolgere una terza parte, come un garante, che garantisce di riconoscere la transazione. I processori di pagamento odierni come PayPal lavorano su queste linee. Nella modalità più semplice, due parti possono persino scambiare le loro chiavi private coinvolgendo una quantità fissa di criptovalute. In questo modo, le monete non lasciano mai il portafoglio, ma la valuta riceve un nuovo proprietario off-chain.

  Il vantaggio delle transazioni off-chain è che possono essere eseguite istantaneamente, non hanno commissioni poiché non accade nulla sulla blockchain e nessun miner è tenuto a convalidare e, inoltre, offrono maggiore sicurezza e anonimato ai partecipanti, poiché i dettagli non vengono trasmessi pubblicamente.

Dopo aver compreso il concetto di transazione off-chain è possibile fornire i dettagli del funzionamento di Lightning Network. In pratica, l'idea è che non tutti i pagamenti vengano registrati come transazioni sulla blockchain ma che si sviluppino all'interno di canali privati fra le due parti, noti come *canali di pagamento bidirezionali* (o bidirectional payment channel).

Le uniche transazioni registrate sulla blockchain sono due: quella che serve a creare il canale, in cui le due parti trasferiscono fondi al canale stesso, e quella in cui il canale viene chiuso ed il saldo finale viene redistribuito alle due parti. Si consideri un semplice esempio in cui Alice vuole comprare merce da Bob. Per far ciò, come detto, Alice e Bob devono creare un canale di pagamento. Questo avviene registrando sulla blockchain una transazione nella quale Alice e Bob inviano entrambi un importo stabilito a priori ad un indirizzo a doppia firma (2-2 multisig), ciò significa che lo sblocco dell'output richiede le firme di entrambe le parti. Gli importi depositati non devono necessariamente essere uguali e una delle due parti può anche non depositare nulla.

Si supponga, in questo esempio, che Alice depositi 1 BTC nel canale e Bob 0.5 BTC. Verrà creata e convalidata un transazione, definita *transazione di apertura del canale* (o **funding transaction**), che avrà come input 1 BTC proveniente da Alice e 0.5 BTC provenienti da Bob, e come output 1.5 BTC, che rappresentano il fondo totale, assegnati ad un indirizzo a doppia firma comune alle due parti. Inoltre, Alice e Bob creeranno (e firmeranno) una transazione intermedia (o commitment transaction) in cui i rispettivi saldi vengono restituiti alle due parti, ovvero 1 BTC ad Alice e 0.5 BTC a Bob. Al momento tale transazione, non viene confermata, cioè scritta sulla blockchain, ma viene conservata privatamente dalle due parti.

A questo punto il canale è stato creato ed ha inizio la comunicazione off-chain. Alice effettua un acquisto da Bob di 0.2 BTC. Alice e Bob allora aggiorneranno il saldo sul canale nel seguente modo: 0.8 BTC ad Alice (= 1 - 0.2 BTC) e 0.7 BTC a Bob (= 0.5 + 0.2 BTC). L'aggiornamento avviene creando una nuova commitment transaction che va a sostituire quella precedente, che viene dunque scartata. Quindi i saldi aggiornati da restituire alle due parti sono: 0.8 BTC ad Alice e 0.7 BTC a Bob. Le due parti potranno continuare ad effettuare transazioni fra loro in questo modo, finché non decideranno di chiudere il canale di pagamento. In questo caso la transazione intermedia diverrà una transazione di chiusura del canale che verrà registrata sulla blockchain e i saldi (aggiornati) al suo interno verranno restituiti alle due parti.

È importante precisare che durante questo processo non si stanno scambiando dei bitcoin ma semplicemente si sta aggiornando un registro condiviso. Le uniche occasioni in cui vengono realmente trasferiti dei bitcoin riguardano l'apertura del canale (per "caricare" bitcoin nel wallet a doppia firma) e la chiusura del canale (per redistribuire il saldo finale alle due parti che hanno aperto il canale).

Ma che succede se una delle due parti coinvolte vuol commettere una frode? Cioè, ad esempio, se Bob registra sulla blockchain la precedente transazione in cui a lui sono attribuiti 0.7 BTC anziché 0.5 BTC? Per ovviare a questo problema il protocollo Lightning Network utilizza i **time lock** (o lock temporali), cioè dei meccanismi che consentono di bloccare l'output di una transazione per renderlo non spendibile, sino alla scadenza del tempo definito. Questo è garantito dal fatto che ogni transazione avrà un time lock minore della precedente e quindi sarà trasmissibile prima delle altre.

In questo documento è stata fornita l'idea alla base di Lightning Network, il quale, riassumendo, permette l'apertura di canali off-chain per consentire degli scambi rapidi, a basse commissioni e in numero molto elevato. Inoltre, i pagamenti sarebbero istantanei poiché non sarebbe necessaria la conferma da parte dei miners. Perciò, di fatto, si può dire che l'implementazione di questo Network se presa in considerazione potrebbe risolvere i problemi di scalabilità attualmente presenti in Bitcoin. Nella prossima sezione verrà descritta un'altra delle soluzioni proposte, la Sidechain.

4.1.3 Sidechain

La tecnica delle sidechain è ancora un meccanismo emergente che non si è completamente affermato ma in sostanza una **sidechain** è una blockchain separata ancorata alla sua blockchain madre tramite un canale bidirezionale. Quest'ultimo consente l'interscambiabilità delle risorse e dei dati ad una velocità predeterminata tra la blockchain madre e la sidechain, quindi, si può considerare questo meccanismo parzialmente off-chain. La blockchain originale viene solitamente chiamata "catena principale" e tutte le blockchain aggiuntive vengono chiamate "sidechain".

Un nodo della catena principale deve inviare le sue monete a un indirizzo di uscita, dove verranno bloccate per evitare che vengano spese altrove. Una volta completata la transazione, viene inviata una conferma attraverso le catene, seguita da un periodo di attesa per una maggiore sicurezza. Trascorso il periodo, il numero equivalente di monete viene rilasciato nella sidechain, consentendo al nodo di accedervi e di spenderle. La stessa cosa avviene quando ci si sposta da una sidechain alla catena principale.

Della gestione di tale processo si occupa un'entità nota come **federazione**, la quale garantisce l'interoperabilità del sistema, nonché la possibilità di passare dalla blockchain principale alle varie sidechain in qualsiasi momento. Sono gli stessi creatori della sidechain a scegliere i membri della federazione. Come per la blockchain principale anche in queste secondarie sono presenti dei miner, i quali possono essere incentivati attraverso il cosiddetto "*mining combinato*", in cui due criptovalute separate, basate sullo stesso algoritmo, vengono estratte simultaneamente.

Il vantaggio è che la presenza di nodi privati, con specifiche capacità di elaborazione dei dati, consente la gestione di un numero elevato di operazioni con maggiore velocità e flessibilità. Questo perché le operazioni non vengono registrate sulla blockchain principale e, dunque, le spese di commissione possono essere basse o nulle. Tuttavia, si tratta di una rete basata sulla presenza di federazioni che si occupano della sua gestione, il che collide con la filosofia della blockchain di bitcoin, decisamente più decentralizzata. Inoltre, soffre di alcuni problemi legati alla sicurezza. Infatti, se non c'è abbastanza potenza mineraria per proteggere le sidechain queste potrebbero essere violate, ma dal momento che sono indipendenti, se hackerate o compromesse, il danno sarà contenuto all'interno delle stesse e non influenzerà la catena principale. Viceversa, se la catena principale viene compromessa, la sidechain può funzionare ma perderà la maggior parte del suo valore.

Se in futuro questi meccanismi di sicurezza venissero rafforzati, la tecnologia sidechain sarebbe promettente per il miglioramento della scalabilità delle blockchain. Nella prossima sezione, invece, verrà descritta un'altra tra le proposte fatte per migliorare la scalabilità di Bitcoin, *Bitcoin Unlimited*.

4.1.4 Bitcoin Unlimited

Bitcoin Unlimited (BU) è stato sviluppato con l'intento di eliminare il concetto di limite della dimensione dei blocchi di Bitcoin, dando la possibilità ai miner di decidere autonomamente la propria soglia, o meglio permettendo loro la creazione di blocchi di dimensione arbitraria e la trasmissione degli stessi sulla rete. Tali blocchi saranno in competizione gli uni con gli altri per una posizione nella Blockchain.

Apportare queste modifiche significherebbe dare il via ad una hard-fork di Bitcoin con la conseguente suddivisione della blockchain e con tutti i rischi che comporta l'aumento della dimensione dei blocchi. In particolare, questo potrebbe far gonfiare a dismisura la Blockchain, la quale, al momento ha una dimensione di circa 150 gigabyte. Se il limite di dimensione dei blocchi aumentasse al punto da poter gestire un bacino di utenti di portata globale, la Blockchain crescerebbe di diversi petabyte, se non addirittura di più. Questo porterebbe ad una maggiore centralizzazione dei Bitcoin: solo le grosse compagnie sarebbero,infatti, in grado di permettersi lo spazio e la potenza di calcolo necessari a processare una tale quantità di dati. Gli operatori più piccoli verrebbero gradualmente eliminati dalla rete, in maniera discorde all'idea fondante del Bitcoin come moneta governata da ciascuno dei suoi utenti.

Per queste ragioni questa soluzione non è stata presa in considerazione dagli sviluppatori ma, al contrario, è stata approvata la tecnica di *Segregated Witness*, descritta nella prossima sezione.

4.1.5 Segregated Witness

Segregated Witness, o SegWit (traducibile come *Testimone Segregato*), rappresenta un soft fork applicato al protocollo Bitcoin per risolvere alcuni problemi di scalabilità nel formato delle transazioni. Questo update è stato necessario poiché la rete stava diventando sempre più utilizzata e di conseguenza più lenta. Ciò causò un aumento significativo delle commissioni e dei tempi di attesa per ciascuna transazione. Tale modifica venne applicata ad altre criptovalute come, ad esempio, Litecoin, descritta in precedenza.

Vi erano principalmente due questioni da risolvere:

- **Limite dei blocchi di 1 MB**
  La SegWit introduce una nuova struttura dati chiamata **witness** (testimone), in cui vengono spostati i dati necessari a verificare la validità della transazione ma non a definirne gli effetti, nello specifico, le firme e gli eventuali script di sblocco. In una transazione Bitcoin la firma, realizzata con la chiave privata del mittente, rappresenta la condizione di spendibilità di quei determinati bitcoin, e occupa circa il 65% della dimensione totale dei dati relativi alla transazione. Pertanto, isolando la firma in una struttura a parte si avrà una riduzione della dimensione delle transazioni, consentendo di aggiungerne un numero maggiore all'interno di ogni blocco, il cui limite di memoria è fissato a 1 MB. Secondo alcune stime, l'adozione di questa tecnica avrebbe gli stessi effetti di un incremento diretto della dimensione del blocco a 2 MB.

- **Problema della Transaction Malleability**
  L'isolamento della firma in una struttura a parte risolverebbe anche il problema della Transaction Malleability, cioè un attacco che consentirebbe a qualcuno di modificare l'ID univoco di una transazione Bitcoin (ovvero il suo hash) prima che venga confermata sulla rete. A soffrire di questo problema sono soprattutto le reti che utilizzano transazioni custom, come Lightning Network. L'adozione della modifica SegWit risolverebbe il problema poiché le firme non verrebbero più utilizzate per creare l'hash della transazione e ciò ne renderebbe difficile l'alterazione. Dunque, sarebbe possibile l'applicazione della tecnologia Lightning Network, per rendere le transazioni immediate, anonime e con minori commissioni.

La modifica del protocollo Bitcoin per migliorare la scalabilità sfruttando il modello Segregated Witness, subordinata ad una adesione dell'80% della comunità, venne attivata il 24 agosto 2017. Venne fatta anche una seconda proposta, chiamata *Segregated Witness 2x* che prevedeva l'aumento della dimensione dei blocchi invece della riduzione del peso delle transazioni, ma l'8 novembre 2017, gli sviluppatori di SegWit2x annunciarono che l'hard fork pianificato per il 16 novembre 2017 era stato cancellato a causa della mancanza di consenso della rete.

