Elaborato di tesi

BLOCKCHAIN & TEORIA DEI GIOCHI

Relatore: Massimo Monetti
Candidati: Emanuele Peirolo Maritano
Pier Paolo Picco

UST

Politecnico di Torino

Politecnico di Torino

Design e Comunicazione
A.a. 2022/2023
Sessione di Laurea Luglio 2023

Blockchain

Teoria & Usi

Relatore:

Massimo Monetti

Candidati:

Emanuele Peirolo Maritano

Pier Paolo Picco

Introduzione

Introduzione

Blockchain, letteralmente **“catena di blocchi”**, è una tecnologia che viene spesso associata al mondo Internet, rappresenta un vero e proprio **stravolgimento infrastrutturale** con possibili utilizzi in innumerevoli settori e con molte potenzialità ancora da scoprire.

Blockchain ▶

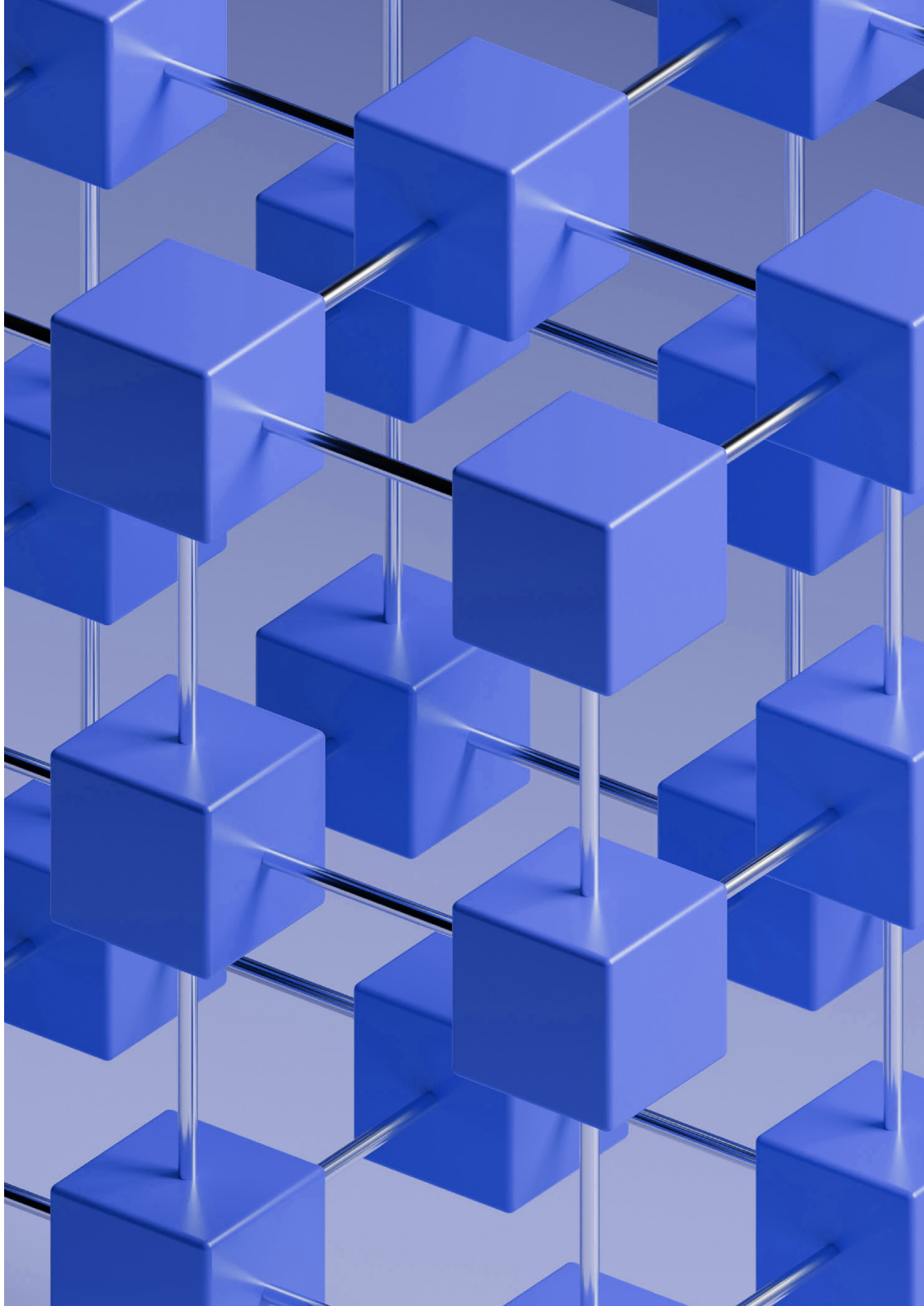
Il termine iniziò a circolare nel 2008, quando Satoshi Nakamoto inventò il Bitcoin, la prima moneta elettronica, il cui funziona-mento si basa su questa tecnologia.

