



Bitcoin: Tecnologie e Applicazioni

Relazione finale per il corso di Crittografia

Elia Zavatta

A.A. 2021/2022

Professore: Luciano Margara

Indice

1	Introduzione	2
2	Storia	3
2.1	Dalla crittografia alle criptovalute	3
2.2	I predecessori	3
2.3	La nascita di Bitcoin	5
2.4	La diffusione fino ad oggi	5
3	Tecnologie	8
3.1	La Blockchain	8
3.2	Come si svolge una transazione di bitcoin	9
3.3	Il ruolo del Mining e la Proof of Work	14
3.3.1	Il problema ambientale e la Proof of Stake	17
3.4	L'architettura Peer-to-Peer	18
4	Applicazioni	21
4.1	Altcoins	21
4.1.1	Ethereum e gli smart contracts	21
4.1.2	Stablecoins	23
4.2	Binance, l'exchange più grande al mondo	24
4.3	NFT	25
5	Conclusioni	27
A	L'utilizzo della funzione Hash	28
A.0.1	SHA256	29
A.0.2	RIPEMD160	29
B	Merkle tree	30

Capitolo 1

Introduzione

Una delle innovazioni tecnologiche di cui si è sentito maggiormente parlare negli ultimi anni è senza dubbio Bitcoin. La sua rapida espansione è dovuta soprattutto alla speculazione in atto sul suo valore monetario "variabile", ma cos'è Bitcoin?

Come dice il nome, Bitcoin è una "moneta" fatta di bit, più precisamente è una **criptovaluta**: una valuta digitale indipendente da qualsiasi unità centrale che utilizza la crittografia per verificare le transazioni e regolare l'emissione di nuove unità di valuta.

Bitcoin è la prima e più famosa criptovaluta creata, dopo anni mantiene ancora la testa del mercato.

Capitolo 2

Storia

La nascita di Bitcoin è piuttosto recente, per capirne le origini è necessario fare qualche passo indietro partendo dalla storia della crittografia.

2.1 Dalla crittografia alle criptovalute

Inizialmente la crittografia era uno strumento utilizzato esclusivamente dalle istituzioni per mantenere la segretezza di piani o operazioni, negli anni '70 con l'espansione dell'era digitale e il conseguente bisogno di privacy nell'uso di dispositivi tecnologici questa tecnologia divenne pubblica.

Rendere la crittografia alla portata di tutti conseguì un aumento della privacy nei servizi di pagamento offerti dalle banche e, successivamente, la nascita di sistemi di pagamento elettronici che usavano denaro virtuale.

L'idea di una **criptomoneta** non è completamente innovativa, sin dagli albori di internet ci sono stati tentativi di creazione di una moneta virtuale, tuttavia non si è mai riusciti a risolvere problematiche connesse alla natura del dato informatico, afflitto da fenomeni non autorizzati di copia in quanto dato digitale.

2.2 I predecessori

Nel 1983 venne creato il primo sistema di pagamenti virtuali eCash ad opera della "DigiCash Inc.", fondata dal crittografo americano David Chaum.

L'innovazione stava nel contenere il denaro virtuale nel proprio computer e poterlo spendere per acquisti su Internet o nei negozi che lo accettavano, il

tutto quindi senza passare attraverso circuiti bancari. Le banche si dimostrarono ostili a questo sistema di pagamenti, in molte non lo accettarono impedendo così ad e-cash di crescere e facendo fallire la Digicash.



Logo di eCash

Un altro esempio di un predecessore di Bitcoin è quello di **e-gold**, una moneta digitale creata dalla società "Gold and Silver Reserve Inc." nel 1996, detenere questa valuta quindi significava detenere una certa quantità di metalli preziosi presso la Gold and Silver Reserve.

E-gold poteva essere usata per trasferimenti di denaro istantanei tra privati e per acquisti on-line, questo comportò l'adozione di questa valuta da sempre più persone fino a che nel 1999 il mercato crebbe talmente tanto da provocare la nascita di piattaforme di exchange indipendenti.

Nel 2007 e-gold venne accusato dal governo statunitense di permettere il riciclaggio del denaro provocando il definitivo blocco degli account e delle transazioni nel 2009.

La gran parte dei sistemi di pagamento virtuali esistenti fino a prima degli anni 2000, tra cui quelli appena descritti, erano sistemi centralizzati ovvero avevano come pilastro portante una banca o un'istituzione che ne regolava il funzionamento e ne garantiva le transazioni.

La svolta dal punto di vista concettuale avvenne nel 1998 anno in cui il programmatore Wei Dai e il crittografo Nick Szabo propongono entrambi separatamente due diversi sistemi di pagamento decentralizzati.

Wei Dai creò una moneta chiamata **b-money** basata su alcune caratteristiche riscontrabili tutt'ora in Bitcoin: la creazione di moneta si effettua tramite risoluzione di problemi mediante una certa potenza di calcolo, le transazioni avvengono attraverso una firma digitale e infine gli utenti si registrano in un network anonimo tramite pseudonimi o nomi che non ne rivelino l'identità. Nello stesso periodo Nick Szabo ideò **bit-gold**, anche in questo caso la creazione di moneta avveniva grazie a calcoli effettuati da diversi processori, nello specifico i calcolatori devono trovare la cosiddetta "challenge string", ovvero una stringa di bit tramite un processo definito "proof-of-work".



Operatore di e-gold.



Logo di Bit-gold.

Ogni challenge string è unica e può essere rilevata da un solo utente (il primo in ordine cronologico che riesce a trovarla) e solo una volta terminata la ricerca della stringa precedente si può passare alla successiva; l'utente che riesce a rintracciare per primo tale stringa la fa propria ed è di conseguenza autorizzato a spenderla: in questo modo nel sistema bit-gold viene generata "moneta".

Tutti gli eventi appena descritti contribuirono in modi diversi alla nascita di Bitcoin.

2.3 La nascita di Bitcoin

Nel Novembre del 2008 un certo Satoshi Nakamoto pubblicò su Internet un documento intitolato “Bitcoin: A Peer-to-Peer Electronic Cash System” il cui obiettivo era spiegare come fosse possibile il trasferimento di denaro digitale senza avere come tramite un’istituzione finanziaria o qualsiasi altro ente.

Da allora Satoshi Nakamoto è riconosciuto come il creatore di Bitcoin, ma sulla sua identità si sa ben poco: si ritiene che tale nome sia in realtà uno pseudonimo che nasconde una persona estremamente esperta di crittografia o un’organizzazione.

La data ufficiale in cui è stato emesso il primo blocco di bitcoin (“blocco 0” o “genesis block”) è il 3 Gennaio 2009 e il 12 Gennaio dello stesso anno venne registrata la prima transazione con cui Satoshi Nakamoto invia 10 BTC ad un esperto crittografo.

2.4 La diffusione fino ad oggi

Ovviamente nei primi mesi di vita dei bitcoin il loro valore era irrilevante, gli unici a possederne erano gli sviluppatori che li avevano generati e non esistevano nemmeno quelle piattaforme online che permettevano il cambio con la valuta tradizionale, detti in seguito exchange.

L’obiettivo principale degli sviluppatori e di questo forum era diffondere sia la conoscenza della criptovaluta che la criptovaluta stessa in modo da coinvolgere sempre più utenti e in modo da ingrandire il sistema Bitcoin; per

raggiungere tale scopo vennero create transazioni di qualsiasi tipo tramite le quali i possessori di bitcoin acquistavano praticamente qualsiasi cosa al solo fine di diffondere informazioni: la più famosa di queste transazioni è avvenuta ad opera del programmatore Laszlo Hanyecz il quale offrì 10.000 Bitcoin (pari a circa 25 dollari all'epoca) per due pizze: tale operazione passò poi alla storia come la “pizza da 10.000 BTC”.