Nonostante l'adozione di questo protocollo abbia contribuito a migliorare la gestione delle transazioni, i sostenitori di SegWit2x sostengono che questa sarà solo una soluzione momentanea ai problemi di scalabilità. Infatti, se si pensa ad una prospettiva futura in cui un maggior numero di utenti inizierà a far uno di Bitcoin, probabilmente si incorrerà nuovamente nello stesso problema legato al rallentamento della rete. Tutti questi problemi di scalabilità, sommati alla quantità elevata di risorse necessarie per il funzionamento del PoW hanno influito anche negativamente sull'ambiente. Di questo argomento si discuterà nella prossima sezione.

4.2 Proposte per Ridurre l'Impatto Ambientale

I dispositivi di cui tutti fanno uso al giorno d'oggi possono apparire come privi di effetti sull'ambiente. Quando si accende un computer o uno smartphone non si percepiscono inquinamento o calore, ma è soltanto una sensazione soggettiva piuttosto sbagliata. Anche se può sembrare strano dispositivi come i computer, gli smartphone, i tablet, i router, i sensori, i server e tutto ciò che è connesso ad Internet dell'universo IoT, hanno degli effetti sull'ambiente. Infatti, possono contribuire al riscaldamento globale tramite emissioni di gas serra (spesso definite CO2 equivalenti) o all'inquinamento. Innanzitutto consumano una grande quantità di energia per il loro funzionamento e l'incremento della richiesta energetica contribuisce al riscaldamento globale. Inoltre, il loro smaltimento a fine vita ha un forte impatto ambientale: può essere inquinante e pericoloso.

Bitcoin si può includere in questa vasta gamma di sistemi che creano problematiche ambientali, proprio per il grande consumo di risorse e di energia che richiede il PoW per funzionare. In particolare, ha contribuito all'aumento dell'**impronta di carbonio** (carbon footprint), cioè vale a dire la quantità di emissioni di gas serra generate lungo il suo ciclo di vita. Per la precisione la Carbon Footprint indica la quantità di carbonio (espressa in tonnellate). Inoltre, alcuni studi hanno portato a concludere che tra qualche decennio se Bitcoin continuerà con questo andamento potrebbe causare il surriscaldamento globale.

Di seguito verrà fornito un elenco cronologico di una raccolta di articoli, dal 2018 al 2020, in cui sono state fatte delle analisi, in merito ai rischi ambientali che Bitcoin ha provocato o potrebbe provocare, e sono state proposte alcune possibili soluzioni.

- **Bitcoin emissions alone could push global warming above 2°C**[Mor+18]
  In questo studio dell'università delle Hawaii, che è stato pubblicato sulla rivista scientifica Nature Climate Change, chi ha condotto la ricerca definisce Bitcoin come una criptovaluta assetata di potere che viene sempre più utilizzata come sistema di investimento e pagamento. Nello specifico, i ricercatori sostengono che l'utilizzo previsto di Bitcoin, se dovesse seguire il tasso di adozione di altre tecnologie ampiamente adottate, potrebbe da solo produrre abbastanza emissioni di CO2 da spingere il riscaldamento sopra i 2°C in meno di tre decenni.

  Il 5 ottobre 2016 i leader di 176 paesi hanno stipulato **l'accordo di Parigi**[2], entrato poi in vigore il 4 novembre 2016, il quale prevede di mantenere il riscaldamento globale al disotto dei 2°C e con alcuni sforzi limitarlo a 1,5°C, in modo da prevenire pericolosi eventi climatici quali: siccità, ondate di caldo, incendi, tempeste, ecc. Con le premesse fatte in questo articolo questo sembrerebbe un obiettivo non raggiungibile. Infatti, il tutto è già considerato come è una sfida ardua dovuta alla crescita della popolazione e alla mancanza di volontà da parte di istituzioni politiche. Quindi se si aggiunge anche l'avvento di Bitcoin diventa ancora più difficile pensare di rientrare in quei limiti.

  I ricercatori riportano che nel solo 2017 la produzione di bitcoin ha causato l'emissione di 69 milioni di tonnellate di CO2. La crescita accelerata dell'utilizzo di Bitcoin potrebbe rientrare nell'intervallo di emissioni che riscalderanno il pianeta di 2°C in soli 16 anni, entro 22 anni se il tasso attuale è simile ad alcune delle tecnologie più lente e ampiamente adottate, o entro 11 anni se adottato al ritmo più veloce con cui sono state incorporate altre tecnologie. Data la natura decentralizzata di Bitcoin e la necessità di massimizzare i profitti economici, è probabile che il suo processo di verifica migrerà verso luoghi in cui l'elettricità è più economica.

[2]https://ec.europa.eu/clima/policies/international/negotiations/paris_it

A seguito degli studi condotti la loro idea è che la riduzione dell'impronta di carbonio di Bitcoin non dovrebbe basarsi esclusivamente su alcuni hardware ancora da sviluppare, ma includere semplici modifiche al sistema complessivo, come l'aggiunta di più transazioni per blocco o la riduzione della difficoltà o del tempo necessario per risolvere la prova di lavoro - entrambi potrebbero comportare riduzioni immediate dell'elettricità per l'utilizzo di Bitcoin. Inoltre, precisano che la loro analisi riguarda soltanto Bitcoin ma che il problema dell'elevato consumo di elettricità è comune a diverse criptovalute, dunque, suggeriscono che qualsiasi ulteriore sviluppo dovrebbe mirare in modo critico a ridurre la domanda di elettricità, se si vogliono evitare conseguenze nell'ambito del riscaldamento globale.

- **Bitcoin's Growing Energy Problem** [Vri18]
  Alex De Vries nel suo articolo del 2018 parla del problema dello spreco di energia e ha stimato che la rete Bitcoin consumava, fino a quel momento, almeno 2,55 gigawatt di elettricità e potenzialmente 7,67 gigawatt in futuro, rendendola paragonabile a paesi come l'Irlanda (3,1 gigawatt) e l'Austria (8,2 gigawatt). Inoltre, secondo i modelli economici il consumo di elettricità di Bitcoin si sarebbe aggirato verso quest'ultimo numero. Con la rete Bitcoin che elabora solo 200.000 transazioni al giorno, ha fatto anche una stima sull'elettricità media consumata per transazione, con la conclusione che era pari ad almeno 300 KWh e avrebbe potuto superare i 900 KWh per transazione entro la fine dell'anno.

  Non sapendo molto sui costi dell'hardware ha fatto delle ipotesi, considerando che in alcuni casi i costi potrebbero non avere alcun ruolo se le macchine e/o l'elettricità venissero rubate o abusate. Ha riportato il caso di un ricercatore che ha utilizzato in modo improprio i super computer finanziati della National Science Foundation per estrarre 8.000 - 10.000 dollari di Bitcoin e l'operazione ha finito per costare all'università 150.000 dollari. In conclusione, ha fatto presente che la comunità di sviluppo di Bitcoin sta valutando soluzioni come Lightning Network per migliorare il throughput (produttività) della rete, il che potrebbe alleviare la situazione, ma ricordando comunque che il grosso problema di Bitcoin è che cresce molto rapidamente.

- **The Carbon Footprint of Bitcoin** [SKG19]
  Gli autori di questo articolo hanno fatto una stima del consumo energetico in emissioni di carbonio, utilizzando un modello tecnico-economico per la determinazione del consumo di elettricità della rete Bitcoin al fine di fornire una stima accurata della sua impronta di carbonio.

  In primo luogo, hanno registrato il consumo energetico, basandosi sull'hardware utilizzato dai miner, supponendo che sia il più efficiente, e hanno stimato un consumo di energia di 345 MWh alla fine del 2016, 1.637 MWh alla fine del 2017 e 5.232 MWh a novembre 2018. Moltiplicando il consumo energetico a novembre 2018 per 8.760 ore, hanno concluso che il totale annuo è di 45,8 TWh. Successivamente hanno sviluppato tre scenari che rappresentano l'impronta geografica del mining di Bitcoin, sulla base della localizzazione di indirizzi IP:

  1. **IP del server del pool**: hanno determinato che i miner tendono ad allocare la potenza di calcolo in pool locali, per un 68% in Asia, 17% in Europa e 15% in Nordamerica. Lo svantaggio di questo primo scenario è che potrebbe sovrastimare la quota di miner asiatici;
  2. **IP del dispositivo**: con questo secondo approccio hanno riscontrato una concentrazione negli Stati Uniti più forte rispetto al metodo precedente, infatti, i risultati riportano una concentrazione significativa negli Stati Uniti del 19%, Venezuela 16%, Russia 11%, Corea 7%, Ucraina 5% e Cina 4%. Questo conferma che la seconda metodologia ha fruttato migliori risultati rilevando posizioni che non erano state precedentemente individuate;
  3. **IP dei nodi peer-to-peer**: con questo terzo metodo hanno registrato che il 93% di tutti i blocchi vengono trasmessi sul suolo statunitense.

  In ultimo hanno calcolato l'impronta di carbonio, combinando queste informazioni con quelle relative alle emissioni causate dall'energia usate nelle singole regioni, e hanno stimato che l'emissione globale in atmosfera è di una quantità tra 22,0 e 22,9 milioni di tonnellate di CO2 ogni anno. Il che si può paragonare alle emissioni prodotte da nazioni quali Giordania e Sri Lanka.

- **Bitcoin Mining and Its Environmental Effects** [DF19]
  Questo studio esamina le elevate quantità di energia consumate da Bitcoin e suoi effetti ambientali. Si sostiene che l'energia consumata a seguito dell'aumento dell'estrazione di Bitcoin avrà conseguenze ambientali e sociali, come il riscaldamento globale e il cambiamento climatico. Inoltre, si fa notare che le criptovalute, e Bitcoin in particolare, siano nuove e di status legale poco chiaro, questo potrebbe comportare il rischio di essere coinvolte in attività illegali o essere utilizzate come strumento di investimento volatile e speculativo. Nello specifico si parla di 2 visioni di pensiero:

  1. Opinioni ottimistiche che enfatizzano i vantaggi di Bitcoin. Chi possiede un approccio più ottimistico si basa sul fatto che Bitcoin abbia una solida base tecnologica/crittografica che lo rende sicuro e non manipolabile;
  2. Opinioni pessimistiche in cui gli svantaggi di Bitcoin sono predominanti. Chi è pessimista sostiene che poiché manca di un centro specifico, potrebbe causare danni finanziari ed ambientali a causa dell'energia che consuma. La più grande critica alle criptovalute è la loro propensione ad essere utilizzate per attività illegali come il riciclaggio di denaro e si sottolinea che possano creare delle opportunità per gli evasori fiscali.

  Si fanno stime sul consumo: L'estrazione di bitcoin consuma più elettricità di 159 paesi. Se il tasso di consumo energetico dovesse aumentare si prevede che utilizzerà più elettricità rispetto al Regno Unito entro ottobre 2018. Inoltre, entro luglio 2019 eguaglierà il consumo totale di energia degli Stati Uniti e se questo consumo di elettricità continuerà fino al 2020, si prevede che aumenterà tanto quanto l'uso di elettricità in Danimarca.

  Inoltre, fanno presente che l'estrazione di bitcoin che si verifica nelle aree in cui l'elettricità è ottenuta dal carbone comporterebbe il peggioramento della qualità dell'aria e si formerebbe un ostacolo significativo al raggiungimento degli obiettivi fissati nell'accordo di Parigi.

- **Blockchain: An Unorthodox Solution to Reduce Global Warming** [Tas19]
  John Taskinsoy nel suo articolo fa una premessa sostenendo che il riscaldamento globale provocherà dei disagi inimmaginabili in ogni aspetto della vita umana entro il 2050 se alcune azioni non verranno intraprese immediatamente per ridurre la sua rapida accelerazione. Ricorda, inoltre, che scienziati e ambientalisti avvertono che se nel prossimo decennio non si farà nulla per affrontare i cambiamenti climatici, il riscaldamento globale potrebbe accelerare fino a circa 1,5°C entro il 2050, il che potrebbe portare a cambiamenti climatici con conseguenze catastrofiche.

  John vuole dare una prova di come una blockchain, se utilizzata nel modo corretto, possa fornire una vasta gamma di opportunità per affrontare le sfide del riscaldamento globale. Egli sostiene che un uso di blockchain decentralizzate potrebbe potenzialmente svolgere un ruolo nella riduzione dei gas serra indotti dall'uomo; a sua volta, un calo stimato fino a 0,5°C della temperatura media globale allevierà le pressioni e consentirà agli ecosistemi di adattarsi ai cambiamenti climatici.