Se si volesse trovare una definizione della blockchain si potrebbe paragonarla ad un **libro mastro** (in inglese Ledger, da qui DLT, distributed ledger technology). Un registro digitale, **decentralizzato** e distribuito sulla rete internet, strutturato come una catena di blocchi che contengono informazioni, da qui nasce il termine.

È possibile aggiungere nuovi blocchi, ma non è possibile modificare i precedenti o rimuoverli, pena l’**invalidazione dell’intera catena.**
Sistemi di crittografia e di distribuzione del consenso ne garantiscono la **sicurezza e l’immutabilità**.

È doveroso precisare che le **criptovalute**, sebbene al momento costituiscano il maggior esempio di utilizzo della tecnologia Blockchain, non sono altro che una tra le **molte possibili applicazioni** che questa tecnologia offre.

Potremmo dire che Bitcoin sta a Blockchain come Google sta ad Internet.



Perché la Blockchain

Per comprendere al meglio la blockchain nella sua complessità è bene iniziare analizzando il perché sia nata questa tecnologia e quali vantaggi offre rispetto al sistema attualmente in uso. La blockchain nasce per affrontare uno dei più grandi problemi della nostra società: **la fiducia**.

Il tacchino induttivista

metafora del filoso Bertrand Russel su ciò che diamo per scontato a causa dell'abitudine.

La collettività si regge su fondamenta di fiducia reciproca sorretta da **più parti coinvolte**, ad esempio la banca garantisce sicurezza riguardo ai possedimenti, e i commercianti si fidano che in cambio di un bene riceveranno il denaro dovuto. La banca, in quanto autorità, ricopre un **ruolo di garante**, ma di fatto non si può avere la certezza che questa non possa un giorno agire in maniera illecita nei nostri confronti, tendiamo a darlo per scontato a causa delle nostre abitudini.

È difficile e dispendioso guadagnare e mantenere la fiducia degli utenti, soprattutto online, ed è per risolvere tali problematiche e tutelare l'utente che nasce la blockchain.

I valori fondanti della Blockchain

Essa ha rivoluzionato il sistema, ponendo **trasparenza** e **incorruttibilità** come fondamenta della tecnologia. Per rispettare tali propositi Blockchain deve risultare: sicura, immutabile, trasparente, decentralizzata ed estendibile.

Comprendere come queste qualità vengano garantite è più facile analizzando il funzionamento della tecnologia.

Figura 1

Sede della banca centrale europea, denominata BCE, che gestisce la moneta, ne definisce la politica economica e la applica nell'UE.

Tecnologia

La Tecnologia

Una volta compresa l'importanza che la blockchain assumerà nel prossimo futuro, è chiaro che comprenderne le dinamiche e il funzionamento diventa una competenza essenziale per avere una **visione del mondo che ci circonda,** senza rischiare di finire a usufruirne in maniera passiva, come già accade per molte tecnologie odierne.

Non è necessario conoscerne gli aspetti tecnici nella loro totalità, ma è sufficiente riuscire a **comprendere in maniera pratica** come avverranno i pagamenti, i contratti e cosa li tutelerà.

Perchè ci appare così complicata

A rendere così complessa la tecnologia della blockchain è in particolar modo la sua **attuale interfaccia**, si potrebbe paragonarla all'esordio dei computer che, non disponendo di un'interfaccia intuitiva, richiedevano una conoscenza della tecnologia molto avanzata, allontanando l'utenza generalista. Solamente in seguito, con l'invenzione dei sistemi operativi, i computer si sono adattati all'uomo e hanno potuto essere sfruttati al massimo per le loro capacità e applicazioni. Allo stesso modo la blockchain al momento è in **continua evoluzione** e la mancanza di una interfaccia chiara e semplice allontana i più dal comprendere questa tecnologia che a livello di logica risulta meno complessa rispetto a quanto ci si potrebbe aspettare.

Le nozioni necessarie a comprendere la tecnologia variano in base al tipo di fruizione che si che si desidera avere della blockchain.

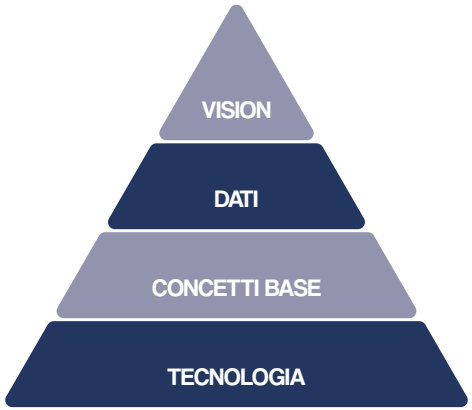
Figura 2

Operatrice a lavoro con un IBM 704, primo computer nel 1954 in grado di eseguire calcoli in virgola mobile prodotto in serie.