Transaction View information about a bitcoin transaction

a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d	
1XPtgDRhN8RFnznIWCddobD9lKZatrVH4	→ 17SkEw2md5avVNyYgj6RlXuQKNwkXaxFyQ
	10,000 BTC
10,000 BTC	
Summary	Inputs and Outputs
Size	23620 (bytes)
Weight	94480
Received Time	2010-05-22 18:16:31
Included In Blocks	57043 (2010-05-22 18:16:31 + 0 minutes)
Confirmations	519889
Visualize	View Tree Chart
Show scripts & coinbase	

Dettaglio della transazione della pizza da 10.000 BTC

Nel 2010 vennero creati i primi exchange e ciò provocò una perdita di controllo sulle transazioni per gli sviluppatori, con gravi conseguenze: nell'agosto del 2010 venne scovato un punto debole nel sistema di sicurezza, ovvero le transazioni non venivano controllate in modo preciso ed esaustivo prima di venire registrate; ciò permise ad un gruppo di hacker anonimi di generare dal nulla un blocco del valore di 184 milioni di BTC e di spenderli in molteplici modi.

In poco tempo gli sviluppatori intervennero correggendo il bug del sistema e annullando le transazioni fasulle.

Il 2011 è l'anno in cui il mondo ha iniziato a rendersi conto dell'esistenza di Bitcoin, infatti il suo utilizzo crebbe rapidamente; molte associazioni iniziarono ad accettare tale criptovaluta per le donazioni e vennero aperti moltissimi siti web per scambiare bitcoin con prodotti di qualsiasi tipo.

Nel biennio 2012-2013 aumentò moltissimo il numero dei commercianti in grado di accettare pagamenti in bitcoin grazie soprattutto alla semplificazione dei processi di pagamento e all'attivazione di sistemi (ad esempio Bitpay,

CoinBase e GoCoin) che permettono ai negozianti e alle imprese di convertire i bitcoin in valuta locale.

Utilizzato a fini illegali per la sua anonimità delle transazioni, nel 2013 la Fbi chiuderà il famigerato mercato della droga online Silk Road, sequestrando 3,6 milioni di dollari in bitcoin.

Nel 2015 la startup di San Francisco Coinbase lancia il primo exchange regolato degli Usa. Il co-fondatore Fred Ehrsam dichiara: “In qualche modo, questo aiuterà davvero a ridurre la volatilità”.

Nel 2017 il valore raggiunge l'enorme cifra di 19.800 dollari, a fine dell'anno successivo scende a neanche un quinto.

A fine 2021 Elon Musk, proprietario di Tesla Inc. , accetterà bitcoin come pagamento per le sue macchine, per poi far retromarcia qualche mese dopo a causa della non sostenibilità della moneta, infatti i costi per mantenere il sistema Bitcoin sono elevatissimi e gran parte dell'energia deriva da fonti non rinnovabili.

Questa mossa farà oscillare notevolmente il prezzo dell'asset, che da più 60 mila dollari dimezzerà il suo valore e che, come dalla sua nascita, non troverà mai una stabilità fino ad oggi, rendendolo più uno strumento di speculazione rispetto ad una riserva di valore.



Grafico storico del valore di bitcoin dal 2013 ad oggi (maggio 2022)

Capitolo 3

Tecnologie

Il successo di Bitcoin è dovuto alle tecnologie estremamente innovative e rivoluzionarie su cui è sviluppato, tali da permettere la forte espansione di questi anni.

3.1 La Blockchain

A svolgere la funzione di registro digitale delle transazioni c'è la Blockchain: una struttura dati condivisa ed immutabile, fatta di blocchi che memorizzano al loro interno tutti i trasferimenti validi avvenuti.

In ogni blocco è contenuto il valore di hash (generato dalla funzione di hash che approfondiremo nel capitolo successivo) del blocco precedente, questo consente verificare l'integrità del blocco e di collegare insieme i blocchi consecutivi formando una catena in cui ogni anello aggiuntivo rinforza quello precedente.

Da un punto di vista tecnico la Blockchain è un insieme di blocchi contenenti transazioni, posti in ordine cronologico a partire dal **Genesis block**: il primo blocco generato.

Rappresenta un'importante innovazione per via della sua natura decentralizzata: ogni cambiamento ed aggiornamento sulla Blockchain è pubblicamente visibile ad ogni utente, seguendo lo stesso approccio dei sistemi Peer-to-Peer (argomento approfondito nel capitolo 3.4).

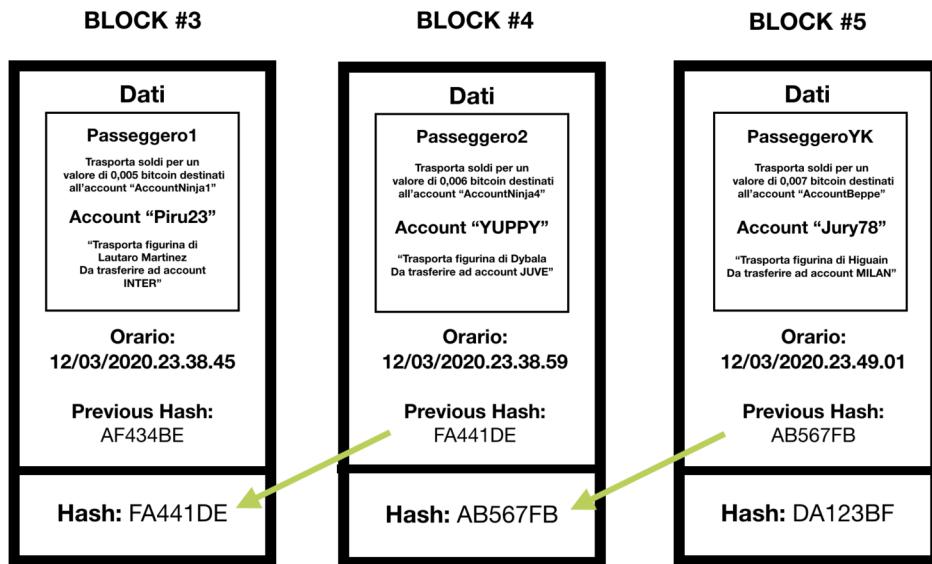
Questo permette di evitare un Single Point of Failure(SPoF, singolo punto di fallimento) non avendo un punto della rete in cui è concentrata tutta la sicurezza e l'integrità del sistema, sarà più difficile da attaccare.

Inoltre nei sistemi centralizzati bisogna riporre la propria fiducia in un'autorità centrale che gestisce tutta la rete, mentre i sistemi basati su Blockchain vengono definiti **trustless** (senza fiducia) perché tutti i nodi della rete sono

allo stesso livello di importanza.

Questi nodi sono entità indipendenti (persone o gruppi di persone) che mettono a disposizione del sistema la potenza di calcolo dei loro calcolatori, ognuno di loro è identificato con un indirizzo.

Ogni transazione viene eseguita nel giro di un'ora, è anonima e una volta registrata non può essere alterata o cancellata, questo porta ad un alto livello di sicurezza del sistema.



Esempio di collegamento dei blocchi della blockchain

3.2 Come si svolge una transazione di bitcoin

Una transazione è uno scambio di bitcoin tra due utenti, Bitcoin utilizza la crittografia in chiave pubblica: vengono generate 2 chiavi di cui quella pubblica può essere diffusa, mentre quella privata deve rimanere a conoscenza del solo proprietario. La loro principale caratteristica è che ciò che viene cifrato con la chiave pubblica può essere decifrato solo con la chiave privata. Ora vediamo nel dettaglio come si svolge una transazione identificando Bob come il ricevente, Alice il pagante [3].