  Inoltre, precisa che il problema del riscaldamento globale si potrebbe controllare, in futuro, se gli esseri umani dipendessero meno dall'agricoltura intensiva che spreca risorse vitali non rinnovabili. L'allevamento intensivo (cioè carne, latte e uova) produce enormi quantità di gas serra che favoriscono lo sviluppo di cambiamenti climatici estremi e aumenta la deforestazione per coltivare mangime (colture), che non solo utilizza grandi quantità di energia ma rilascia nell'atmosfera il carbonio precedentemente immagazzinato.

  Secondo quanto letto, egli sostiene che la blockchain potrebbe aiutare a preservare l'ecosistema. Ad esempio, può aiutare a ridurre il riscaldamento globale creando un mondo senza carta; in questo modo, meno carbonio verrà rilasciato dalla biosfera come risultato della riduzione della deforestazione e il ciclo del carbonio della Terra sarà più equilibrato. Se Bitcoin, spronasse le banche centrali di tutto il mondo a introdurre le proprie criptovalute, rimuovendo le monete cartacee dalla circolazione, la blockchain potrebbe salvare circa 973 milioni di alberi dal taglio.

Pone un altro esempio riguardo al settore immobiliare, il quale comprende una serie di terze parti fidate (cioè intermediari). Dal momento che la blockchain è una tecnologia di registro distribuito sarebbe in grado di riunire tutti gli intermediari coinvolti sulla stessa piattaforma, evitando inutili emissioni di gas a effetto serra indotte dall'uomo. Inoltre, come ultimo esempio, ne propone l'utilizzo in ambito sanitario per archiviare varie ed estese cartelle cliniche di persone a cui possono accedere medici e pazienti da qualsiasi parte del mondo, sostenendo che questo potrebbe far risparmiare tempo e molte vite nelle emergenze mediche. Quindi in sostanza, il concetto è che attraverso l'efficace implementazione di varie tecnologie di blockchain, lo spreco di risorse potrebbe essere ridotto o in alcuni casi eliminato.

- **An approach to minimize the energy consumption during blockchain transaction** [Nai+20]
  In questo articolo, l'attenzione si concentra sui diversi approcci adottati durante il processo di gestione delle transazioni all'interno di una blockchain, per ridurre al minimo le perdite. Si fa un confronto tra due importanti paradigmi che utilizzano questa tecnologia: Bitcoin, la prima applicazione ben nota basata su blockchain, ed Etherum, una piattaforma basata su smart contract.

  Tra gli approcci proposti per migliorare la velocità e la scalabilità del processo blockchain vengono citati: sharding, sidechain e utilizzo dei canali di pagamento. Gli ultimi due sono stati descritti nei precedenti capitoli di questo documento, mentre, lo sharding (letteralmente "*frammento*") è un tipo di partizionamento, con cui gli sviluppatori stanno lavorando per migliorare la scalabilità di Ethereum. Questo sistema è come una rete di mini-blockchain che hanno una propria rete di nodi che elabora le transazioni solo per il frammento specifico. Questo consente una maggiore velocità di elaborazione delle transazioni su tutti i frammenti, i quali, ereditano tutte le stesse caratteristiche di sicurezza e il consenso della blockchain principale. All'interno di uno shard, i nodi vengono selezionati in modo casuale per votare periodicamente sulla validità dei blocchi. I voti vengono esaminati dalla catena principale e uniti in un contratto di gestione dello sharding. Gli shard sono concatenati come avviene per i blocchi di una blockchain.

Tornando all'articolo, dopo questa breve digressione, sono state analizzate problematiche relative a:

- Consumo energetico: Si stima che vengano consumati 2,55 GW di elettricità e a breve sarà 7,67 GW, il che la rende equivalente a paesi come l'Irlanda (3,1 GW) e l'Austria (8,2 GW).
- Costi di raffreddamento: Per il corretto funzionamento del processo della blockchain, è necessaria una tecnologia di raffreddamento che dissipa il calore generato dalle macchine, allo stesso tempo questa tecnologia di raffreddamento richiederà una quantità significativa di elettricità. Le operazioni di mining nella tecnologia blockchain vengono eseguite a porte chiuse, quindi vi è una conoscenza molto scarsa sull'efficacia dell'utilizzo dell'energia. In alcune parti della Cina, la tecnologia di raffreddamento viene sostituita da un sistema evaporativo. Tuttavia, ora non esiste un rapporto esatto sull'utilizzo di elettricità durante il raffreddamento.

Infine, si fa riferimento a ciò che affermano gli esperti, vale a dire, che questo consumo di energia sta peggiorando di giorno in giorno e si prevede che entro il 2021 consumerà tanto quanto l'elettricità consuma il mondo.

- **Cryptocurrency and climate change: an overview** [EO20]
  Anche in questo articolo si parla delle problematiche legate al clima. Nello specifico si fa riferimento alle criptovalute che aumentano le emissioni di carbonio, sommandosi sequenzialmente agli effetti complessivi del riscaldamento globale. Questo studio esamina l'impatto della criptovaluta sull'ambiente con focus sui cambiamenti climatici (riscaldamento globale). Sebbene il destino del Bitcoin sia attualmente imprevedibile, si crede che se il suo tasso di adozione viene aumentato, la richiesta di elettricità sarà in grado di produrre emissioni sufficienti per superare i 2°C del riscaldamento globale in pochi decenni.

  Lo studio raccomanda che l'ulteriore sviluppo delle criptovalute dovrebbe mirare analiticamente a ridurre la domanda di energia in modo da evitare le conseguenze potenzialmente demoralizzanti dei 2°C del riscaldamento globale.

Viene proposta come soluzione l'adozione di fonti alternative di energia pulita e rinnovabile (solare, eolica, biomassa, geotermica e idroelettrica). Queste fonti di energia non producono gas tossici che causano inquinamento e provocano il riscaldamento globale. Inoltre, viene fatto presente che i governi dovrebbero ideare e approvare politiche che incoraggino le aziende energetiche e le persone, in generale, a utilizzare l'energia rinnovabile invece dell'energia convenzionale.

- **Bitcoin Carbon Footprint: Mining Pools Based Estimate Methodology** [KD20]
  Il documento si occupa dell'impatto della criptoeconomia sull'ambiente. Il termine "criptoeconomia" viene utilizzato per designare il settore emergente attorno alle criptovalute e alla blockchain. L'estrazione di criptovalute consuma molta elettricità. A settembre 2019, il consumo annuo stimato di elettricità dei miners era di 78,93 TWh. Secondo la stima, le emissioni di anidride carbonica erano circa 80,43 milioni di tonnellate di CO2, che corrisponde allo 0,24% delle emissioni di anidride carbonica totali del mondo. Lo scopo di chi ha ideato questo documento è quello di proporre una metodologia di stima dell'impronta di carbonio del mining di Bitcoin. Il metodo suggerito si basa sulla distribuzione geografica dei miner ottenuta analizzando il traffico delle pagine di accesso ai mining pool. La metodologia include:

  1. La valutazione della distribuzione geografica dei miners;
  2. La stima delle emissioni di anidride carbonica dei miners per regione.

  Secondo la metodologia proposta, le emissioni di anidride carbonica dei minatori sono di circa 44,12 milioni di tonnellate all'anno (0,13% delle emissioni totali mondiali), che è due volte inferiore alla stima del limite superiore.

In questo capitolo sono state raccolte tutte le idee, alcune delle quali sono state realizzate e altre solo proposte, per poter migliorare la scalabilità del protollo Bitcoin e ridurre lo spreco di energie e risorse dovute al PoW. Nel prossimo capitolo verrà introdotto il concetto di Proof of Useful Work, che è un alternativa alla PoW nata con l'intento di migliorarne il protocollo di consenso.

Capitolo 5

Proof of Useful Work

La **Proof of Useful Work (PoUW)**, o prova di lavoro utile, è un nuovo protocollo di consenso blockchain utilizzato per migliorare l'efficienza e la sicurezza della blockchain. In questo capitolo verranno illustrate alcune proposte realizzate o solo teorizzate basate sul PoUW, per dimostrare come questa tecnologia si possa sfruttare per ridurre lo spreco di risorse e di energia che caratterizza il classico metodo di PoW.

5.1 Progetto PAI basato sull'Intelligenza Artificiale

Il **Progetto PAI**, acronimo di **Personal Artificial Intelligence**, nasce con lo scopo di fornire a tutti il proprio avatar intelligente (detto PAI) che sia in grado di comportarsi come una persona. Questo avatar si potrà usare in tutti gli aspetti della vita quotidiana, dall'assistenza sanitaria ai social network, ai viaggi e all'intrattenimento.

In questo progetto la blockchain è necessaria per permettere la presenza in tutto il mondo di questi avatar, senza limitazioni spaziali o legate a un singolo server, inoltre, è utile per proteggere ed autenticare i PAI creati dagli utenti. Lo sviluppo è a carico della società Oben di Los Angeles, la quale, in un recente articolo [Lih+20], ne ha descritto le funzionalità e i vantaggi rispetto ai servizi offerti da Bitcoin. Di seguito ne verranno riportati gli aspetti essenziali.

Nell'articolo viene introdotto il protocollo PoUW basato sull'addestramento di un modello di apprendimento automatico sulla blockchain. Inoltre, vengono descritti meccanismi per premiare il lavoro utile e punire i malintenzionati, con l'obiettivo di costruire sistemi di intelligenza artificiale migliori utilizzando la sicurezza della blockchain.

Facendo un confronto con il PoW sostengono che esso sia facile da verificare ma difficile da produrre, inoltre fanno presente che i miner hanno la possibilità di coniare monete a piacimento e vengono premiati per aver costruito la catena più lunga. Il loro obiettivo, invece, è quello di premiare solo i più produttivi. Per fare ciò, il PoW dovrebbe essere combinato con l'apprendimento automatico (Machine Learning - ML)[1] e i miner dovrebbero competere per fornire una prova di lavoro utile (PoUW). Dunque, hanno progettato un'infrastruttura blockchain per coordinare l'addestramento di una rete neurale profonda (Deep Neural Network - DNN)[2] e una rete decentralizzata con un protocollo di consenso per eseguire e verificare il lavoro utile basato sul ML. Al centro del protocollo c'è un nuovo modo per creare nonce derivati da un lavoro utile.

5.1.1 Rete PAI

La struttura di un'ambiente PAI, riportata in Figura 5.1, è una rete P2P decentralizzata con al suo interno una blockchain ibrida Proof of Work/Proof of Stake (PoW/PoS) ed è composta da una serie di attori:

- **Client**: nodi che pagano per addestrare i loro modelli sulla blockchain PAI;
- **Miners**: nodi che eseguono l'addestramento. Possono estrarre un nuovo blocco con nonce speciali ottenuti dopo ogni iterazione. La formazione viene distribuita e tutti i miner collaborano condividendo aggiornamenti sul loro modello locale;
- **Supervisors**: attori che registrano tutti i messaggi durante un'attività in un registro chiamato **message history** (cronologia dei messaggi). Inoltre, proteggono da comportamenti dannosi durante la formazione poiché l'ambiente potrebbe contenere anche nodi malevoli;

[1] https://en.wikipedia.org/wiki/Machine_learning
[2] https://en.wikipedia.org/wiki/Deep_learning#Deep_neural_networks

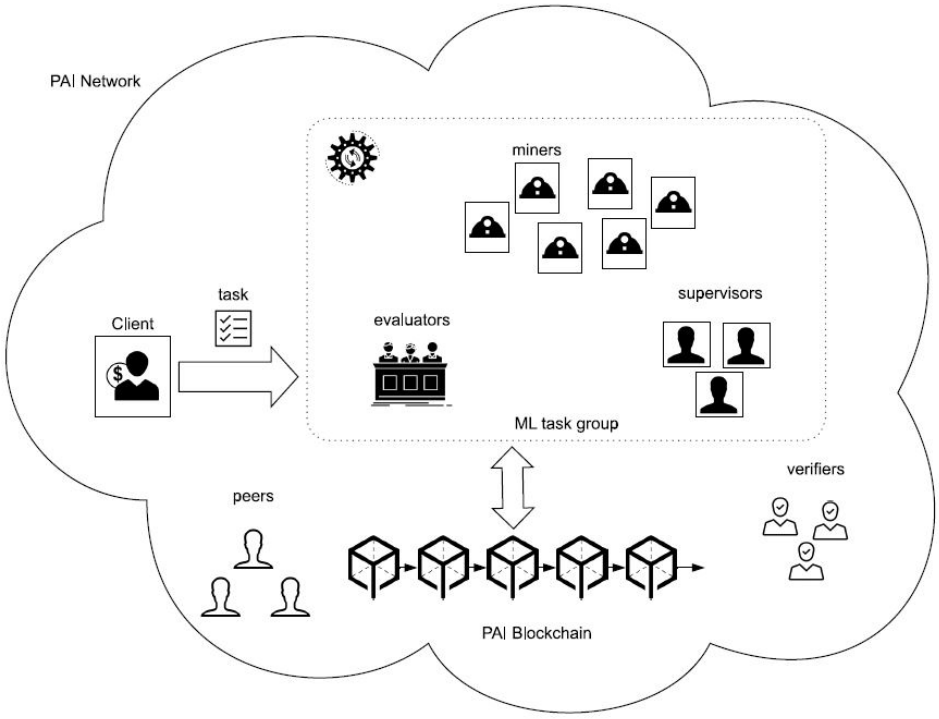

Figura 5.1: La rete PAI

- **Evaluators**: nodi indipendenti che testano i modelli finali di ogni miner e inviano il migliore al client. Inoltre, ridistribuiscono la quota pagata dal client in parti uguali a tutti i nodi;
- **Verifiers**: nodi che verificano se un blocco è valido. Sono necessari poiché la verifica è computazionalmente costosa e non viene eseguita da tutti i nodi;
- **Peers**: nodi che non hanno nessuno dei ruoli sopra menzionati e usano semplicemente normali transazioni blockchain.