È comunque possibile rappresentare i vari **layer di complessità** attraverso la rappresentazione di una piramide, che differenzia nozioni base ed essenziali di blockchain e quelle più dettagliate e d'interesse per specialisti del settore e progettisti.

Figura 3

Piramide esemplificativa dei 4 livelli di conoscenza di una tecnologia, dalla semplice fruizione alla comprensione critica di questa.



Alla base della piramide vanno a posizionarsi le conoscenze base della tecnologia blockchain e delle sue principali caratteristiche e applicazioni. Con "tecnologia" ci si riferisce le basi riguardanti la sua struttura e le sue proprietà: i **nodi e i blocchi**, gli **algoritmi di consenso**, i diversi tipi di mining, la decentralizzazione, gli smart contract ecc.

Ad un secondo livello si trova la conoscenza dei principi di un **token** o di un progetto su blockchain: il **whitepaper**, i "needs" a cui si vuole trovale soluzione, l'uso specifico della tecnologia nel progetto, l'**affidabilità** del team ecc.

Il terzo livello raccoglie tutte quelle capacità di **analisi critica** di dati e informazioni ricavabili attraverso: analisi del mercato, notizie di rilevanza, obiettivi raggiunti da team di sviluppo ecc.

L'ultimo livello rappresenta la capacità di correlare i dati tramite una **visione d'insieme**. Chi si affida esclusivamente alle analisi o alle spiegazioni necessariamente semplificate dei media o al passaparola, a opinioni circolanti sui social media, viene limitato a una **comprensione parziale** dell'argomento, che spesso gli impedisce di afferrarne il reale potenziale.

I Blocchi

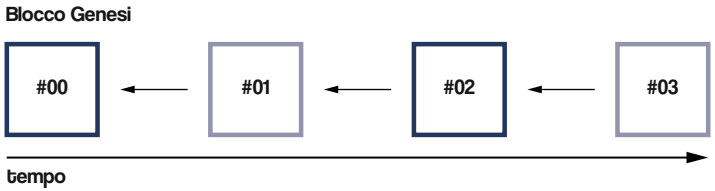
Come deducibile dal nome, questa tecnologia è rappresentabile come una **sequenza di blocchi**, ognuno di questi è un **pacchetto d'informazioni** con una quantità di memoria a disposizione definita e costante, all'interno di ogni blocco vi è un dato fisso che consente d'identificare il blocco precedente, mentre il resto dello spazio può essere riempito liberamente, **qualsiasi genere di file** può essere inserito in un blocco ed essere crittografato nella blockchain: immagini, video, audio, pdf, file di software; qualsiasi documento in quanto dato informatico può quindi usufruire delle funzioni della blockchain.

Il contenuto di un blocco

In una catena di blocchi il primo di questi viene denominato "**blocco genesi**".

Figura 4

Rappresentazione di una sequenza di blocchi a partire dal blocco genesi, primo della catena.



Benché il concetto dei blocchi risulti facilmente comprensibile, più complesso è spiegare come si faccia a garantire in maniera univoca la sequenzialità dei blocchi e la loro invulnerabilità ad eventuali attacchi informatici, per entrambe queste esigenze viene utilizzata la "**funzione crittografica di hash**" come principale soluzione.

Figura 5

Rappresentazione dei tre elementi principali contenuti all'interno di un blocco, gli hash sono essenziali al corretto funzionamento della catena.

Passando attraverso questo **algoritmo matematico** ogni blocco genererà un valore denominato "**hash**" che verrà salvato nel blocco successivo che a sua volta genererà un hash e verrà **memorizzato nel seguente**, in questo modo ogni blocco contiene le informazioni necessarie a rintracciare il suo blocco precedente in maniera univoca ed è possibile generare una sequenza potenzialmente infinita.

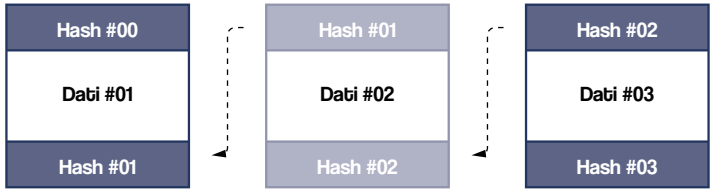


Figura 6

Rappresentazione del collegamento che va ad instaurarsi tra i blocchi di una catena grazie ai loro hash.

Come già detto la blockchain è trasparente, significa che è possibile controllare lo stato della catena, di ogni blocco e il suo contenuto, basta sapere come navigare tali informazioni.