1. Bob genera in modo del tutto casuale un numero intero senza segno lungo 256 bit che diventerà la sua chiave privata, è noto solo all'utente a cui fa riferimento ed è l'unico modo per attestare che le criptovalute sono di sua proprietà.

2. La chiave privata viene convertita in una chiave pubblica tramite un procedimento matematico basato sull'algoritmo ECDSA (**Elliptic Curve Digital Signature Algorithm**), che utilizza la curva ellittica Secp256k1 di equazione $y^2 = x^3 + 7$ definita negli **Standards for Efficient Cryptography** (SEC).

Il software di Bob genera automaticamente le chiavi quando Bob chiede all'applicazione di creare un indirizzo da comunicare al mittente.

È teoricamente possibile ma statisticamente impraticabile scoprire la chiave privata partendo da quella pubblica: il procedimento matematico applicato è unidirezionale, il processo inverso per indovinare la chiave privata richiederebbe una quantità di tentativi e una potenza di calcolo talmente enorme da essere al di là di ogni possibilità.

Se ci fosse un supercomputer in grado di indovinare la chiave privata, allora probabilmente qualsiasi password nel mondo sarebbe vulnerabile e i bitcoin potrebbero non essere la prima fonte di preoccupazione.

3. Per generare l'indirizzo del portafoglio di Bob partiamo dalla chiave pubblica, che viene convertita per praticità in una stringa di massimo 35 caratteri utilizzando ripetutamente l'algoritmo di hashing SHA256 (appendice A.0.1) e l'algoritmo RIPEMD160(appendice A.0.2). Come ultimo passaggio l'output viene riportato in Base58, codifica inventata da Nakamoto per eliminare i caratteri non alfanumerici e quelli molto simili tra loro.
4. Bob spedisce il suo indirizzo ad Alice.
5. Il software di Alice decodifica l'indirizzo nell'hash della chiave pubblica di Bob.



Metodi di conversione ed esempi di chiavi.

6. Alice con la propria chiave pubblica e privata conferma la sua proprietà sui bitcoin da spedire a Bob, infatti ha ricevuto a sua volta dalla transazione di un'altra persona i bitcoin.

Alice crea la transazione, un record contenente:

- Version Number: è il numero della versione utilizzata nella transazione, permette di indicare agli altri nodi della rete l'insieme di regole da usare per validare quella transazione senza invalidare le passate transazioni, poiché queste ultime risulteranno registrate nella blockchain come valide pur non rispettando le nuove regole del protocollo.
- Input: uno o più output di una transazione precedente fatta nei confronti di Alice, da cui prende i bitcoin che spedisce nel nuovo output.

In una transazione sono spesso elencati più input, tutti i valori di input della nuova transazione vengono sommati e il totale (meno qualsiasi commissione di transazione) viene completamente utilizzato dagli output della nuova transazione.

L'input è a sua volta composto dal TXID (transaction identifier), indice che identifica la transazione sulla blockchain; e dallo ScriptSig: la prima parte dello script, con lo scopo di verificare l'auten-

ticità dell'input.

Lo script per dimostrare che la transazione è stata creata dal vero proprietario dei bitcoin in questione, utilizza una firma e una chiave pubblica: la chiave pubblica deve corrispondere all'hash fornito nello script dell'output riscattato e viene utilizzata per verificare la firma dei redentori; la firma utilizza l'algoritmo ECDSA su un hash di una versione semplificata della transazione [4].

- Output: contiene le istruzioni per l'invio di bitcoin, al suo interno è presente il valore, il numero di Satoshi (l'unità minima in cui un bitcoin può essere suddiviso, $1 \text{ BTC} = 100.000.000$ di Satoshi) che varrà questo output una volta rivendicato e lo ScriptPubKey, la seconda parte dello script che indica l'indirizzo a cui accreditare la somma.

Possono esserci più di un output, essi condivideranno il valore combinato degli input che deve essere inviato in un output se non si desidera perderlo.

Se l'input vale 50 BTC ma vuoi inviare solo 25 BTC, Bitcoin creerà due output del valore di 25 BTC: uno a destinazione e uno a te. Qualsiasi bitcoin in ingresso non riscattato in un output è considerato una commissione di transazione.

- Signature script: l'istruzione per la firma, ovvero le istruzioni che Bob dovrà fornire per convalidare la transazione, dimostrando di essere il possessore del nuovo output. È proprio per la creazione dello script che il software di Alice ha bisogno dell'hash della chiave pubblica fornito da Bob.

Per validare la firma sono necessarie le due chiavi, che dovranno combaciare con l'hash della chiave pubblica specificato da Alice nello script. Tutto il necessario in questo momento è già in possesso di Bob.

- Sequence version: è l'eredità di una versione del protocollo Bitcoin vecchia e non ha più alcuna funzione.
- Locktime: indica il primo momento in cui una transazione può essere aggiunta alla blockchain.

7. Tutti i bitcoin a disposizione di Alice vengono "spediti" nella transazione, come detto in precedenza i bitcoin in eccesso torneranno nel portafoglio del pagante.

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

da chi riceve i bitcoin.

Il software che utilizziamo per conservare, ricevere o spedire bitcoin (il nostro portafoglio o wallet) presenta sempre un “conto” con un certo numero di bitcoin, in realtà tale conto esiste solo implicitamente, non c’è uno spazio in cui quei bitcoin sono depositati.

Il portafoglio ci comunica un certo valore semplicemente ricercando all’interno della blockchain il numero di output non spesi che siamo in grado di spendere tramite le nostre chiavi private, quindi utilizzandoli come input per nuove transazioni.

8. Alice trasmette a tutti gli altri nodi le informazioni relative alla transazione.

9. I minatori (ruolo che approfondiremo nel prossimo capitolo) inseriscono le transazioni ancora non confermate nella blockchain.

Per inserire le transazioni all’interno della blockchain il miner deve creare un nuovo blocco, processo che richiede una quantità di calcolo molto elevata e dunque una spesa in energia elettrica e strumenti. Un miner ha interesse a inserire quante più transazioni nel blocco che vuole creare poiché guadagnerà tutte le commissioni pagate su ciascuna transazione. Se una transazione non include alcuna commissione, il miner non ha alcun interesse economico nell’inserirla nel blocco.

Per inserire le transazioni nel blocco, i minatori partono dai TXID, ciascuno dei quali rappresenta l’hash di tutte le informazioni inerenti una singola transazione.

I TXID verranno messi in un Merkle tree (appendice B) per creare un unico hash prodotto di tutti gli altri, detto Merkle root.

Grazie alla struttura del Merkle tree, non è necessario conoscere tutte le transazioni incluse in un blocco per verificare che una singola transazione ne faccia parte, è sufficiente seguire un particolare ramo che collega una transazione alla merkle root.