In sostanza, il client invia un task ML alla rete PAI, i nodi di lavoro che sono i miner e i supervisori eseguono la formazione, mentre, i valutatori decidono come pagare. La blockchain PAI garantisce la sicurezza del processo ML, grazie anche alla collaborazione dei verificatori. I miner e i supervisori sono connessi tra loro tramite dei canali veloci, attraverso i quali possono scambiarsi dei messaggi. Anche i miner possono scambiare dei messaggi tra di loro, ma questo è facoltativo.

5.1.2 Transazioni

Una transazione Bitcoin è una struttura dati con firma digitale in cui l'input deve far riferimento esattamente ad un output di una transazione precedente e affinché sia valida questo output non deve essere speso (UTXO). **OP_RETURN** è un campo di operazioni che contrassegna l'output non valido di una transazione, ma può essere utilizzato per memorizzare dati arbitrari nella blockchain. Nella blockchain PAI, si utilizzano transazioni speciali per gestire la formazione, la verifica, la valutazione e il pagamento delle attività di ML. Per fare ciò, vengono codificate tutte le informazioni aggiuntive richieste nello script OP_RETURN, di uno degli output della transazione.

Prima dell'inclusione nei blocchi, le transazioni attendono nel **mempool**, un buffer di transazioni in sospeso. I nodi inoltrano le transazioni dal mempool l'uno all'altro e così avviene la propagazione lungo la rete. I messaggi off-chain e le transazioni vengono firmati utilizzando la chiave ECDSA privata del partecipante. Quando sono necessarie delle transazioni multi-parte sfruttano lo schema di firme digitali *Boneh-Lynn-Shacham (BLS)* [BLS04], che in sostanza consente di aggregare più firme in un'unica. Questo è utile quando i supervisori devono concordare una decisione comune.

5.1.3 Stacking

Ad eccezione dei normali peer, tutti i nodi devono prima depositare monete come garanzia, questo processo prende il nome di **stacking**. I depositi rappresentano denaro bloccato che viene successivamente restituito insieme a commissioni extra se i partecipanti finiscono correttamente il loro lavoro. Staking significa acquistare i biglietti, cioè i nodi possono emettere transazioni **BUY_TICKETS** (acquista biglietti), che sono transazioni speciali contenenti il ruolo desiderato (miner, supervisore, ecc.) e le preferenze per task specifici (contenuti nello script OP_RETURN). I biglietti diventano "attivi" dopo essere stati inclusi nella blockchain, con un numero massimo di 50 biglietti per blocco. Un altro tipo di transazione è la **PAY_FOR_TASK**, che viene emessa dai client quando inviano un nuovo task e include una descrizione dell'attività e una quota di formazione.

Nello specifico un task contiene: una descrizione del modello da addestrare, il criterio di arresto, un'ottimizzatore (indica ad esempio la velocità di apprendimento), la strategia di convalida, informazioni sui dati e sulle prestazioni (tempo di formazione previsto). Come già detto, la quota del client viene suddivisa tra i nodi seguendo uno schema di ricompensa: una parte viene ricevuta dai miner in base alle prestazioni, una parte dai supervisori e un'altra parte dai valutatori. Tutti i nodi sono incentivati a partecipare alla blockchain PAI: i client ricevono un modello addestrato, i miner possono ricevere ricompense in blocco e una frazione della commissione del client, i supervisori e i valutatori ricevono anche una parte della commissione del client. I miner compensano i verificatori con una quota della ricompensa del blocco.

Lo staking è un modo per proteggersi da comportamenti dannosi poiché la posta in gioco degli attori disonesti viene catturata e ridistribuita ai giocatori leali. Alla fine della formazione, i valutatori decidono come dividere la parcella del cliente e punire i cattivi attori. Emettono, dunque, una transazione chiamata **CHARGE_FOR_TASK** per pagare i partecipanti onesti. La commissione del client viene restituita se l'attività non può essere eseguita. La quota che i nodi depositano all'inizio ha un tempo di scadenza dopo il quale, se il nodo non è stato assegnato a svolgere i lavori, l'importo viene restituito. Inoltre, la quota dei nodi disonesti viene ridistribuita agli altri nodi, mentre, chi non lavora correttamente ne perde una parte (es. 5% miner, 10% supervisori).

5.1.4 Protocollo

Secondo questo sistema un client utilizza la blockchain PAI per addestrare un modello ML e per pagare il servizio. Dopo aver trasmesso il task alla rete PAI, i miner e i supervisori vengono abbinati casualmente dalla rete in base alle preferenze dei nodi di lavoro. Il set di dati iniziali di addestramento viene suddiviso in:

- Un set di formazione, rivelato ai miner per eseguire il lavoro di ML su di esso;
- Un set di convalida selezionato dal set di dati di addestramento iniziale per la convalida ML;
- Un set di test, rivelato ai valutatori quando il modello finale dovrà essere testato.

Il set di dati di addestramento è ulteriormente suddiviso in mini-batch (campioni) di dimensioni uguali (tipicamente da 10 a 1000 record). Ad ogni iterazione viene elaborato un mini-batch finché l'epoca (ciclo di addestramento) non si conclude, a seguito dell'elaborazione di tutti i mini-batch. Inoltre, viene scelto un supervisore leader e se in una delle iterazioni successive compare una transazione speciale **REPLACE_LEADER**, confermata da almeno 2/3 supervisori, allora questo viene sostituito. La transazione conterrà il motivo del rimpiazzo (offline, troppo lento, dannoso, ecc). Un supervisore, invece, viene sostituito quando non riesce a registrare più del 10% delle iterazioni. A quel punto, il leader, avvia la procedura di sostituzione pubblicando una speciale transazione denominata **RECRUIT_WORKER_NODE**.

Una volta avviata la formazione, i miner migliorano in modo iterativo i loro modelli locali in base al loro lavoro sui mini-batch e in base ai messaggi che ricevono dagli altri miner. Ognuno di loro condivide le modifiche al proprio modello con altri e le estrazioni avvengono con diversi nonce ottenuti dopo ogni iterazione. I supervisori registrano tutti i messaggi durante un'attività e si occupano di comportamenti dannosi, inoltre sono di aiuto ai miner per dimostrare che hanno svolto un onesto lavoro di ML, registrando i messaggi inviati durante la formazione nella *message history*, tali messaggi saranno utili ai verificatori per dimostrare la prova di lavoro utile dei miner. Se un miner completa prima il lavoro per un'epoca, allora aspetterà che anche la maggior parte dei suoi colleghi finisca e applicherà ad interim i loro aggiornamenti.

I valutatori testano i modelli finali, selezionano il modello migliore per il cliente e distribuiscono la tariffa del cliente. Affinché questo accada, però, almeno i 2/3 dei valutatori deve produrre conclusioni identiche (contenenti metriche ML). Quando questo accade il risultato della valutazione viene pubblicato in una transazione speciale chiamata **CHARGE_FOR_TASK**. Un valutatore malevolo potrebbe attendere di leggere le conclusioni degli altri sulla mempool e poi pubblicarne una identica, ma questo viene evitato facendo pubblicare le conclusioni in forma cifrata e quando sono presenti tutte ogni valutatore fornisce la sua chiave pubblica, in modo che vengano lette. Questo metodo prende il nome di *commit-then-reveal*.

Riassumendo quanto detto: i miner costruiscono blocchi come nel protocollo Bitcoin, ma con l'aggiunta di un lavoro utile, ovvero eseguendo onestamente un'iterazione dell'attività ML. Un miner scansiona il mempool, raccoglie le transazioni, crea il blocco ed inserisce informazioni aggiuntive (campi extra) per la prova del lavoro utile. Per convalidare un blocco prima di aggiungerlo alla blockchain, i verificatori riceveranno i dati di input, rieseguiranno l'iterazione e verificheranno se gli output sono riproducibili. Un miner invierà ai verificatori tutti i dati e il contesto necessari per la prova del lavoro utile. I validatori si occuperanno del test del modello finale, del recapito del risultato finale al client e della divisione della quota ai nodi lavoratori.

La differenza sta nel processo di mining. Nel Bitcoin classico, i miner usano tutta la potenza di calcolo per cercare un nonce che risolva l'hash puzzle. In questo caso il processo di mining è lo stesso ma vogliono fare in modo che l'hashing sia insignificante e che la maggior parte della potenza di calcolo venga spesa per la formazione ML.

5.1.5 Vantaggi e Svantaggi

Il protocollo proposto offre diversi vantaggi rispetto a Bitcoin. Viene utilizzato un consenso PoW/PoS ibrido modificato per fornire maggiore sicurezza contro gli attacchi, migliore efficacia energetica e maggiore stabilità della rete, garantita dall'aumento degli incentivi ai partecipanti. Tuttavia gli ideatori fanno presente che, a causa della sua complessità intrinseca, questa soluzione potrebbe presentare anche dei rischi per la sicurezza. Dunque, hanno fornito un'analisi economica e discusso diverse ottimizzazioni volte a migliorare la sicurezza del sistema.

Analisi economica

Per dimostrare che la loro soluzione sia più economica rispetto a Bitcoin hanno analizzato il ROI (ritorno sull'investimento). Dai calcoli è emerso che con il prezzo di Bitcoin pari a $ 8243,41 (a ottobre 2019), solo il miglior impianto di mining Bitcoin sul mercato (Antminer S17 Pro) ha ottenuto un ROI del 18%, mentre, con il mining PoUW hanno raggiunto un ROI medio di circa il 200%. Pertanto, il mining di PAICoin PoUW è stato circa 10 volte più redditizio di Bitcoin, con commissioni per i client ridotte del 30%.

Considerazioni sulle prestazioni

Sostengono che una soluzione distribuita non sarà mai efficiente come eseguire l'intero addestramento su una macchina locale e propongono delle ottimizzazioni per migliorare le prestazioni. Ad esempio: i mini-batch possono essere pre-caricati, l'estrazione può essere eseguita in un processo diverso, i nodi di lavoro possono eliminare i dati non necessari, solo i verificatori eseguono verifiche complete.

Sicurezza

Partendo dal presupposto che la maggioranza dei nodi sia onesta, hanno progettato il protocollo PoUW per scongiurare varie minacce da parte di attori bizantini. Viene fornito un estratto delle strategie adottate per disincentivare e rendere impossibile barare.