Blockchain Explorers

Navigare la Blockchain

Sono nati a tale scopo appositi strumenti software chiamati **blockchain explorer** perché consentono di controllare il contenuto dei blocchi, vedere il costo delle transazioni e il codice degli smart contract, uno dei più utilizzati è **Etherscan**, che consente di monitorare la blockchain di **Ethereum**.

Le principali informazioni ricavabili sono:

- Stato: se il blocco ha avuto successo;
- N° Blocco: numero che identifica il blocco;
- Timestamp: quanto tempo fa è stato approvato il blocco;
- From e to: indirizzi coinvolti in una transazione;
- Value: il valore della transazione;
- Txn fee: commissione sulla transazione;

Inoltre è possibile, cliccando sul numero del blocco, vedere tutte le transazioni che contiene e gli smart contract che ha svolto e sono stati confermati, con tanto di indirizzi mittenti e destinatari oltre che gli UTXO utilizzati e la loro origine dal primo all'ultimo proprietario del titolo.

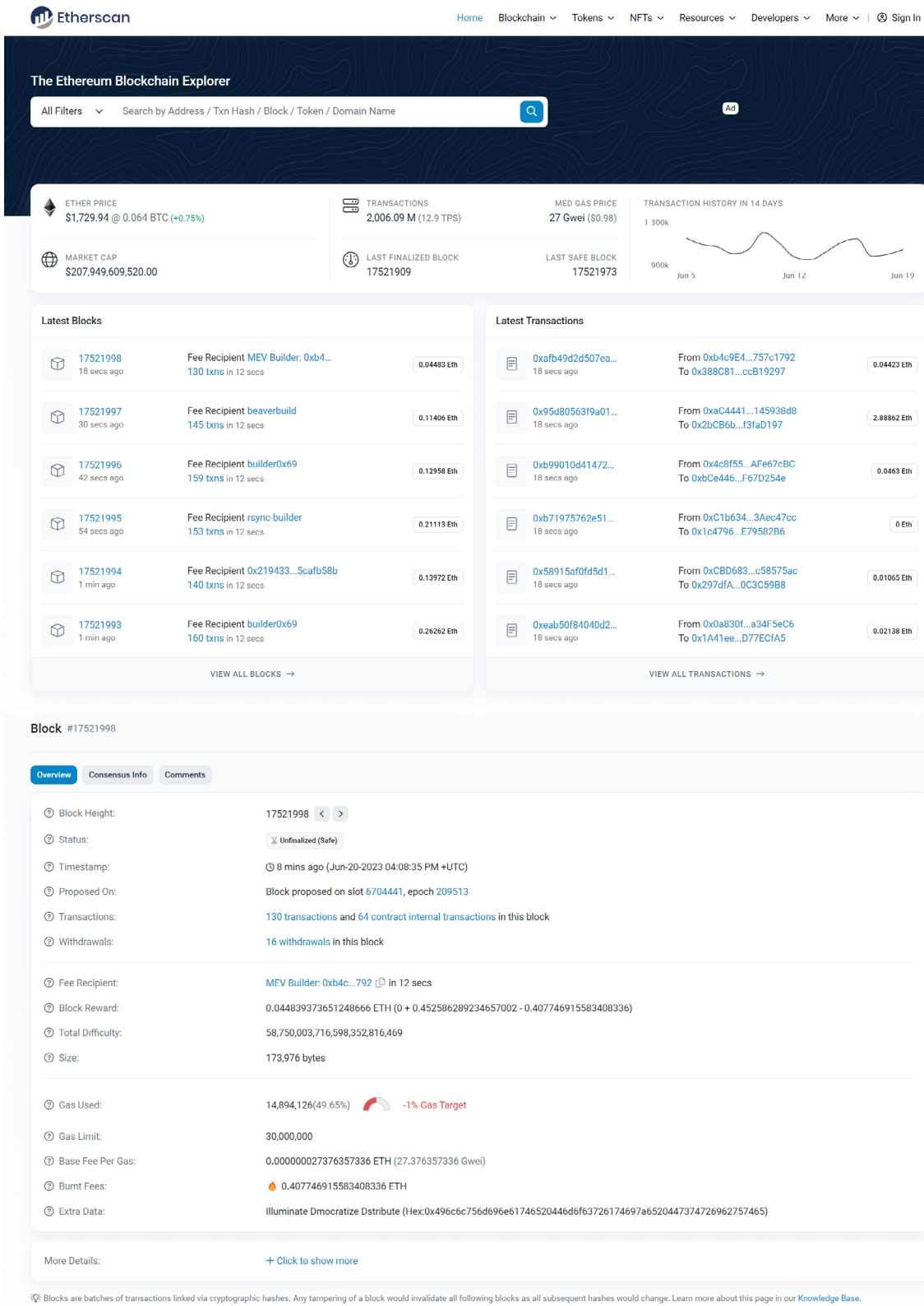


Figura 7

Schermata principale di Etherscan, un blockchain explorer consultabile online, è possibile esplorare il contenuto degli ultimi blocchi e la loro origine.