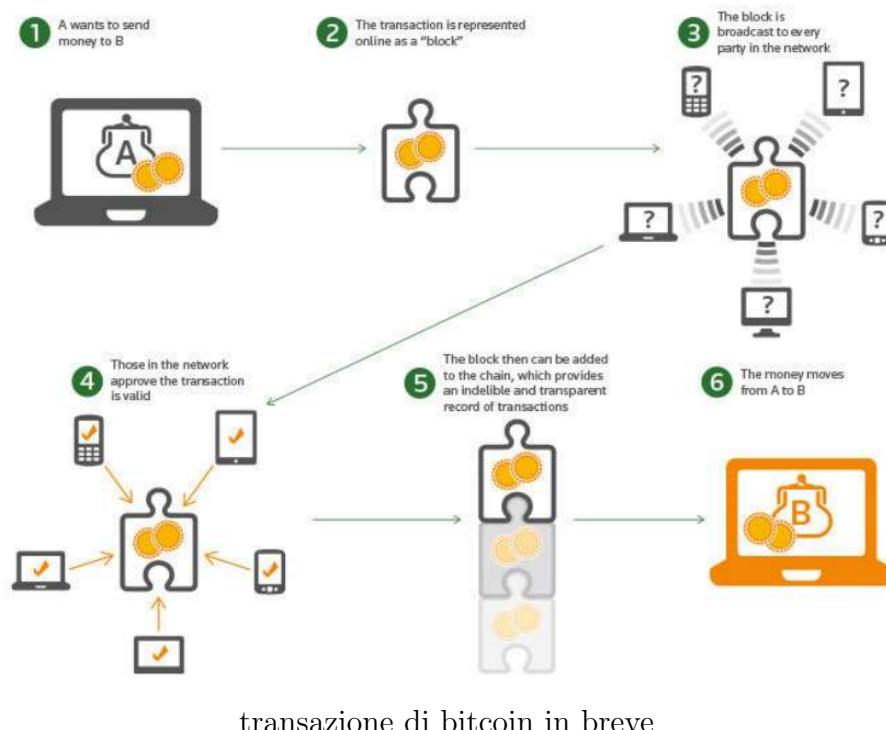
10. Bob ora vuole spendere i suoi nuovi bitcoin in una nuova transazione, il destinatario è Charlie.

Bob segue la stessa procedura che ha seguito Alice, creando una transazione specificando output, signature script (per cui gli serve l’hash della chiave pubblica di Charlie), timestamp e versione del software.

Bob però deve dimostrare di essere il possessore dei bitcoin che invia a Charlie, ovvero i bitcoin presenti nell’input della transazione. Tale input è anche l’output della transazione fra Alice e Bob.

Ricordiamo che nella sua transazione Alice ha inserito una signature

script con l'hash della chiave pubblica di Bob. Quest'ultimo per dimostrare di possedere l'output di quella transazione deve porre la sua firma (signature). Bob inserisce quindi la sua chiave pubblica, verificando che corrisponde all'hash della chiave pubblica dato in precedenza ad Alice, e la sua chiave privata, che rappresenta la conferma che Bob solo è la persona che ha originato inizialmente quella chiave pubblica. Il procedimento di firma è del tutto automatizzato da Bitcoin.



3.3 Il ruolo del Mining e la Proof of Work

Si sente parlare di mining come un metodo per generare criptovalute, ma non si limita a questo: è il metodo con cui vengono convalidate le transazioni effettuate in criptovaluta sulle relative blockchain.

Come detto in precedenza la blockchain è un registro pubblico e condiviso delle transazioni in ordine cronologico, ogni 10 minuti circa il sistema produce nuove transazioni, esse vengono inviate alla `memory pool` in attesa di approvazione. Qui entra in gioco il miner: un nodo della blockchain che mette a disposizione il suo terminale per svolgere operazioni per conto della rete.

Per prima cosa eseguirà la funzione hash su ogni transazione in attesa, ottenendo l'hash di ciascuna di esse; successivamente aggiunge una transazione personalizzata chiamata **transazione coinbase**, in cui invia a sé stesso la ricompensa del blocco. Questo processo porta alla creazione di nuove monete. Gli hash che abbiamo ottenuto vengono organizzati in un Merkle tree che ci restituisce una Merkle root che rappresenta tutti gli hash che contiene.

Ora bisogna trovare un header del blocco valido, ogni blocco ha un hash univoco e per crearne uno nuovo bisogna combinare: l'hash del blocco precedente della rete, la merkle root del nuovo blocco e un valore casuale o pseudo casuale detto **nonce**.

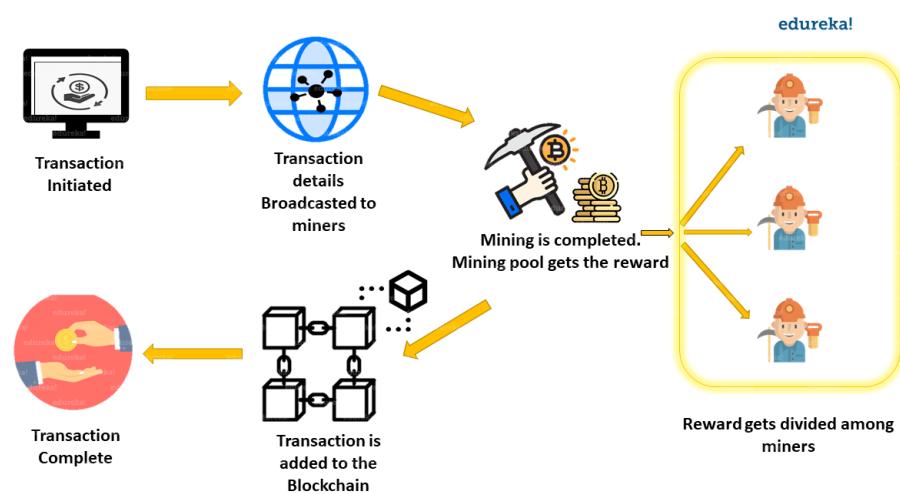
Per generare l'hash corretto del nuovo blocco in grado di collegarlo al resto della catena i due valori hash non possono essere cambiati, il solo a poterlo fare è il nonce.

Una volta trovato l'hash valido il miner trasmetterà il blocco alla rete, tutti gli altri nodi controlleranno se il blocco e il relativo hash sono validi e, in tal caso, aggiungeranno il nuovo blocco alla loro copia della blockchain.

Il miner che ha calcolato la soluzione viene ricompensato con una quantità di bitcoin; più miner hanno partecipato a questa estrazione, più la ricompensa viene suddivisa.

A questo punto, il blocco candidato diventa un blocco confermato e tutti i miner passano al mining del blocco successivo, i miner che non sono riusciti a trovare in tempo un hash valido scartano il blocco candidato e ricominciano le operazioni appena descritte su un nuovo blocco.

Il mining in sintesi è il processo che porta all'aggiunta di nuovi blocchi alla blockchain.



Il ruolo del mining in una transazione.

Questi complessi ed univoci calcoli crittografici prendono il nome di **proof of work** (PoW), un algoritmo incredibilmente complesso che proverà moltissimi nonce prima di trovare quello giusto.

I messaggi sulla rete sono trasmessi su base best effort, ottimizzando le prestazioni a discapito dei controlli; i nodi possono lasciare e ricongiungersi con la rete a loro piacimento, accettando la catena proof-of-work più lunga come prova di quello che è avvenuto mentre erano non erano presenti. [5]

La rete sarà affidabile finché che la maggior parte della potenza in essa contenuta è controllata da nodi che non cooperano per attaccarla.

Questo sistema è soluzione al problema del **double-spending**: il fenomeno in cui una singola unità di valuta viene spesa contemporaneamente più di una volta, da cui le valute digitali sono afflitte.