- **Il client invia una definizione dell'attività non valida**: è consentito ai nodi di lavoro di ispezionare e segnalare se l'attività T non è valida. In quel caso, la quota del client viene confiscata e distribuita ai nodi di lavoro e ai valutatori;
- **Il miner esegue solo il mining**: viene limitato il numero di nonce per rendere insignificante l'attività di mining classica. Un miner che farebbe un lavoro di ML fasullo e si concentrerebbe solo sul mining non sarebbe in grado di dimostrare la validità dei blocchi prodotti. Il lavoro di ML fasullo include: ripetere gli aggiornamenti ricevuti, abbandonare l'attività prima del completamento o non seguire i passaggi dell'addestramento. È economicamente dannoso per i miner impegnarsi in tali comportamenti perché perderebbero la loro quota e non riceverebbero comunque alcuna commissione dal cliente;
- **Attacchi Sybil**: I nodi cattivi possono impostare diverse Sybil (false identità) sulla rete per generare un modello non valido. Per evitare questo attacco, i nodi di lavoro non sono autorizzati a selezionare le attività da soli, ma dichiarano solo le loro preferenze. In questo modo, non possono scegliere compiti facili;
- **Leader bizantino**: se il leader dei supervisori ritarda la pubblicazione delle transazioni MESSAGE_HISTORY, viene immediatamente eletto un altro leader. Se il leader pubblica transazioni MESSAGE_HISTORY non valide viene aggiunto alla lista nera e sostituito;

- **Attacchi DOS**: i nodi di lavoro possono sospettare che si verifichi un attacco DOS quando non ricevono abbastanza aggiornamenti o se il processo di addestramento è molto lento (o bloccato). Dunque, possono mettere in pausa il processo di addestramento e riprenderlo quando l'attacco è finito.

  La procedura è la seguente: i nodi emettono una transazione CONSIDER_PAUSE con il motivo DOS ATTACK. Se la maggioranza fa la stessa cosa, entro un periodo di tempo predefinito, i nodi onesti emettono una transazione PAUSE e tutti si fermano. In modalità pausa, ogni nodo interessato invierà messaggi fuori catena ai nodi precedenti nel gruppo di attività ML. Quando si forma una nuova maggioranza di nodi attivi, si pubblicano messaggi CONSIDER_RESUME e, infine, transazioni RESUME per continuare il processo di formazione. Un verificatore può rifiutare un blocco estratto durante un attacco DOS se ci sono elementi sufficienti per sospettare che sia stato estratto da un aggressore;

- **Spam blockchain**: un miner dannoso potrebbe inondare la blockchain con blocchi fasulli e provocare ai verificatori onesti uno sforzo considerevole per convalidarli. Anche questo è un attacco DoS perché è difficile convalidare i blocchi molto velocemente. Si adottano le seguenti contromisure: viene data la priorità alle operazioni di verifica meno costose da eseguire per prime, la quota di un miner viene confiscata e questo viene inserito nella lista nera se invia blocchi non validi, si limita il numero di blocchi che un miner può pubblicare durante un intervallo di tempo predefinito.

Riassumendo quanto detto, in questo articolo è stato presentato un modello che fornisce un utilizzo del PoUW, in alternativa al classico PoW di Bitcoin, applicato ad un sistema di apprendimento automatico distribuito e decentralizzato su blockchain. Proposta, che secondo gli sviluppatori, si può facilmente estendere ad altri algoritmi di intelligenza artificiale. Hanno dimostrato che la loro soluzione PoUW è più conveniente e professionale per i miner rispetto al mining di Bitcoin, facendo vedere che i loro modelli di ML possono essere addestrati collettivamente con buone prestazioni utilizzando hardware di base di proprietà di individui. Prospettano per il futuro di continuare a migliorare le prestazioni e la sicurezza del protocollo per renderlo più efficiente possibile.

Nella prossima sezione verrà descritto un altro modello realizzato per fornire una prova di lavoro utile, nello specifico, si farà riferimento a Primecoin.

5.2 Primecoin

Nel marzo del 2013, Sunny King, ebbe l'idea di creare un sistema alternativo basato sulla PoW. Il progetto prende il nome di **Primecoin** [Kin13] e riguarda la ricerca di catene di numeri primi puri, per fornire sia il conio sia la sicurezza per le reti di criptovaluta simili a Bitcoin.

Nell'articolo si parte da un escursus sulla storia dei numeri primi. I numeri primi, un semplice ma profondo costrutto aritmetico, hanno lasciato perplesse generazioni di brillanti matematici. La loro esistenza infinita era conosciuta già oltre 2000 anni fa, tuttavia il teorema, relativo alla distribuzione dei numeri primi, fu provato solo nel 1896, in seguito allo studio di Bernhard Riemann[3] ma rimangono ancora numerose congetture irrisolte fino ad oggi. I record mondiali in numeri primi sono stati in gran parte concentrati sul primo di Mersenne $2^p - 1$, dal nome del monaco francese Marin Mersenne[4], e attualmente i primi 10 più grandi conosciuti sono tutti numeri primi di Mersenne. Due tipi ben noti di coppie prime sono i *twin primes*, ovvero i numeri primi gemelli dove p e $p+2$ sono numeri primi, e i numeri primi di Sophie Germain[5], dove sia p che $2p+1$ sono numeri primi.

Per fornire una PoUW per la criptovaluta, il lavoro deve essere verificabile in modo efficiente da tutti i nodi della rete. Ciò richiederebbe che i numeri primi non siano troppo grandi ma di dimensioni ragionevoli, quindi preclude i numeri primi di Mersenne e si basa, invece, sulla catena di Cunningham. Vale a dire, una certa sequenza di numeri primi, nota anche come "*catena di numeri primi quasi raddoppiati*", che prende il nome dal matematico Alan J. C. Cunningham[6].

[3] https://en.wikipedia.org/wiki/Bernhard_Riemann
[4] https://en.wikipedia.org/wiki/Marin_Mersenne
[5] https://en.wikipedia.org/wiki/Sophie_Germain
[6] https://en.wikipedia.org/wiki/Allan_J._C._Cunningham

Nello specifico fa riferimento a catene di numeri primi di 3 tipi:

1. **Catena Cunningham di 1° tipo (1CC)**: ha ciascuna un numero primo superiore al doppio del numero primo precedente in catena;

2. **Catena Cunningham di 2° tipo (2CC)**: ha ciascuno un numero primo inferiore al doppio del numero primo precedente in catena;

3. **Catena Bi-twin (TWN)**: una catena di numeri primi gemelli in cui ogni coppia gemella fondamentalmente raddoppia la coppia gemella precedente.

Viene fornito un esempio per comprendere meglio queste catene principali. 5 e 7 sono numeri primi gemelli, 6 è la loro media. Raddoppiando 6 si ottiene 12, mentre 11 e 13 sono di nuovo numeri primi gemelli e 12 è la loro media. Quindi 5, 7, 11, 13 è una catena bi-gemella di lunghezza 4, che può effettivamente essere divisa dalle loro medie, ovvero, i numeri inferiori alle medie sono 5, 11, una catena Cunningham di primo tipo, i numeri superiori alle medie sono 7, 13, una catena Cunningham di secondo tipo. Il numero 6, in questo esempio, viene considerato l'origine della catena dei primi. Da questa origine si può continuare a raddoppiare per trovare i numeri primi immediatamente adiacenti ai numeri centrali.

Per fornire una prova di lavoro utile che migliori il classico meccanismo di PoW, la soluzione adottata in questo progetto si è basata sul test di Fermat[7], un modo rapido per controllare se un numero è (molto probabilmente) primo. Un'altra proprietà importante della prova di lavoro è la non riutilizzabilità, cioè, la prova di lavoro su un particolare blocco non dovrebbe essere riutilizzabile per un altro blocco. Per ottenere ciò, la catena di numeri primi è collegata all'hash dell'intestazione del blocco, ovvero, la sua origine deve essere divisibile per l'hash dell'intestazione del blocco. Il quoziente della divisione diventa quindi il *certificato* della prova di lavoro, la cui univocità è garantita dal fatto che ogni blocco ha un hash diverso e, dunque, questo procedimento ne rende impossibile la duplicazione.

[7] https://it.wikipedia.org/wiki/Test_di_Fermat

Diversamente da Bitcoin, che aggiorna il target di difficoltà ogni 2016 blocchi (circa ogni 2 settimane) per ottenere un blocco ogni 10 minuti, Primecoin esegue l'aggiornamento ad ogni blocco, rendendo la conferma delle transazioni circa 8-10 volte più veloce. Si potrebbe argomentare dicendo che un aggressore potrebbe provare ad effettuare un tentativo di double-spending 10 volte più velocemente, ma aumentando il numero di conferme (6 di base come per Bitcoin) il problema verrebbe risolto.

Primecoin è la prima moneta matematica sul mercato a far uso di una prova di lavoro utile per generare una particolare sequenza di numeri primi. Questa ricerca ha lo scopo di aprire la strada all'emergere di altri tipi di prove di lavoro con diversi valori di calcolo scientifico. I primi numeri sono molto utili. Essi sono importanti nella crittografia e sono utilizzati in molti sistemi di crittografia di keysecret. Dunque, progetti di questo genere potrebbero non solo accrescere le conoscenze a livello matematico ma migliorare anhce la sicurezza dei metodi di crittografia che li utilizzano.

Nella prossima sezione verrà descritto un modello teorico, chiamato Coin.AI, che introduce uno schema di lavoro utile per supportare le criptovalute in esecuzione su una blockchain, sfruttando l'addestramento di modelli Deep Learning.

5.3 Coin.AI

A differenza dei progetti appena descritti, questo è solamente un modello teorico, ideato da Alejandro Baldominos e Yago Saez nel 2019 [BS19]. Lo scopo è quello di fornire un modello di PoUW per migliorare il processo di mining sfruttando tecnologie di apprendimento Deep Learning.

Innanzittutto, è bene introdurre la differenza che c'è tra il Machine Learning, sfruttato nello progetto PAI, e il Deep Learning. Entrambe le metodologie sono due sotto-categorie dell'intelligenza artificiale e in sostanza servono per dimostrare che i computer sono in grado di prendere decisioni intelligenti. Il Machine Learning si basa sull'apprendimento supervisionato, mentre, il Deep Learning, su quello non supervisionato.

Il Machine Learning utilizza un algoritmo che viene prima istruito con dati strutturati e categorizzati, in modo che sia in grado di capire come classificare i nuovi dati a seconda del tipo. In base alla classificazione, il sistema esegue poi le attività programmate, ad esempio il riconoscimento degli oggetti. Dopo questa fase, l'algoritmo viene ottimizzato dal feedback umano, che indica al sistema quali sono le classificazioni errate e quali quelle corrette. Questo è il tipo di apprendimento supervisionato.

Nel caso del Deep Learning i dati strutturati non sono necessari. Questo approccio è particolarmente indicato per compiti complessi, quando non tutti gli aspetti degli oggetti possono essere categorizzati in anticipo. Infatti, è il sistema stesso a individuare le caratteristiche distintive adeguate, senza la necessità di una categorizzazione dall'esterno. L'addestramento da parte di uno sviluppatore non è necessario, ed è per questo che si parla di apprendimento non supervisionato. Il problema è che richiede molti più dati per poter fornire risultati affidabili, inoltre, è una tecnologia più complessa da implementare e più costosa del Machine Learning.

Tornando al progetto, come già detto, lo schema di mining richiede l'addestramento di modelli di Deep Learning e un blocco viene estratto solo quando le prestazioni di tale modello superano una certa soglia. Di seguito verranno forniti i dettagli in merito, descritti all'interno dell'articolo.

5.3.1 Requisiti Formali

In questa proposta, il problema da risolvere per poter aggiungere un nuovo blocco alla blockchain consiste nella risoluzione di un problema di intelligenza artificiale, tramite un modello di apprendimento automatico che deve essere addestrato e valutato. Nel rispetto delle seguenti proprietà:

1. Il problema deve essere complesso e richiedere uno sforzo computazionale, al fine di garantire che alcuni lavori effettivi siano stati eseguiti dai miner, i quali, a quel punto potranno ottenere la ricompensa prestabilita;

2. Per garantire l'integrità della blockchain è necessario introdurre come variabile del problema l'hash del blocco precedente;

3. Lo schema di mining deve avere una componente competitiva, in modo che sia il primo miner a risolvere il problema (o al contrario, il miner che fornisce la soluzione migliore) quello che estrae il blocco e ottiene la ricompensa;

4. Data la soluzione di un problema, deve essere facile verificarne la validità e la qualità.

5. Una volta che un miner ha trovato un blocco e questo è stato aggiunto alla blockchain, tutti gli altri potenziali blocchi in fase di mining, devono essere scartati. Ciò garantisce che un miner non possa "salvare blocchi" da scoprire in futuro.