Funzione di Hash

La funzione di hash viene utilizzata per mappare pacchetti di dati di dimensioni arbitrarie in un corrispettivo denominato "**hash**", consiste in una **stringa di lettere e numeri di dimensione fissa**. Ogni genere di file può essere sottoposto a tale funzione (mp3, png, pdf, fogli di calcolo, un'intera blockchain). I dettagli matematici della funzione di hash sono estremamente specifici e non essenziali allo scopo della tesi, quindi non saranno approfonditi, ma sono da tenere presenti le sue caratteristiche che la rendono così funzionale nella sua applicazione:

File sottoponibili all'hashing

- Dato un **input** questo produrrà **sempre lo stesso output**, ovvero sempre la stessa stringa di hash
- La minima differenza all'interno dell'input comporta radicali differenze nell' hash output della funzione
- É una funzione **unidirezionale**: a livello di calcolo computazionale **è molto semplice generare un hash**, risulta invece complicato partendo dall' hash ricavare l'input della funzione, **non esiste una formula inversa**, l'unico modo è andare per tentativi (brute-force).

Figura 8

Dimostrazione della radicale alterazione di hash alla mininima variazione dell'input

Un impronta digitale virtuale

Potremmo immaginare l'hash di un file come la sua **impronta digitale** e ogni alterazione del file comporta variazioni nella sua impronta.
Nel momento in cui si calcola l'hash di un file è quindi in seguito possibile per chiunque conoscere se ci si trovi di fronte al file originale oppure una copia semplicemente confrontando i loro hash invece che andando ad analizzare per intero i file.

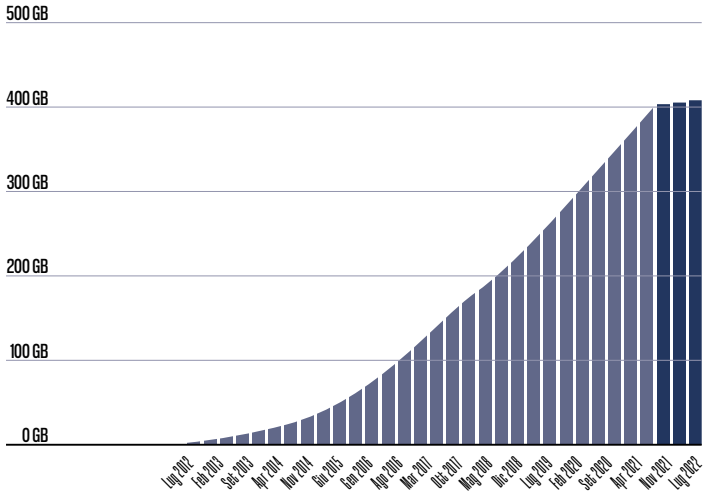


Figura 9

Grafico rappresentatante la crescita in termini di spazio di memoria occupato da Bitcoin, arrivando nel 2022 sopra i 400 GB

Risulta funzionale soprattutto con grandi volumi di dati, interi database gestibili attraverso 256bit, per esempio nel 2022 Bitcoin ha raggiunto i 400 GB ($1{,}25*10^{10}$ volte un hash) di memoria totale, ma continua e continuerà essere possibile verificarne l'integrità tramite una breve stringa di caratteri, generabile in pochi secondi.

La Crittografia

La blockchain utilizza l'hashing per un motivo di praticità e sicurezza, l'hash consente di **verificare lo stato dell'intera blockchain** e di bloccare sul nascere tentativi di manomissione.

Ogni blocco contiene i dati che sono destinati a essere immagazzinati più l'hash del blocco precedente, a sua volta tutto l'insieme verrà sottoposto all' hashing e il risultato inserito nel blocco successivo, così facendo è possibile **verificare l'integrità della catena** confrontando semplicemente due stringhe. In caso di manomissione di un blocco ciò causerebbe non solo modifiche all'hash del blocco alterato ma anche a tutti quelli successivi, rendendo evidente il tentativo di manomissione.

Figura 10

Rappresentazione di un tentativo di alterazione di un blocco e come questo grazie agli hash venga riconosciuto e bloccato.