L'offerta di bitcoin è limitata a 21 milioni di unità, somma che si prevede raggiungere nel 2140 circa. La difficoltà di mining viene adeguata regolarmente dal protocollo in base alla quantità di potenza computazionale (hash rate) dedicata alla rete, così da assicurare che la velocità con cui vengono creati nuovi blocchi rimanga costante e prevedibile. Maggiore è la potenza di calcolo complessiva immessa nel sistema, più difficile diventa la proof of work per tutti; al contrario meno miners partecipano, minore sarà la complessità. Ad oggi infatti è praticamente inutile "minare" criptovalute dal proprio PC, serve un sistema specializzato nel risolvere i calcoli della PoW. Per questo motivo si utilizzano sistemi con GPU (più comunemente chiamate schede video): perfette per svolgere attività ripetitive e molto più efficienti di una CPU.

Così nascono i **Mining Rig** di GPU: computer che dispongono di più GPU collegate che permettono ottime prestazioni nell'estrazione di criptovalute.



Piccolo Mining Rig di GPU

3.3.1 Il problema ambientale e la Proof of Stake

Ad oggi, con il vasto interesse dimostrato in questo campo, la potenza richiesta per mettere in funzione la PoW è molto alta, ne consegue l'utilizzo di attrezzature costose oltre ad un dispendio di elettricità enorme e sempre più in crescita.

L'Università di Cambridge ha calcolato in uno dei suoi studi la quantità di energia elettrica consumata in seguito alle operazioni di mining di bitcoin: il consumo è di circa 118 terawattora ogni anno, paragonabile all'intero fabbisogno energetico dell'Argentina.



Consumo di Bitcoin a confronto con il consumo di interi paesi. [11]

In un altro studio è stato calcolato che l'emissione di anidride carbonica originata sempre dal mining corrisponde a circa 37 milioni di tonnellate ogni anno, questo dato corrisponde all'impatto ambientale annuale provocato dalla Nuova Zelanda.

Infine, lo stesso studio ha posto il settore di fronte al fatto che il consumo di una sola transazione di bitcoin equivale a quello di circa 600mila transazioni Visa.

Una soluzione più sostenibile per questo sistema incredibilmente dannoso sarebbe l'adozione della **Proof of Stake** (PoS), un algoritmo di consenso in cui la garanzia della validità delle operazioni non deriva dalla risoluzione di un problema matematico, ma dallo stanziamento di criptovalute. Di fatto, chi vuole essere validatore deve depositare proprie criptovalute nella rete, impegnandole come una sorta di garanzia o deposito cauzionale, non potendole utilizzare una volta depositate.

Questo sistema offre una maggiore velocità e scalabilità, perché non esegue alcun lavoro di calcolo che richieda tempo, di conseguenza rende PoS perfetto

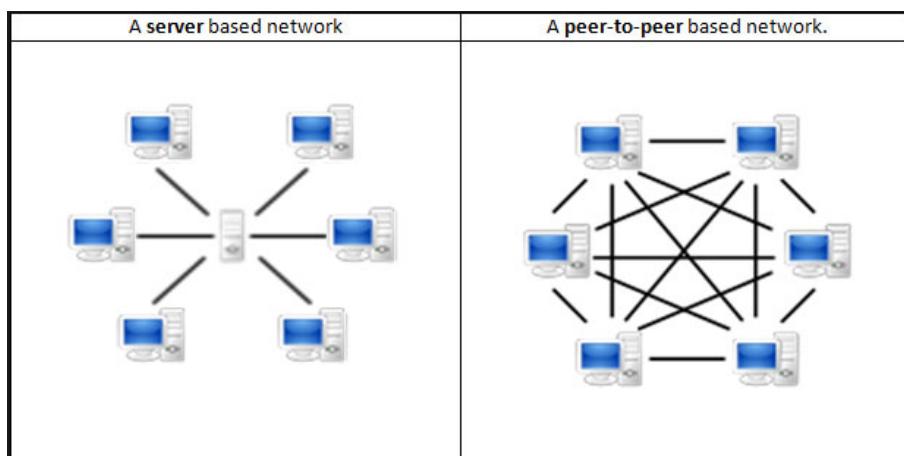
per blockchain che vogliono essere utilizzate come sistemi di pagamento al dettaglio, dove è necessario verificare grandi quantità di transazioni al secondo.

La consegna dei premi è più proporzionale grazie al sistema di selezione casuale all'interno della rete, esso mira ad assegnare compiti a chi possiede monete. Chi ne possiede di più ha maggiori possibilità di essere scelto, di fare verifiche e di trarne profitto, ma anche i piccoli investitori hanno la possibilità di guadagnare unendo le forze nelle **staking pool**: degli smart contract (approfonditi insieme ad Ethereum nel capitolo 4.1.1) che permettono di combinare il potere di staking e condividere le ricompense in modo proporzionale ai contributi individuali dati dai partecipanti.

PoS viene già impiegato da diverse piattaforme basate su blockchain e anche Ethereum sta lavorando per adottarlo.

3.4 L'architettura Peer-to-Peer

Il sistema Bitcoin non possiede un'architettura client-server ma un'architettura client-client in cui tutti i nodi sono allo stesso livello e le informazioni sono equamente distribuite tra di essi, senza dipendere da alcun nodo centrale chiamata Peer-to-Peer (P2P).



Architettura client-server e P2P a confronto

Ogni nodo possiede una copia dei file, agendo sia da client che da server per altri nodi, in questo modo nessuno possiede o controlla Bitcoin e ognuno può prendere parte al progetto essendo completamente open source.

Anche se l'architettura P2P è intrinsecamente distribuita, è importante notare che ci sono vari gradi di decentralizzazione che dipendono dalla loro

struttura.

Possiamo categorizzare i sistemi peer-to-peer in base alla loro architettura:

- Network P2P non strutturati: non presentano nessuna organizzazione specifica dei nodi, i partecipanti alla rete comunicano tra di loro in modo casuale. Sono considerati resistenti contro attività di churn elevato: una dinamica dove diversi nodi si uniscono e lasciano il network frequentemente.

Sono più semplici da costruire ma potrebbero richiedere un maggiore uso di CPU e memoria, in quanto le query di ricerca vengono trasmesse al più alto numero di peer possibile.

- Network P2P strutturati: presentano un'architettura organizzata, permettendo ai nodi di cercare file in modo efficiente, anche se il contenuto non è largamente disponibile grazie all'uso di funzioni di hash che facilitano le ricerche nel database.

Queste reti risultano più efficienti ma tendono a presentare livelli di centralizzazione elevati e, in genere, comportano costi di setup e manutenzione più alti oltre ad essere meno resistenti ad attività di churn elevato.

- Network P2P ibridi: combinano il modello client-server convenzionale con alcuni aspetti dell'architettura peer-to-peer, ad esempio potrebbero designare un server centrale che facilita la connessione tra peer.

La combinazione delle due architetture rende le prestazioni generalmente migliori.

Le reti P2P offrono una maggiore sicurezza grazie alla distribuzione su grandi numeri di nodi: sono immuni agli attacchi Denial-of-Service (DoS) e all'alterazione di dati, dal momento che la maggioranza dei nodi deve stabilire il consenso prima che i dati vengano aggiunti.

Le blockchain più piccole, non estese come Bitcoin, sono più suscettibili ad attacchi **51 percent attack**, basati sull'ottenere il controllo della maggioranza dei nodi.

Questi sistemi permettono di avere una resistenza alla censura da parte di autorità centrali: a differenza dei normali conti bancari i wallet di criptovalute non possono essere congelati o prosciugati dai governi. Venditori online hanno adottato i pagamenti in criptovalute come un modo per evitare che i propri pagamenti vengano bloccati da terze parti.