5.3.2 PoUW nel Contesto Coin.AI

Lo scopo della proposta contenuta in questa sezione è la descrizione di una nuova rete blockchain che sostiene una moneta alternativa, ovvero "Coin.AI". Naturalmente, il fulcro della proposta è il meccanismo di prova del lavoro utile, che è descritto in questa sezione in modo che sia conforme ai requisiti delineati nella sezione precedente. Per soddisfare il primo requisito, propongono che il problema da risolvere da parte dei miner sia l'addestramento di un modello di intelligenza artificiale che è generalmente considerato un compito computazionalmente costoso e, dunque, soddisfa tale requisito.

In Figura 5.2 viene illustrato il processo di aggiunta di un nuovo blocco alla blockchain, riassunto come segue:

1. Ogni miner prende l'hash dell'ultimo blocco nella blockchain e sceglie un massimo di N transazioni tra quelle non confermate. Il valore di N rappresenta il numero massimo di transazioni memorizzate in un blocco. La scelta è indipendente e casuale. Infine, recupera un nonce, che si suppone sia generato casualmente;

2. I tre elementi verranno concatenati e il relativo hash verrà calcolato. Questo è l'hash del blocco candidato N + 1.

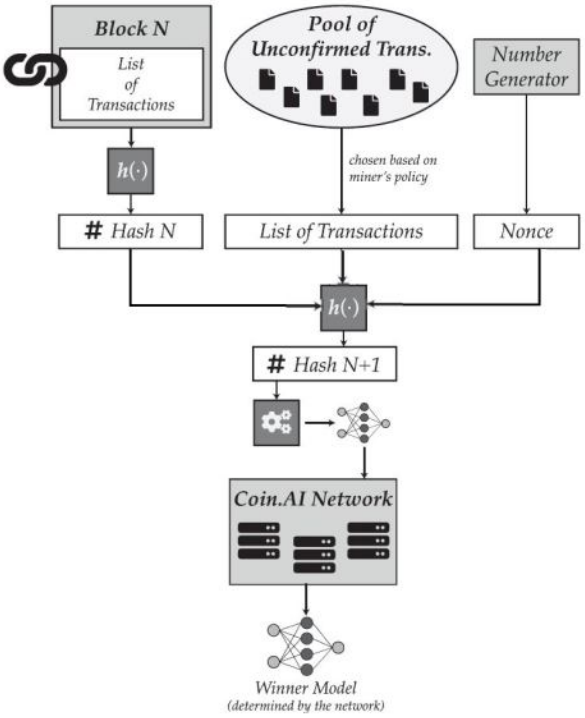

Figura 5.2: Processo PoUW nel contesto Coin.AI

3. L'hash ottenuto determinerà le caratteriste strutturali dell'architettura del modello di apprendimento da addestrare per ottenere un modello valido. Con architettura del modello ci si riferisce ad una grammatica generativa che presenta un insieme di regole di base e può essere modificata di volta in volta secondo le caratteristiche di questo hash. In questo modo, anche il secondo requisito viene soddisfatto, poiché l'hash viene introdotto come variabile del problema;

4. A questo punto, il miner può iniziare l'addestramento del modello. Per determinare chi deve aggiungere il blocco, invece di lasciare che vinca il primo che ottiene un modello, la decisione si basa su chi trova il modello migliore, rispettando quindi il terzo requisito;

5. Per scegliere un vincitore, verrà stabilita dalla piattaforma una soglia di prestazione minima, la quale, sarà ridotta col passare del tempo per consentire l'estrazione dei blocchi in un tempo ragionevole;

6. Durante questo periodo, tutti i miner possono proporre un blocco candidato. Dal momento che sono loro a scegliere i parametri di addestramento, saranno costretti a trovare un compromesso. Infatti, un allenamento scadente, ad esempio che coinvolge poche epoche di allenamento, si tradurrà in un modello non competitivo che difficilmente potrà superare la soglia di prestazione. Al contrario, una formazione molto esauriente potrebbe non essere in grado di fornire una soluzione rapida, consentendo a un altro miner di presentare una soluzione valida più velocemente e quindi di estrarre il blocco;

7. Se il modello supera la soglia di qualità, viene trasmesso alla rete per essere sottoposto ad un processo di convalida. Durante il quale si valuteranno anche le prestazioni del modello. Quest'ultima operazione è molto meno costosa rispetto all'addestramento, perciò, anche il quarto requisito è soddisfatto;

8. Se il modello non supera la soglia di qualità, non deve essere trasmesso alla rete per la valutazione in modo da risparmiare larghezza di banda. Il processo riparte dal punto (1), con un nuovo nonce o diverse transazioni;

9. Una volta determinato il modello vincente, cioè quando il blocco N+1 verrà estratto, tale blocco verrà aggiunto alla fine della blockchain. In questo modo, l'hash dell'ultimo blocco cambia, diventando ora l'hash del blocco appena estratto, questo implicherà necessariamente una modifica nell'architettura del modello e quindi tutti gli altri modelli dovranno essere scartati. Così facendo anche il quinto requisito viene soddisfatto. Infine, il processo può ripartire dal punto (1), per iniziare il processo di mining del blocco successivo.

5.3.3 Proof Of Storage

Un ulteriore problema che si pone con lo schema proof-of-work descritto in precedenza è dove memorizzare il modello vincente, cioè quello consegnato dal miner che ha estratto con successo il blocco. In questo contesto viene suggerito che solo alcuni nodi siano in grado di memorizzare i modelli. Di seguito verrà descritto il processo di Proof of Storage, cioè i passi che porteranno a questo salvataggio. Il tutto viene graficamente illustrato nella Figura 5.3.

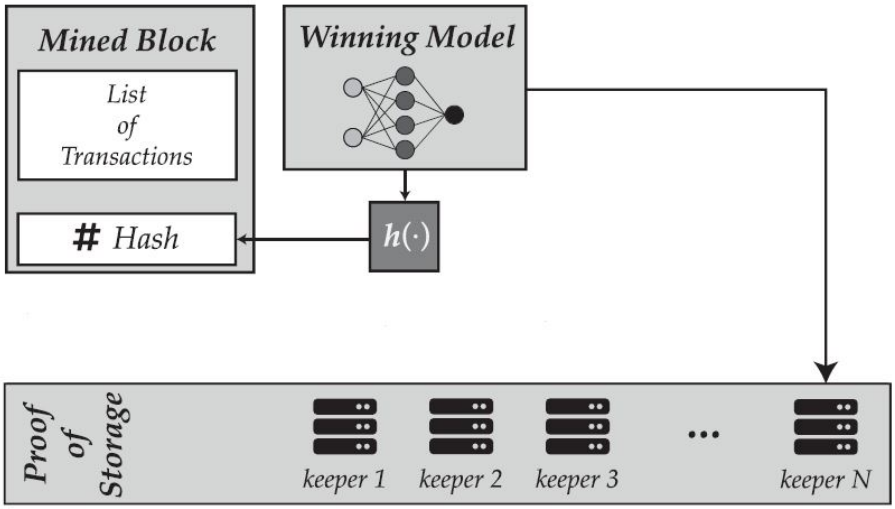

Figura 5.3: Schema Proof Of Storage Coin.AI

1. Una volta estratto un blocco, verrà calcolato un hash del modello di deep learning risultante che sarà allegato al blocco;

2. Il blocco verrà sottoposto a diversi nodi del sistema, denominati *custodi*, che memorizzeranno il modello. Il loro lavoro è simile a quello dei miner, ma invece di fornire potenza di elaborazione alla rete forniranno capacità di archiviazione. Inoltre, proprio come accade con i miner, i custodi saranno ricompensati per il loro lavoro, sotto forma di un certo valore della criptovaluta;

3. La prova di archiviazione funzionerà come un sistema distribuito con replica. Vale a dire, se un custode lascia la rete, verrà inviata una replica del modello ad un nuovo custode. Questo meccanismo fornisce la ridondanza necessaria per evitare la perdita di informazioni e garantisce un'archiviazione distribuita dei modelli di apprendimento addestrati;

4. Poiché un hash del modello è memorizzato nella blockchain, qualsiasi tentativo di un custode di manomettere una copia locale del modello verrebbe rilevato e potrebbe essere esposto. A quel punto la replica sarebbe considerata non valida e il custode verrebbe penalizzato per un tale comportamento.

Questo sistema potrebbe essere utilizzato anche per memorizzare i dati necessari per poter addestrare i modelli. In questo caso, poiché ai miner servirebbe un accesso rapido ai dati per addestrare i modelli, potrebbe essere utilizzato un fattore di replica più elevato, con una memorizzazione di copie locali nella cache. Ciò è fattibile poiché i dati richiederanno probabilmente molto meno spazio di tutta la cronologia dei modelli.

5.3.4 Risoluzione Democratica dei Problemi

Si potrebbero creare dei problemi di intelligenza artificiale durante il processo di mining. In nessun modo si saprà in anticipo quali vale la pena risolvere, poiché questa decisione sarà presa in base agli interessi della comunità e probabilmente cambierà nel tempo. L'interesse della comunità potrebbe dipendere da chi costituisce tale comunità, ma dovrebbe idealmente essere allineato con quegli interessi della comunità scientifica o anche della società in generale. Inoltre, consentendo ai possessori di poter scegliere problemi di proprio interesse da risolvere, si cerca di fornire un valore aggiunto alla valuta, dandole quindi stabilità e fattibilità a lungo termine.

La soluzione proposta prevede che qualsiasi detentore di valuta, anche se in quantità minima, possa proporre un nuovo problema da risolvere. Facendo riferimento a un "problema" si intende in realtà un set di addestramento e un set di convalida associato ad una metrica di qualità da calcolare su quest'ultimo, che può quindi essere utilizzato dai miner per apprendere i modelli e da altri nodi della rete per convalidarli. Oltre a proporre un nuovo problema, gli utenti devono essere in grado di supportare le proposte degli altri unendosi o votando su di loro.

La piattaforma può decidere in maniera casuale qual è il problema successivo da risolvere, ma sempre in proporzione alla quantità totale di valuta posseduta dai sostenitori di ciascun problema. In tal modo, viene fornito un accesso democratico alle risorse di rete, a chiunque ve ne faccia parte, e vengono incentivati quegli utenti che hanno una maggiore quantità di valuta.

Riassumendo in questo articolo è stato proposto un quadro teorico di uno schema di PoUW per il mining, in un ambiente blockchain, supportando una criptovaluta alternativa chiamata "Coin.AI". Lo scopo è quello di fare ricerche sull'architettura neurale, con potenziali implicazioni per il progresso dello stato dell'arte nell'intelligenza artificiale, sfruttando la tecnologia blockchain e cercando di fornire un elenco di requisiti che soddisfino una prova di lavoro utile.

Nella prossima sezione verrà descritto l'ultimo progetto realizzato basato, sul concetto di PoUW. Si tratta di un framework per lo sviluppo di applicazioni decentralizzate.

5.4 Proofware

Proofware è un prototipo di framework che nasce nel 2009 [DLZ19]. Gli ideatori hanno pensato di creare un'alternativa alla maggior parte dei protocolli di consenso, i quali non sono progettati per svolgere lavori utili a causa della troppa concorrenza e della limitazione della scalabilità e, inoltre, necessitano di un'enorme potenza elettrica e risorse di calcolo. Questo progetto, invece, consentirebbe agli sviluppatori di creare facilmente le loro applicazioni decentralizzate (dApp) con le risorse di elaborazione esistenti e crowd-based (letteralmente significa "basati sulla folla", quindi si intendono applicazioni di sviluppo collettivo).

Secondo le loro idee con un protocollo di consenso appropriato, una rete P2P e applicazioni decentralizzate (dApp), si potrebbero connettere tutte le risorse informatiche mondiali insieme per costruire un sistema informatico su larga scala basato sulla folla. Per risorse informatiche non intendono solo la CPU, l'archiviazione o la rete, ma anche altri dispositivi di input/output, come sensori, fotocamera, GPS, ecc. Uno sviluppatore potrebbe voler costruire un grande sistema di archiviazione distribuito affidabile in brevissimo tempo con un costo molto limitato. Per farlo basterebbe sfruttare gli spazi di archiviazione di riserva e le risorse di elaborazione distribuite su sistemi personali in tutto il mondo, come il PC di casa o il sistema commerciale, oppure l'archiviazione aziendale inutilizzata.