La facilità di verifica in confronto alla complessità della manomissione di una blockchain è il primo fattore a scoraggiare tentativi di hacking. Ad esempio la blockchain di Bitcoin pur pesando a oggi 400 gigabyte può essere verificata nella sua integrità semplicemente attraverso una stringa di 256 bit, mentre un tentativo di hacking

costerebbe enormi cifre in termini di potenza di calcolo e corrente, grandi sforzi e investimenti che verrebbero vanificati in tempi inferiori al secondo.

L'hacking è più dispendioso che profittevole

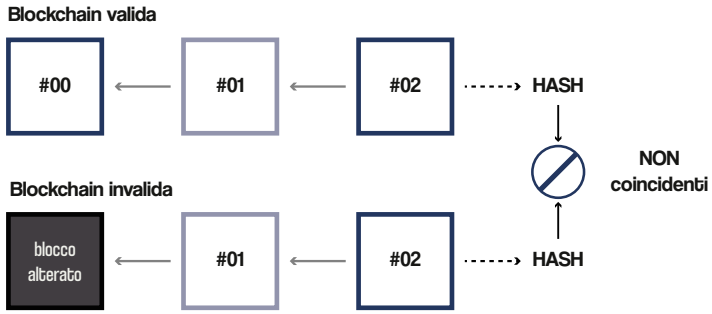


Figura 11

Schema raffigurante la comparazione tra due versioni della stessa blockchain per determinare quale delle due sia quella valida.

Inoltre c'è da considerare che chi tenta un attacco lo fa per un ritorno personale ma nel momento stessso in cui anche per ipotesi riuscisse nel suo intento, ipotizziamo intestandosi una grossa quota di una criptovaluta, questa crollerrebbe automaticamente perchè rivelando delle vulerabilità non presenterebbe più alcun valore di mercato, per questo motivo specialmente coloro in possesso di grandi quote sono i primi a preoccuparsi che la blockchain rimanga inviolata.

2 - TECNOLOGIA

Hash Rate

I miners

All'interno di una blockchain vi è necessità quindi di fornire potenza di calcolo al fine, tra le altre cose, di processare continuamente funzioni di hash. A tale scopo partecipano i **miners**, che mettono a disposizione del sistema le loro **risorse hardware**, in cambio di un ricompensa economica.

Più grande è una blockchain, più nodi ha a disposizione e necessiterà di maggiore potenza di calcolo. L'**hash rate** di una blockchain indica quanti cicli di hash vengono eseguiti al secondo per una determinata blockchain. Bitcoin presenta un hash rate di circa 160 mila cicli al secondo, è un valore altissimo che dimostra la sua diffusione e l'interesse delle persone e dei miners nei suoi confronti.

Figura 12

Grafico raffigurante l'intensità dell'hash rate di Bitcoin, che ha raggiunto picchi di 160 mila operazioni di hash al secondo.

(fonte: glassnode)

Come si può osservare, la ragione di questa **grande quantità di energia consumata** è l' elevatissima capacità di calcolo messa a disposizione delle blockchain, che consuma moltissima corrente, ciò è però necessario al fine di garantire il corretto funzionamento della catena: **contrastare attacchi**, **eseguire transazioni**, convalidare li smart contract, verificare che venga diffusa la corretta versione della catena e **generare nuovi blocchi**.

Ridurre i consumi

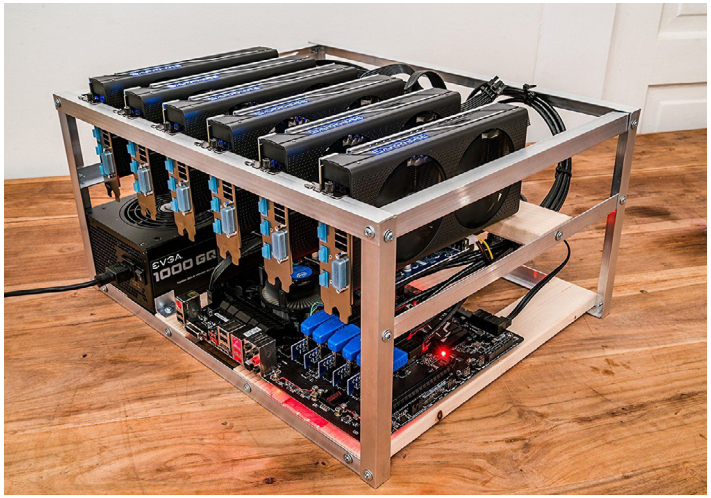
Trattandosi di una tecnologia in sviluppo sono state ideate anche alternative in modo da garantire il funzionamento della catena **abbattendo il consumo energetico**, come per esempio il Proof of Stake, sistema che sarà approfondito nei prossimi capitoli.