Nonostante i numerosi vantaggi, l'uso di reti P2P nelle blockchain ha anche alcuni limiti: aggiungere transazioni ad esempio richiede una grande quantità di potenza calcolo, dato che i registri distribuiti devono essere aggiornati su

ogni singolo nodo invece di un server centrale; il controllo e la regolazione sono complicati a causa della natura distribuita dei network, infatti diverse applicazioni e compagnie P2P sono state coinvolte in attività illegali. Inoltre un altro potenziale limite riguarda gli attacchi che potrebbero verificarsi durante gli eventi di **hard fork**: dato che quasi tutte le blockchain sono decentralizzate e open source, gruppi di nodi sono liberi di copiare e modificare il codice per separarsi dalla catena principale per formare un nuovo network parallelo.

Gli hard fork sono completamente normali e non costituiscono di per sé una minaccia, tuttavia se determinati metodi di sicurezza non vengono applicati correttamente, entrambe le catene potrebbero essere vulnerabili da **replay attack**, che permettono di impossessarsi delle credenziali di un altro utente del sistema e simulare la sua identità.^[7]

Capitolo 4

Applicazioni

Da Bitcoin hanno preso spunto nuove tecnologie sviluppate negli ultimi anni, in questo capitolo ne presenteremo alcune.

4.1 Altcoins

Le "alternative coin" sono le migliaia di criptovalute nate dopo Bitcoin, basate su blockchain ma progettate con obiettivi differenti, al giorno d'oggi ne esistono quasi 20mila. La maggior parte di queste sono dei semplici utility/-reward token, pensate per aiutare nella capitalizzazione o nel finanziamento di progetti e funzionanti su specifiche app o piattaforme, mentre altre devono il loro successo alle tecnologie che implementano.

4.1.1 Ethereum e gli smart contracts

Tra esse spicca Ether (ETH), la criptovaluta generata dal protocollo Ethereum come ricompensa per i miner in un sistema proof-of-work per l'aggiunta di blocchi alla blockchain. È l'unica valuta accettata per pagare le commissioni di transazione (chiamate `gas fees`) ed è fondamentale per il funzionamento della rete Ethereum.

Ethereum è la piattaforma decentralizzata regina delle criptovalute, con una capitalizzazione di 220 miliardi di euro (Capitalizzazione di mercato = prezzo corrente x offerta circolante) è dietro solo a Bitcoin con i suoi 520 miliardi [8].



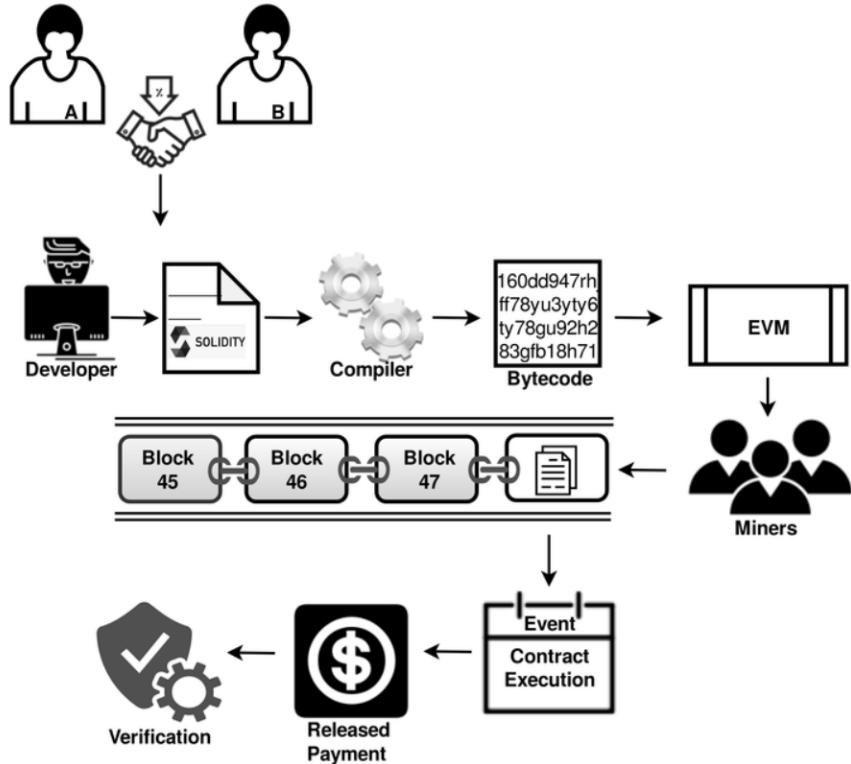
Ecosistema Ethereum

Basata su una blockchain riprogrammabile dagli utenti, ha utilizzi differenti rispetto a quelli di mero trasferimento di criptovalute. Ogni utente che possiede una propria copia della rete è nodo di essa, per operare utilizza codice Solidity, un linguaggio di programmazione molto simile a Java che viene eseguito sulla Ethereum Virtual Machine (EVM). EVM è l'ambiente di runtime per lo sviluppo e la gestione di smart contracts in Ethereum, opera in modo protetto risultando completamente separata dalla rete ETH.

Ethereum deve parte del suo successo agli **smart contracts**: proposti per la prima volta nel 1997 da Nick Szabo sono definiti dal nostro regolamento come: “un programma per elaboratore che opera su tecnologie blockchain e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse”.

Giuridicamente parlando non sono ”contratti”, ma funzioni “if-this-then-that” incorporate in software o protocolli informatici; un esempio di contratto potrebbe essere che se c’è una scadenza allora sarà eseguito il pagamento. Ne consegue che il supporto legale ha utilità nella stesura dello smart contract, ma non nella fase di verifica e attivazione, che avviene in maniera del tutto automatica dalla rete blockchain di riferimento.

Questo permette di avere la certezza giuridica dell’esecuzione di obbligazioni contrattuali, visibili a tutti i partecipanti della rete e non solo alle parti coinvolte, oltre alla loro trasparenza e immutabilità.



Processo di creazione ed esecuzione di uno Smart Contract.

4.1.2 Stablecoins

Una stablecoin è una valuta digitale ancorata ad un'attività di riserva stabile, come il dollaro statunitense o l'oro[10]. Sono uno degli strumenti più apprezzati per la conservazione di valore e la negoziazione: essi infatti sono progettati per ridurre la volatilità rispetto alle criptovalute non ancorate come bitcoin e fanno da ponte tra il mondo delle criptomonete e le valute fiat (valuta nazionale non ancorata al prezzo di una materia prima, il suo valore è legato alla fiducia nei confronti dell'autorità che la emette) che usiamo giornalmente.

Nonostante la loro stabilità sono a tutti gli effetti criptovalute e hanno ereditato caratteristiche comuni con esse:

- Sono aperte, globali e accessibili a chiunque tramite Internet in qualsiasi momento.
- Sono rapide, convenienti e possono essere trasferite in modo sicuro.
- Sono digitali, native di Internet e programmabili.



Le principali stablecoins: TerraUSD, USD Coin, Tether, Binance USD, Dai.

Per mantenere il valore ancorato al prezzo stabilito si svolgono due operazioni:

- quando il valore supera il prezzo stabilito, l'algoritmo produce nuove monete per abbassarlo;
- quando il valore invece va sotto il prezzo stabilito, si elimina la quantità che serve a riportarlo su.