Dunque, questo progetto basato sulla Prova di lavoro utile (PoUW), consiste in:

1. Una valuta di applicazione indipendente decentralizzata e un progetto di adeguamento dei prezzi autonomo che può fornire un sistema di incentivi finanziari più efficace, trasparente e stabile in tutte le applicazioni;

2. Un contratto di servizio decentralizzato per definire i requisiti e la qualità del servizio (QoS);

3. Un'architettura flessibile che può supportare diverse applicazioni decentralizzate.

Il sistema di incentivi di Proofware, appreso da Bitcoin, aggiunge la funzione di scambio di credito autonomo e la funzione di scoperta dei prezzi, utilizzando un sistema di credito basato su blockchain per premiare tutti i proprietari di dispositivi e incentivarli a contribuire onestamente con i loro dispositivi alla rete. Utilizzano, inoltre, uno smart contract, in esecuzione sulla blockchain, per dare la possibilità allo sviluppatore di definire l'elenco di requisiti dei vari servizi. Di seguito verranno forniti maggiori dettagli su tutte queste implementazioni.

5.4.1 Architettura

L'architettura di questo framework è progettata per fornire una vasta gamma di servizi a chi ne fa uso, tra i quali: trasparenza degli algoritmi per costruire un sistema di elaborazione affidabile basato sulla folla; protocolli di consenso per una coerenza permanente e unanime dei nodi; software e indirizzi globali; comunicazione e archiviazione basate sul P2P per mantenere decentralizzazione e robustezza; supporto API e linguaggi di programmazione per consentire agli utenti di inserire la propria logica di business; il servizio SDK[8] per lo sviluppo e i test delle proprie dApp tramite risorse pubbliche; un sistema di incentivazione del credito basato su blockchain, il quale, fornisce la funzione di trasferimento crediti e negoziazione tra le varie dApp; una blockchain decentralizzata e pubblica che mantiene le informazioni sulla rete e può essere interrogata in qualsiasi momento.

[8] https://en.wikipedia.org/wiki/Software_development_kit

All'interno della piattaforma esistono, dunque, diversi parteciparti a cui sono associati dei ruoli. Di seguito viene fornito un elenco dettagliato.

1. **Sviluppatori di servizi pubblici**: sono gli utenti che utilizzano il framework Proofware per fornire servizi di informazione pubblica;

2. **Nodi di servizio pubblico (miner)**: possono provenire da server cloud, PC, dispositivi mobili, dispositivi IoT e così via. Si classificano in:

   - **Nodi di consenso**: supportano la personalizzazione del protocollo di consenso e forniscono meccanismi di consenso popolari come PoW, PoS e DPoS per impostazione predefinita;
   - **Nodi di raccolta delle informazioni**: raccolgono informazioni sui risultati degli eventi, sull'opinione pubblica e sul voto;
   - **Nodi di elaborazione**: per calcoli decentralizzati ad alte prestazioni;
   - **Nodi di archiviazione** : responsabili di una grande quantità di dati aziendali e di altri archivi di file di grandi dimensioni. Forniscono anche analisi dei dati e funzioni di intelligenza artificiale;
   - **Nodi IoT**: per il servizio di raccolta delle informazioni IoT (es. sensori per prevedere le condizioni del traffico);
   - **Nodi di arbitrato**: utilizzati per verificare i risultati rilevanti e regolare quando si verificano controversie;
   - **Nodi personalizzati**: in base alle esigenze e agli scenari aziendali, gli sviluppatori possono definire i propri nodi aziendali in base al modello del framework Proofware.

3. **Sviluppatore dApp**: utilizzano l'interfaccia del servizio pubblico e possono sfruttare gli incentivi esistenti di Proofware per la promozione di dApp e il funzionamento sostenibile. Inoltre, possono costruire le proprie reti informatiche e reti di consenso in base alle loro caratteristiche aziendali e costruire il proprio sistema di incentivi basato sul sistema di crediti di Proofware.

Il framework utilizza, inoltre, due algoritmi per il funzionamento del sistema di credito decentralizzato, quali:

1. **Algoritmo di scambio di crediti autonomo**: grazie al quale il credito viene scambiato istantaneamente sul portafoglio dell'utente senza attendere il prelievo da una piattaforma di centralizzata. Le commissioni sono minime poiché non sono presenti intermediari durante lo scambio di crediti;

2. **Algoritmo decentralizzato di rilevamento dei prezzi**: grazie al quale è possibile determinare il prezzo corretto del servizio calcolando la domanda e l'offerta di mercato senza un servizio di intermediazione centralizzato. Gli utenti possono sempre scambiare le unità di credito guadagnate tramite contratti intelligenti.

5.4.2 Esperimento OurTube

Come caso d'uso hanno creato un'applicazione per la condivisione di video basata sulla folla, chiamata **OurTube**. Con questa demo, vogliono dimostrare come una dApp creata con il sistema Proofware sia economica e affidabile, sostenendo che il costo di esecuzione è solo circa il 5,4% del costo di esecuzione su Amazon EC2.

Poiché non esiste un server centralizzato, nessuno può interrompere i server o rimuovere i contenuti, ma quest'ultimi e la politica di censura degli stessi possono essere gestiti in autonomia dalla folla, tramite regole definite nei contratti intelligenti. Dal momento che utilizzano un modello di prezzo decentralizzato sostengono che il sistema può prevenire la manipolazione del mercato e controllare la stabilità del prezzo delle risorse informatiche che possono supportare l'elasticità e la scalabilità dell'applicazione OurTube. Inoltre, sostengono che sia anche facile incorporare un sistema di incentivi finanziari autonomo e un sistema di revisione affidabile.

Per testare le prestazioni di OurTube sono stati utilizzati 40 PC virtuali collegati. Lo stesso carico di lavoro di riproduzione video è stato eseguito su un cluster Amazon EC2 centralizzato a 4 nodi. Infine, sono stati confrontati il costo e l'affidabilità tra le due.

Riassumendo, le caratteristiche di base di OurTube sono le seguenti:

- Trasmette uno streaming nella rete P2P e salva il video nel sistema di archiviazione basato sulla folla. Lo sviluppatore o il consumatore paga la tariffa e i fornitori di contenuti e servizi riceveranno una ricompensa;
- Il fornitore di contenuti o il consumatore possono richiedere che il flusso video venga codificato in più formati e dimensioni;
- I clienti possono guardare lo streaming da qualsiasi nodo e pagano la spesa tramite il portafoglio di credito dell'applicazione;
- L'alta scalabilità consente ai nodi della rete di codificare il video nel formato migliore per il dispositivo dello spettatore;
- Riduzione dei prezzi di archiviazione, trasporto, codifica e decodifica, con meccanismi di incentivazione finanziaria basati su blockchain;
- Non è controllato da nessuna entità e grazie all'algoritmo di rilevamento dei prezzi decentralizzato nessun indicatore di mercato può manipolare il prezzo della risorsa.

Per l'esperimento, hanno utilizzato 1000 client in contemporanea per visualizzare un flusso video di 2 settimane. Dal confronto tra il sistema centralizzato di Amazon EC2 e OurTube sono emersi i seguenti dati statistici:

- **Affidabilità**: OurTube ha raggiunto un'affidabilità del 99,5%, rispetto al 99,7% di Amazon EC2;
- **Costo**: OurTube utilizza circa il 5% del costo Amazon EC2. Quest'ultimo costa circa 128,5$ australiani, mentre, OurTube circa 7$ australiani, all'interno del loro ambiente simulato;
- **Latenza**: OurTube ha riscontrato un notevole ritardo durante la fase iniziale di connessione. Complessivamente, ha raggiunto un ritardo di 240,5 millisecondi, rispetto al ritardo di 136 millisecondi di Amazon EC2. Sostengono che sia comunque un risultato abbastanza buono per una soluzione basata sulla folla e che diventerà normale dopo che il nodo avrà trovato sempre più nodi nella rete peer-to-peer.

In conclusione sostengono, anche a seguito dello sviluppo di questa demo, che il loro framework Proofware offre la capacità di sviluppare dApp in modo efficace. Il meccanismo di rilevamento dei prezzi efficace e l'algoritmo di scambio automatico del credito che hanno ideato, migliorerebbero la trasparenza e l'autonomia dell'intero sistema, al fine di prevenire la corruzione e la manipolazione dei prezzi. Grazie alla blockchain e agli smart contract, Proofware promuove in modo significativo il crowd-based computing. Inoltre, sostengono che i loro risultati verificano le affermazioni con una buona redditività ed efficienza dei costi, rispetto ai classichi approcci, per costruire un sistema di elaborazione su larga scala con funzionalità decentralizzate. Per il futuro hanno in programma di indagare ulteriormente su come proteggere la privacy nel sistema in questione.

Tuttavia, ad oggi, dopo circa 11 anni, questo framework non risulta ancora in commercio e rimane pertanto un altro modello teorico basato su una prova di lavoro utile. Nel prossimo capitolo verrà fornito un resoconto finale di quanto descritto nell'intero elaborato.

Conclusioni

In questo elaborato si è discusso del modello Bitcoin, di come nel corso degli anni abbia acquisito maggiore visibilità e di come tanti altri sviluppatori abbiano provato a mettere in campo dei sistemi che fossero altrettanto competitivi. Si può dire che la nascita di Bitcoin abbia stimolato i programmatori più appassionati a sperimentare nuove idee innovative, alcuni hanno sfruttato il fatto che il codice sia completamente open source e lo hanno usato come base per altri progetti, alcuni ne hanno copiato degli aspetti. Inoltre, si è addirittura verificato un ammutinamento, se così lo si può definire, che ha portato una scissione all'interno del team di sviluppatori di Bitcoin, per ragioni già ampiamente trattate.

Lo scopo di questo ultimo capitolo è quello di fare un bilancio di quanto appreso fino a questo momento. Creare un sistema come Bitcoin è stata senza dubbio un'idea innovativa che se sfruttata in modo lecito può portare notevoli vantaggi, tuttavia, si tratta di una tecnologia ancora in fase di sviluppo che può sicuramente essere migliorata. Più che sugli aspetti positivi, in questo elaborato, la necessità era quella di effettuare delle ricerche in merito agli aspetti negativi, in special modo, i problemi che Bitcoin ha causato nel corso di questi anni rispetto all'ambiente.

Come già visto nelle sezioni precedenti, sono state molte le persone che si sono allarmate leggendo di anno in anno le statistiche legate allo spreco di risorse e ai problemi ambientali che ne derivano. Alcuni hanno proposto come soluzione l'utilizzo di energie rinnovabili, per limitare l'emissione di CO2 e ridurre il consumo di energia. Altri hanno proposto delle modifiche strutturali all'architettura di Bitcoin.

Sono stati sviluppati/teorizzati anche dei progetti basati sul concetto di PoUW che si possono considerare una valida alternativa al classico PoW. Tuttavia, nessuna di queste proposte è stata presa in considerazione e non è ben noto il motivo, ma sotto certi aspetti si può pensare che gli sviluppatori non vogliano alterare la natura del protocollo. Ad esempio, una delle proposte è stata quella di aumentare la dimensione dei blocchi per migliorare le prestazioni del sistema, ma questo comporterebbe un rallentamento dell'intero processo nonché un aumento notevole delle dimensioni della Blockchain. La conseguenza è che alcuni nodi potrebbero non essere in grado di continuare a gestirla nella sua totalità e in completa autonomia, quindi, si perderebbe la decentralizzazione dei nodi, un altro motivo che spinge gli sviluppatori a non voler procedere in questo senso.

Il problema è che le statistiche legate all'impatto ambientale continuano a peggiorare. Sono stati in tanti ad affermare che se le emissioni di CO2 continueranno ad aumentare con questi ritmi, così come la quantità di energia spesa, si spingerà il riscaldamento globale sopra i 2°C nel giro di pochi decenni. Quindi, è stata loro premura fare anche un appello alle autorità e ai governi dei vari stati, per indurli ad intervenire il più presto possibile.

In realtà la necessità di tutta questa energia non è dovuta a cause strutturali ma dipende dalla competizione dei miner durante il processo di estrazione dei blocchi, visto che si effettuano molti calcoli nel giro di pochi secondi il consumo energetico complessivo è molto alto. Dunque, quando la competizione si abbassa si riduce anche il consumo. Questo fenomeno si manifesta temporaneamente dopo il dimezzamento del premio dei miner (o halving), descritto in precedenza. Tutto dipende dal fatto che il mining è un'attività profit, ovvero che deve generare profitto. In altre parole, i miner che non generano un buon profitto interrompono l'attività per non creare gravi perdite economiche.