Il Mining

Il **mining** è il processo alla base della **generazione di nuovi blocchi**, che vengono aggiunti in un intervallo di tempo prestabilito, ad esempio in Bitcoin ogni 10 minuti un nuovo blocco viene generato.
Siccome la blockchain è un **sistema decentralizzato**, privo di un admin che possa prendere decisioni per essa, qualsiasi persona che possieda un dispositivo hardware può metterlo a disposizione di una blockchain, diventando un miner.

Figura 13

Esempio di una piattaforma hardware adibita appositamente al mining, sono presenti molte schede video per aumentare la potenza di calcolo.



I miners sono persone che **forniscono la potenza di calcolo** a loro disposizione a una blockchain. La procedura di mining consiste nella **risoluzione di una funzione** di hash **particolarmente complessa** la cui soluzione consentirà di generare correttamente il prossimo blocco della catena.

Figura 14

Esempio di una sala server.

2 - TECNOLOGIA

I guadagni di un miner

Al fine d'incentivare i miners, il nodo (cioè il dispositivo connesso alla rete di blockchain) che per primo riesce a trovare la soluzione dell'equazione viene **retribuito con della valuta** in base al costo della transazione (es. **Gas fees** di Ethereum).

Non esiste una strategia attraverso la quale è possibile risolvere più o meno velocemente l'equazione al fine di garantirsi un guadagno maggiore, il sistema si basa sulla pura potenza di calcolo dato che gli hardware ripeteranno in continuazione funzioni di hash fino a trovare quella corretta per risolvere il problema.

È una sorta di lotteria dove l'unica variabile per aumentare le proprie probabilità è avere una maggiore potenza di calcolo a propria disposizione, per questo motivo i miners si sono, col tempo, uniti in gruppi dove gli introiti vengono distribuiti tra tutti in maniera proporzionale al contributo offerto dai singoli.

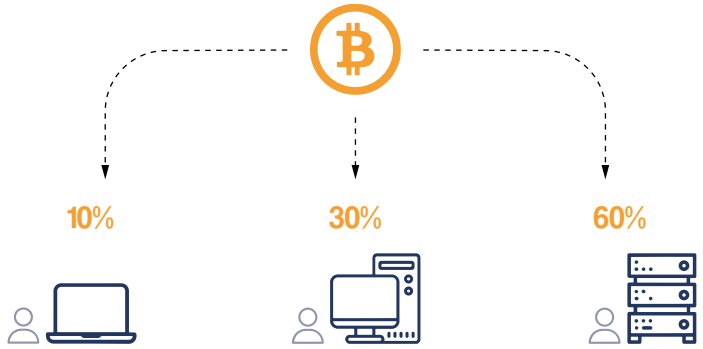


Figura 15

Ipotetico esempio di spartizione delle criptovalute minate in proporzione alle risorse messe a disposizione dagli utenti partecipanti.

Tale sistema di generazione dei blocchi risulta essere di altissima complessità da attaccare e pone le persone nella condizione di non aver alcun interesse nel danneggiare la blockchain perché non porterebbe ad alcun guadagno, anzi danneggerebbe tutti, l'hacker compreso.

World State

Il **mining** è quindi sia un **sistema di evoluzione** che di **sicurezza** della blockchain, ma non solo, ovvia anche al problema del "**world state**", ovvero: non è accettabile che esistano in contemporanea due versioni della catena e bisogna essere certi in maniera univoca su quale versione sia corretta.

Questa situazione è spiegata chiaramente dal **problema dei generali bizantini**. Si tratta di un dilemma logico che illustra come un gruppo di generali potrebbe avere problemi comunicativi.

Il problema dei generali bizantini

fonte ricavata da: academy.binance.com

Il dilemma suppone che ciascun generale abbia la propria armata e che ciascun gruppo sia situato in diverse posizioni intorno alla città che intendono attaccare. I generali devono decidere se attaccare o ripiegare. Non importa la decisione, purché tutti concordino su una scelta comune al fine di agire in maniera coordinata.

Gli obiettivi che devono essere raggiunti sono:

- Ciascun generale deve decidere: attaccare o ripiegare;
- Una volta presa la decisione, questa è definitiva e non può più essere cambiata;
- Tutti i generali devono concordare sulla stessa decisione ed eseguirla in modo sincronizzato.

I problemi di comunicazione menzionati sopra sono legati al fatto che un generale è in grado di comunicare con un altro soltanto tramite messaggi, recapitati da un messaggero. Di conseguenza, la sfida centrale del Problema dei Generali Bizantini è che questi messaggi possono arrivare in ritardo, essere distrutti o smarriti.

Inoltre, anche se un messaggio viene consegnato, uno o più generali potrebbero decidere (per qualsiasi ragione) di agire in modo disonesto e inviare un messaggio falso per confondere gli altri generali, portando a un totale fallimento.