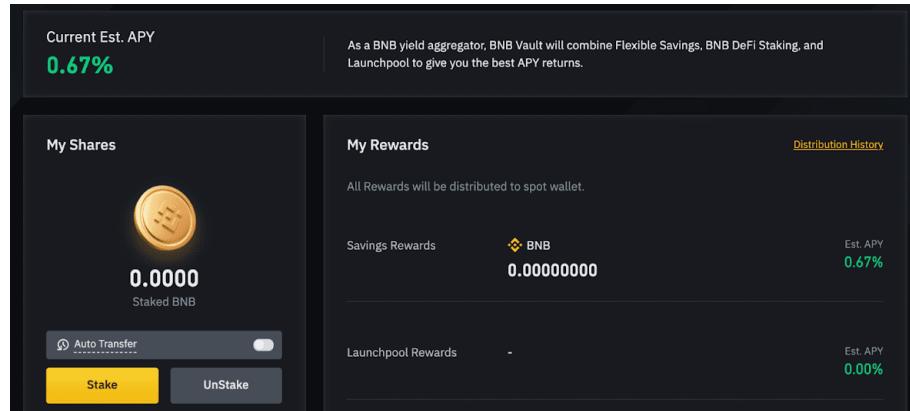
4.2 Binance, l'exchange più grande al mondo

Binance è una piattaforma di scambio di criptovalute fondata nel 2017, a oggi è l'exchange di assets digitali più grande del mondo in termini di volume di scambi.

Si basa su una blockchain chiamata **Binance Chain**: ottimizzata per il trading ma non flessibile come le altre blockchain dal punto di vista della programmabilità.

Per questo motivo le è stata affiancata la **Binance Smart Chain (BSC)**: un'altra blockchain che offre funzionalità smart contract e compatibile con la Ethereum Virtual Machine, offrendo il supporto per gli strumenti e applicazioni decentralizzate Ethereum. L'obiettivo è lasciare intatte le capacità di trading elevate di Binance Chain e al tempo stesso introdurre gli smart contract nel suo ecosistema.

BSC è un esempio di blockchain basata sulla Proof of Stake, i partecipanti fanno staking (bloccare degli asset in cambio di interessi) di Binance Coin (la criptovaluta che alimenta l'ecosistema Binance) in modo da diventare validatori. Se propongono un blocco valido ricevono le commissioni delle transazioni incluse in esso. [7]



BNB Vault, dove mettere in staking i propri Binance Coin.
APY è il rendimento percentuale annuo.

4.3 NFT

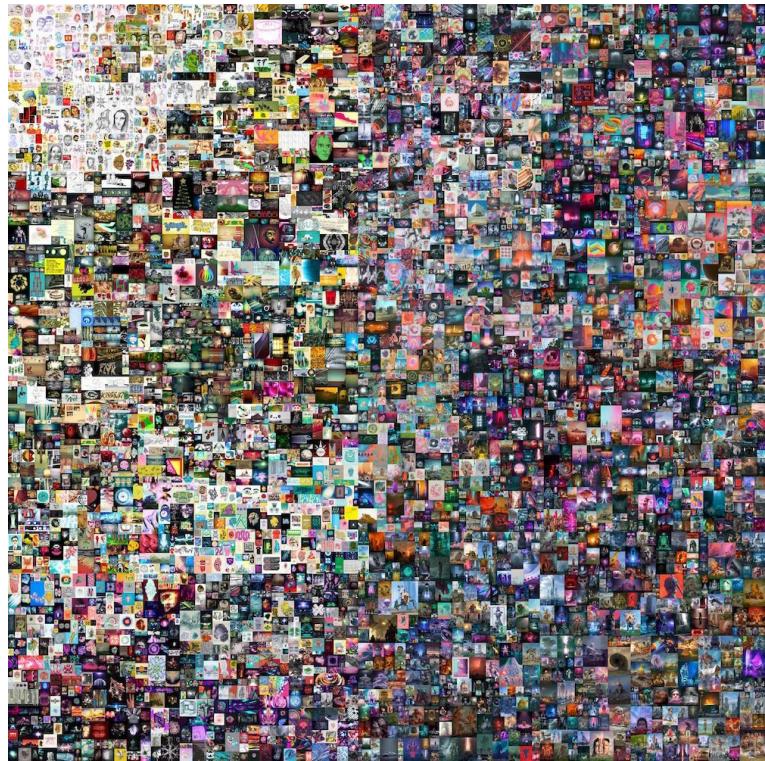
Un non-fungibile token (NFT) è un tipo di token che rappresenta l'atto di proprietà e il certificato di autenticità scritto su catena di blocchi di un bene unico. Non fungibile sta a significare che il gettone non è riproducibile e non è reciprocamente intercambiabile con altri, ciò è in contrasto con il concetto di criptovaluta, che può essere duplicata infinite volte in copie esattamente identiche.

Un NFT serve quindi a identificare in modo univoco e sicuro un prodotto digitale creato su internet, come se avesse sopra la firma dell'autore.

Tutto questo è realizzabile grazie alla blockchain, prima di essa ogni cosa su internet era facilmente riproducibile all'infinito.

Chi acquista un'opera legata a un NFT non acquista l'opera in senso stretto ma si garantisce la possibilità di rivendicare un diritto su quell'opera attraverso uno smart contract.

L'opera originale rimarrà di esclusiva proprietà dell'autore che, grazie al diritto d'autore che esercita su essa, avrà la possibilità di sfruttare economicamente un numero indefinito di volte la propria opera, venendo remunerato per l'acquisto di un gettone ad essa collegato.



”Everydays: the first 5000 Days” di Beeple
è l’opera NFT più costosa mai venduta, battuta all’asta per 69 milioni di dollari.

Capitolo 5

Conclusioni

In questa relazione abbiamo analizzato il sistema Bitcoin e le altre criptovalute scoprendo che il loro punto di forza comune è proprio ciò su cui si basano: la blockchain. La decentralizzazione e la programmabilità di questa tecnologia permette di non avere intermediari ed adattarsi alle più varie esigenze.

Un grosso progresso verso la digitalizzazione: tutti i dati diventano pubblici e consultabili senza andare a discapito della privacy; infatti le informazioni personali rimangono private, protette da diverse tecnologie crittografiche per evitare manipolazioni e furti.

Un'altra conclusione a cui siamo arrivati è l'inadeguatezza di Bitcoin ad essere utilizzato come mezzo di pagamento, questo a causa dei tempi di elaborazione non istantanei e per l'enorme quantità di risorse che richiede. Abbiamo visto nuove tecnologie, come la Proof of Stake, che in un prossimo futuro potrebbero diventare il nuovo standard per la loro sostenibilità.

Ad oggi tra le masse non c'è molta coscienza di quali opportunità possa offrire questo settore, sono le nuove applicazioni con le loro innovazioni a far capire quanto sia prospero; un esempio è il recente boom degli NFT diventati in pochissimo tempo un evento globale.

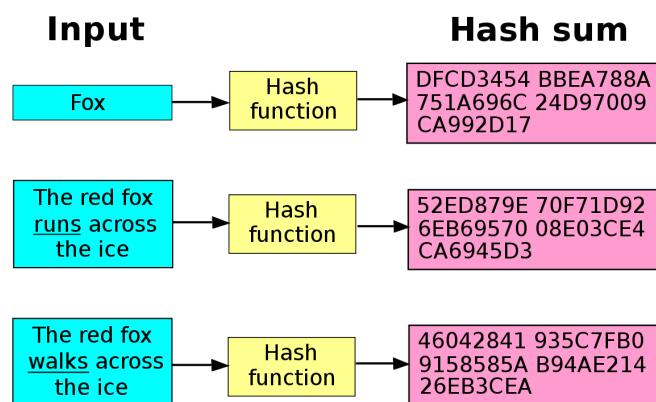
E' necessario che le istituzioni introducano nuove leggi per regolamentare questi fenomeni, per non lasciare dubbi, non farsi trovare impreparate e senza ostacolare lo sviluppo di una tecnologia con così tanto potenziale.