Come già detto, il protocollo Bitcoin prevede un aggiustamento automatico, che avviene circa ogni due settimane, della cosiddetta "difficulty", ovvero la difficoltà legata alla risoluzione del puzzle crittografico e quindi del tempo impiegato per convalidare un blocco. Questa consente di mantenere una media di 10 minuti.

Il grado di difficoltà è strettamente correlato alla potenza di calcolo complessiva a disposizione dei miner (l'hashpower). Se questa si riduce allora la difficoltà diminuisce e viceversa. Quando si verifica il dimezzamento del premio alcuni miner devono interrompere l'attività di mining per non causare perdite e questo può comportare un aumento momentaneo del tempo medio per l'estrazione dei blocchi. Tempo che comunque si ristabilizza dopo qualche giorno. Con l'ultimo halving, avvenuto l'11 maggio 2020, i consumi si sono ridotti di circa il 22% e attualmente i valori riportati [Dig21] sono i seguenti:

Consumo annuale

- Impronta di carbonio: 36,95 Mt CO2. Paragonabile all'impronta di carbonio della Nuova Zelanda;
- Energia elettrica: 77.78 TWh. Paragonabile al consumo di energia del Cile;
- Rifiuti elettronici: 11.19 kt. Paragonabile alla generazione di rifiuti elettronici del Lussemburgo.

Consumo delle singole transazioni

- Impronta di carbonio: 309,26 kgCO2. Equivalente all'impronta di carbonio di 685.438 transazioni VISA o 51.544 ore di visione di Youtube;
- Energia elettrica: 651,08 kWh. Equivalente al consumo di energia di una famiglia americana media in 22,32 giorni;
- Rifiuti elettronici: 93,72 g. Equivalente al peso di batterie da 1,44 pollici o 2,04 palline da golf.

Dal momento che questi halving si verificano ogni 4 anni circa, fino a che il premio per i miner non sarà completamente azzerato, queste riduzioni sono destinate a ripetersi anche in futuro, ma si tratta di riduzioni momentanee. A meno che, il valore di Bitcoin non diminuisca, il quel caso il numero di miner diminuirebbe a sua volta riducendo i consumi energetici.

Attualmente non sembra che questo possa avvenire in tempi brevi e non si sa quando o se realmente avverrà. Quindi se i dati continueranno a peggiorare, secondo una considerazione personale, ad un certo punto le autorità interverranno e cercheranno in qualche modo di appropriarsi di questa risorsa, per poterne controllare gli effetti. A quel punto, gli sviluppatori dovranno fare una scelta, cedere la proprietà andando contro ai loro principi e alla natura decentralizzata del progetto, oppure, attuare il prima possibile delle contromisure per impedire che si arrivi a questo bivio.

Un altro aspetto da considerare sarà l'ultimo halving, previsto nell'anno 2140, a seguito del quale verrà estratto il 21.000.000° BTC. Anche in quell'occasione gli sviluppatori saranno chiamati ad una scelta: estendere le proprietà del protocollo per continuare a garantirne il funzionamento o dismettere il sistema. Vista, però, la rapidità con la quale il consumo di energie e risorse aumenta, il 2140 è un tempo troppo remoto e quasi sicuramente questo tipo di decisioni dovranno essere prese molto prima. Per concludere, al momento si può dire che queste misure di contenimento non sono state attuate e il futuro di Bitcoin rimane incerto.

Bibliografia

[Act20] Bitcoin in Action. *Che cosa è lo SHA256?* Nov. 2020. URL: https://www.corsobitcoin.com/che-cosa-e-losha256-bitcoin/.

[Ast16] Tomaso Aste. "The fair cost of Bitcoin proof of work". In: *Available at SSRN 2801048* (2016).

[BS19] Alejandro Baldominos e Yago Saez. "Coin. AI: A proof-of-useful-work scheme for blockchain-based distributed deep learning". In: *Entropy* 21.8 (2019), p. 723.

[BLS04] Dan Boneh, Ben Lynn e Hovav Shacham. "Short signatures from the Weil pairing". In: *Journal of cryptology* 17.4 (2004), pp. 297–319.

[Dig21] Digiconomist. *Bitcoin Energy Consumption Index - Digiconomist.* https://digiconomist.net/bitcoin-energy-consumption. (Accessed on 02/10/2021). 2021.

[DF19] Şerif Dilek e Yunus Furuncu. "Bitcoin Mining and Its Environmental Effects". In: *Ataturk University Journal of Economics & Administrative Sciences* 33.1 (2019), pp. 91–105.

[DLZ19] Zhongli Dong, Young Choon Lee e Albert Y Zomaya. "Proofware: Proof of useful work blockchain consensus protocol for decentralized applications". In: *arXiv preprint arXiv:1903.09276* (2019).

[ET17] Jacob Eberhardt e Stefan Tai. "On or off the blockchain? Insights on off-chaining computation and data". In: *European Conference on Service-Oriented and Cloud Computing*. Springer. 2017, pp. 3–15.

[EO20] Modesta Amaka Egiyi e Grace Nyereugwu Ofoegbu. "CRYPTOCURRENCY AND CLIMATE CHANGE: AN OVERVIEW". In: *International Journal of Mechanical Engineering and Technology (IJMET)* 11.3 (2020), pp. 15–22.

[Ken19] Will Kenton. *Off-Chain Transactions (Cryptocurrency) Definition*. Ott. 2019. URL: https://www.investopedia.com/terms/o/offchain-transactions-cryptocurrency.asp#:~:text=Off-chain%20transactions%20refer%20to,popularity,%20especially%20among%20large%20participants..

[Kin13] Sunny King. "Primecoin: Cryptocurrency with prime number proof-of-work". In: *July 7th* 1.6 (2013).

[KD20] Kateryna Kononova e Anton Dek. "Bitcoin Carbon Footprint: Mining Pools Based Estimate Methodology". In: *Proceedings of the 9th International Conference on Information and Communication Technologies in Agriculture, Food & Environment (HAICTA 2020)* (2020).

[LS19] Jacob Leshno e Philipp Strack. "Bitcoin: An Impossibility Theorem for Proof-of-Work based Protocols". In: *Cowles Foundation Discussion Paper* (2019).

[Lih+20] Andrei Lihu et al. "A Proof of Useful Work for Artificial Intelligence on the Blockchain". In: *arXiv preprint arXiv:2001.09244* (2020).

[MGT18] June Ma, Joshua S Gans e Rabee Tourky. *Market structure in bitcoin mining*. Rapp. tecn. National Bureau of Economic Research, 2018.

[Mor+18] Camilo Mora et al. "Bitcoin emissions alone could push global warming above 2 C". In: *Nature Climate Change* 8.11 (2018), pp. 931–933.

[Nai+20] Rajit Nair et al. "An approach to minimize the energy consumption during blockchain transaction". In: *Materials Today: Proceedings* (2020).

[Nak08] Satoshi Nakamoto. "A peer-to-peer electronic cash system". In: *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf* 4 (2008).

[Nar+16] Arvind Narayanan et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

[PD15] Joseph Poon e Thaddeus Dryja. "The bitcoin lightning network". In: *Scalable o-chain instant payments* (2015).

[Shi16] Ning Shi. “A new proof-of-work mechanism for bitcoin”. In: *Financial Innovation* 2.1 (2016), p. 31.

[SKG19] Christian Stoll, Lena Klaaßen e Ulrich Gallersdörfer. “The carbon footprint of bitcoin”. In: *Joule* 3.7 (2019), pp. 1647–1661.

[Tas19] John Taskinsoy. “Blockchain: An Unorthodox Solution to Reduce Global Warming”. In: *Available at SSRN 3475144* (2019).

[Vri18] Alex De Vries. “Bitcoin’s growing energy problem”. In: *Joule* 2.5 (2018), pp. 801–805.

Ringraziamenti

Ringrazio il mio relatore, Ugo Dal Lago, per avermi permesso di realizzare questo progetto di tesi in tempi record, per la pazienza, la disponibilità e i consigli dati.

Ringrazio i miei genitori, per non aver mai smesso di incoraggiarmi a continuare e per le parole di conforto nei momenti di difficoltà. Non è stato un percorso facile per mille motivi, ma se sono riuscita a raggiungere quest'ultimo traguardo che chiude il cerchio lo devo soprattutto a loro, quindi infinite grazie.

Ringrazio mia sorella, che con pazienza ha letto tutta la tesi (giusto poche pagine) e, da brava insegnante qual è, mi ha corretto gli errori con la penna rossa facendomi tornare con la mente alle scuole medie. Ecco il voto, però, teniamolo segreto. Come per la triennale sostiene di aver compreso tutto, fidiamoci. Se non avrete più mie notizie dopo quest'affermazione saprete il perché.

Ringrazio il mio responsabile in azienda, Tommaso Pesante, in generale per la fiducia riposta in me in questi anni e, soprattutto, per avermi concesso il tempo che mi serviva per dedicarmi alla stesura della tesi.

Ringrazio anche i miei compagni di team, che col tempo si è allargato, Juri Castellani, Valentina Dallolio, Francesco Lauriola, Marco Salomé, Giusy Rossi, per la pazienza e il sostegno durante i miei primi mesi in azienda e, alcuni di loro in particolare, per essersi fatti carico del mio lavoro nei giorni in cui non ci sono stata, mi sdebiterò.

Ringrazio la mia collega preferita nonché amica super, Giulia Baccolini, per tutto quello che abbiamo condiviso nel lungo percorso universitario, per quello lavorativo che spero condivideremo a lungo e che è cominciato grazie a te. Grazie per i momenti belli, che ci hanno fatto divertire come matte. Grazie per i momenti brutti, che ci hanno rese più forti. Grazie per i consigli, per la pazienza e per il supporto che mi hai dato, soprattutto, in questi ultimi mesi, per aver creduto che potessi farcela quando io avevo perso le speranze. Grazie per essere quello che sei e per lo psicologo che mi pagherai per continuare a sopportarti, anzi, probabilmente dovrò pagarlo io.

Ringrazio un altro collega Dario Loiacono, che definisco con piacere non un amico ma un "fratello mancato". Grazie per esserci stato nei momenti di sconforto, per avermi supportata e sopportata, i tuoi consigli da "nonnetto" mi sono serviti molto. Grazie per le risate, le chiacchierate, le disavventure e, soprattutto, per la fiducia che hai riposto in me, con i miei tempi penso di essere riuscita a ricambiare. Ringraziami perché non sto divulgando il tuo soprannome in mondo visione, ma sicuramente sto suscitando la curiosità di molti. Se tu non lo conoscessi già, saresti il primo tra i curiosi.

Ringrazio Francesca Francica, una collega che col tempo si è rivelata un'amica e consigliera speciale. La definisco lo Xanax naturale, per la pace e la tranquillità che sa infondere e per la saggezza che manifesta in alcune situazioni, ho fatto tesoro di tante preziose parole. Grazie, soprattutto, per quel nostro momento a Verona in cui ci siamo dovute confrontare per raccontare di noi agli altri, ci ha aiutato a capire che in comune non abbiamo solo il nome, il gruppo sanguigno e il disagio.

Ringrazio Federica Licciardi, per essere semplicemente la mia persona (forse non tutti capiranno la citazione), il pezzo mancante del puzzle come si suol dire. Non so bene che parole usare perché ci sono ancora tante cose che non mi spiego, forse sono gli occhi azzurri che mi fregano. Grazie per non aver mollato la presa ed essere stata forte per entrambe, io non ce l'avrei fatta. Grazie per quel "così tanto in così poco" che ha reso speciale quest'amicizia.

Ringrazio gli altri colleghi di lavoro, i colleghi dell'università, dello stadio, la squadra di calcetto, gli amici di sempre e tutte le persone che ho conosciuto da 10 anni a questa parte, avete contribuito a modo vostro nel rendermi la persona che sono, lascio giudicare a voi se sono cambiata in meglio o in peggio. Non me ne vogliate se non ho fatto il nome di ognuno di voi, la tesi è già abbastanza lunga e diversi alberi hanno dato la loro vita per questo, vi porto tutti nel cuore lo stesso.

Ringrazio anche quelli che negli ultimi anni, invece, sono spariti per motivi misteriosi o perché era meglio così, qualcosa mi avete lasciato anche voi e ne farò tesoro.

Francesca Grillo