Appendice A

L'utilizzo della funzione Hash

Come accennato precedentemente la blockchain utilizza la funzione di hash per generare l'indirizzo dalla chiave pubblica, ora vediamo qualche dettaglio di questa funzione.

La funzione hash è una funzione che può ricevere un input di lunghezza arbitraria e produce un output a lunghezza fissa difficilmente invertibile, infatti dato l'output è praticamente impossibile risalire all'input. Per generare il **digest** (il risultato) si eseguono una serie pre-determinata di operazioni di confusione e rimescolamento dell'informazione originale. È una caratteristica comune il fatto che la modifica anche di un singolo bit nell'input faccia sì che la funzione produca un hash molto diverso dal precedente.



Input e Output di una funzione hash

A.0.1 SHA256

La blockchain utilizza in particolare lo SHA256: SHA(Secure Hash Algorithm) indica la famiglia di cinque diverse funzioni crittografiche di hash di cui fa parte, sviluppato a partire dal 1993 dalla National Security Agency (NSA), pubblicato dal NIST nel 2001 e ufficializzato nel 2002 come standard federale dal governo degli USA; mentre 256 sta a significare che l'algoritmo produce un digest di 256 bit [13].

INPUT DATA	HASH OUTPUT (SHA-256)
My name is Toby	cacb5418163039b016be9746818a2926f68fd1e4bad1b04f6791f6aabbb5e8c52
My name is Tony	9cd2444dc56929bdb97123add1f007643effa88bf1ed061eee1eed4e15ac7f9
My name is Toby and this is my project	9abbaa0c54fc028ac51bede2608d06e8d3a026784e34adfac14fadd143d212c

Esempio di conversione in SHA256.

A.0.2 RIPEMD160

E' un algoritmo crittografico di hashing ideato da un gruppo di ricerca della Katholieke Universiteit Leuven (università situata in Belgio), viene oggi utilizzato nelle transazioni Bitcoin per comprimere da 256 (output di SHA256) a 160 bit. Ne esistono varie versioni ma la 160 è la più utilizzata, il suo output è composto da una stringa a 40 caratteri che utilizza numeri esadecimali.

Esempi di conversione:

- RIPEMD-160("The quick brown fox jumps over the lazy dog") = 37f332f68db77bd9d7edd4969571ad671cf9dd3b
- Ecco come varia l'hash cambiando una sola lettera del messaggio: RIPEMD-160("The quick brown fox jumps over the lazy cog") = 132072df690933835eb8b6ad0b77e7b6f14acad7
- Questo è invece l'hash per una stringa di lunghezza nulla: RIPEMD-160("") = 9c1185a5c5e9fc54612808977ee8f548b2258d31

[12]

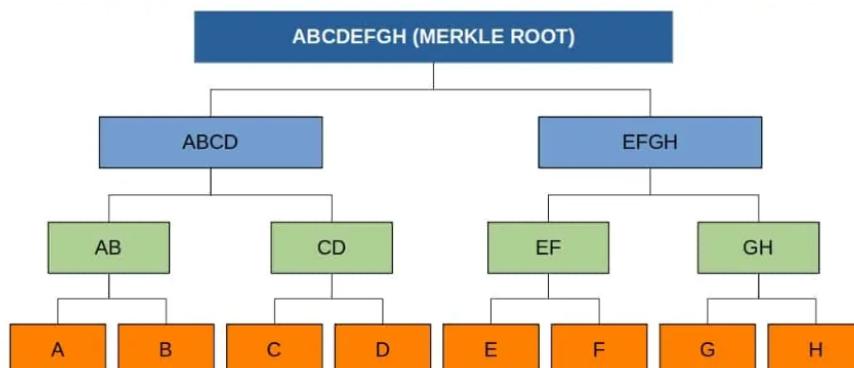
Appendice B

Merkle tree

Nel 1979 Merkle propose l'idea di un albero di hash che permettesse la verifica efficiente e sicura dei contenuti in esso presente, ideò così l'albero di Merkle: una struttura dati suddivisa in diversi livelli il cui scopo è metterli in relazione nodo con un'unica radice associata ad essi.

L'albero ha 2 ramificazioni a ogni passo, in cui ogni nodo è etichettato con l'hash dei suoi nodi figli. Un nodo figlio è chiamato **foglia** e contiene la hash di una transazione (TXID).

La struttura ad albero permette la verifica di un blocco attraverso una quantità di dati proporzionale al logaritmo del numero dei nodi dell'albero. Gli hash di tutti i blocchi vengono accoppiati ogni volta fino ad ottenere un solo hash, chiamato merkle root, che sintetizza tutte le transazioni contenute nel blocco.



Esempio di albero di Merkle.

Più specificamente prendiamo ogni coppia di hash, le combiniamo e creiamo una hash dell'insieme. Quindi creiamo una hash di A + B, C + D, E + F, e G + H. Il risultato finale sono quattro hash: AB, CD, EF, GH. Ora

proseguiamo facendo un'altra operazione di hashing e queste quattro diventano due: ABCD e EFGH. Infine, creiamo la hash delle due rimanenti per ottenere la nostra Merkle root.[6]

Il vantaggio principale degli alberi di Merkle è che quando il dato di un blocco cambia, non è necessario calcolare l'hash sopra ogni altro dato, ma si calcolano solamente i nodi lungo il ramo, fino al nodo radice. Così facendo il numero di calcoli hash richiesto diminuisce logaritmicamente sul numero di blocchi di dati totali. Tale processo risulta essere particolarmente efficiente quando vi sono molte ramificazioni dell'albero.

Bibliografia

- [1] Donald E. Knuth (1986) *The T_EX Book*, Addison-Wesley Professional.
- [2] Leslie Lamport (1994) *L^AT_EX: a document preparation system*, Addison Wesley, Massachusetts, 2nd ed.
- [3] Alberto De Luigi. Transazione Bitcoin. Tratto da albertodeluigi.com:
URL:<https://www.albertodeluigi.com/index/bitcoin/transazione-bitcoin/>
- [4] Bitcoin Wiki (2021). Transaction. Tratto da en.bitcoin.it: <https://en.bitcoin.it/wiki/Transaction>
- [5] NAKAMOTO S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Tratto da bitcoin.org: <https://bitcoin.org/bitcoin.pdf>
- [6] Binance (2020). Merkle Tree e Merkle Root Spiegati. Tratto da academy.binance.com: <https://academy.binance.com/it/articles/merkle-trees-and-merkle-roots-explained>
- [7] Binance (2022). Scopri tutto su Blockchain e criptovalute. Tratto da academy.binance.com: <https://academy.binance.com/it/>
- [8] CoinMarketCap (2022). Prezzi, grafici e capitalizzazioni di mercato delle criptovalute. Tratto da coinmarketcap.com: <https://coinmarketcap.com/>
- [9] SZABO N. (2005). Bit Gold. Tratto da Satoshi Nakamoto Institute: <http://nakamotoinstitute.org/bit-gold/>
- [10] Coinbase. Cos'è uno Stablecoin?. Tratto da coinbase.com: <https://www.coinbase.com/it/learn/crypto-basics/what-is-a-stablecoin>

- [11] Università di Cambridge (2019). Cambridge Bitcoin Electricity Consumption Index. Tratto da ccaf.io: <https://ccaf.io/cbeci/index/comparisons>
- [12] Wikipedia, l'enciclopedia libera. RIPEMD. Tratto da it.wikipedia.org: <https://it.wikipedia.org/wiki/RIPEMD>
- [13] Wikipedia, l'enciclopedia libera. Secure Hash Algorithm. Tratto da it.wikipedia.org: https://it.wikipedia.org/wiki/Secure_Hash_Algorithm