Questa situazione si adatta allo scenario in cui opera una blockchain. I generali possono essere paragonati ai nodi, i traditori ai nodi maligni, i messaggeri possono essere il canale di comunicazione. La blockchain deve **raggiungere un consenso distribuito** anche in uno scenario come quello sopra descritto.

Byzantine fault tolerance

Per risolvere tale problema, ed essere sicuri che entità multiple riescano a trovare un accordo assoluto prima di intraprendere un'azione condivisa, sono stati sviluppati diversi **algoritmi denominati byzantine fault tolerant**. I due algoritmi più utilizzati nell'ambito delle blockchain sono il **Proof of Work** (PoW) e il **Proof of Stake** (PoS), ciascuno con le proprie varianti. I nodi che partecipano attivamente al processo di consenso (aggiungono nuovi blocchi, garantiscono la validità delle transazioni, ecc.) sono i miners.

2 - TECNOLOGIA

Proof of Work

Il **Proof of Work** è il primo sistema ideato per **raggiungere il consenso distribuito** all'interno della blockchain, si basa sul mettere in competizione i miner sulla risoluzione di un complesso problema utile alla realizzazione del blocco, il primo di questi che riuscirà a risolverlo convaliderà il nuovo blocco e otterrà un compenso.

La difficoltà ▶

Dato che è previsto un **tempo fisso** tra la generazione di un blocco e l'altro, la presenza di un alto numero di miners porterebbe automaticamente a un'accelerazione della convalidazione di blocchi per questo motivo viene introdotto un **vincolo denominato difficoltà**.

Bilanciare la difficoltà ▶

Vengono dunque imposte delle condizioni al problema in modo da **aumentarne la complessità e il tempo necessario alla risoluzione**, generalmente viene richiesto che il risultato della funzione di hash risulti inferiore a un determinato valore, minore è tale valore tanto più difficile diventerà trovare una soluzione valida al problema. La **difficoltà** viene quindi c**ommisurata all'hash rate** che la blockchain ha a sua disposizione, in modo da mantenere una generazione di blocchi costante nel tempo, per evitare disservizi o sovrapproduzione.

Tale soluzione presenta però delle **problematiche**:

- **Alto consumo energetico**: più una blockchain si diffonde, maggiore dovrà diventare anche la sua complessità arrivando a consumare sempre più corrente per la validazione dei blocchi.
- **Difficile scalabilità**: questo sistema mantiene costante il tempo tra una generazione dei blocchi e l'altra, ciò però agisce come **collo di bottiglia** nel momento in cui iniziano a registrarsi elevati volumi di transazioni, causando ritardi nei tempi necessari a una transazione ed elevate spese di commissione, i miners daranno logicamente precedenza alle transazioni più remunerative.
- **Vulnerabilità agli attacchi 51%**: tale sistema si basa sulla competizione al fine di randomizzare chi sarà responsabile della generazione dei blocchi e quindi prevenire tentativi di hacking, ma le blockchain piccole e poco diffuse corrono un rischio, se un utente in linea teorica riuscisse da solo a fornire più del 50% della potenza di calcolo a disposizione di una blockchain avrebbe la possibilità, con il vantaggio della maggioranza, di introdurre nodi malevoli nella catena, compromettendone l'integrità.

◀ Vulnerabilità 51%

2 - TECNOLOGIA

2 - TECNOLOGIA

Proof of Stake

Mettere in Staking

Il **Proof of Stake** è successivo al PoW e viene ideato per risolverne le criticità. Il nome nasce dal termine inglese che significa in gergo "**puntare**", nel senso di scommettere. Il funzionamento è semplice: invece di scontrarsi sulla potenza di calcolo, si basa sul **congelare una quota delle criptovalute** possedute dai miners, maggiore sarà la somma posta in **staking** maggiori saranno le probabilità di **essere scelti per la convalidazione del blocco**, viene così **eliminato il fattore della difficoltà**, riducendo il consumo energetico.

Sanzioni

In questo sistema eventuali tentativi di manomissione vengono prevenuti tramite lo staking stesso, una volta che un miner viene incaricato della convalidazione del blocco questo sarà poi **soggetto ad approvazione** da parte degli altri miners del network, nel caso venissero **evidenziate delle irregolarità** il miner incaricato inizialmente subirà una **multa** perdendo la somma che egli aveva posto in staking. Questo sistema previene tentativi di attacchi poichè ponendo come garanzia i propri beni, i miners **non avrebbero vantaggi** nel rischiare una manomissione della blockchain.

Anche il **problema dell'attacco 51% non sussiste** dato che per replicare un tentativo simile sarebbe necessario possedere il 51% dei token in staking e colui che anche riuscisse a possederne una tale percentuale sarebbe il primo interessato a far sì che la blockchain funzioni correttamente, altrimenti tutti i suoi token perderebbero di valore.

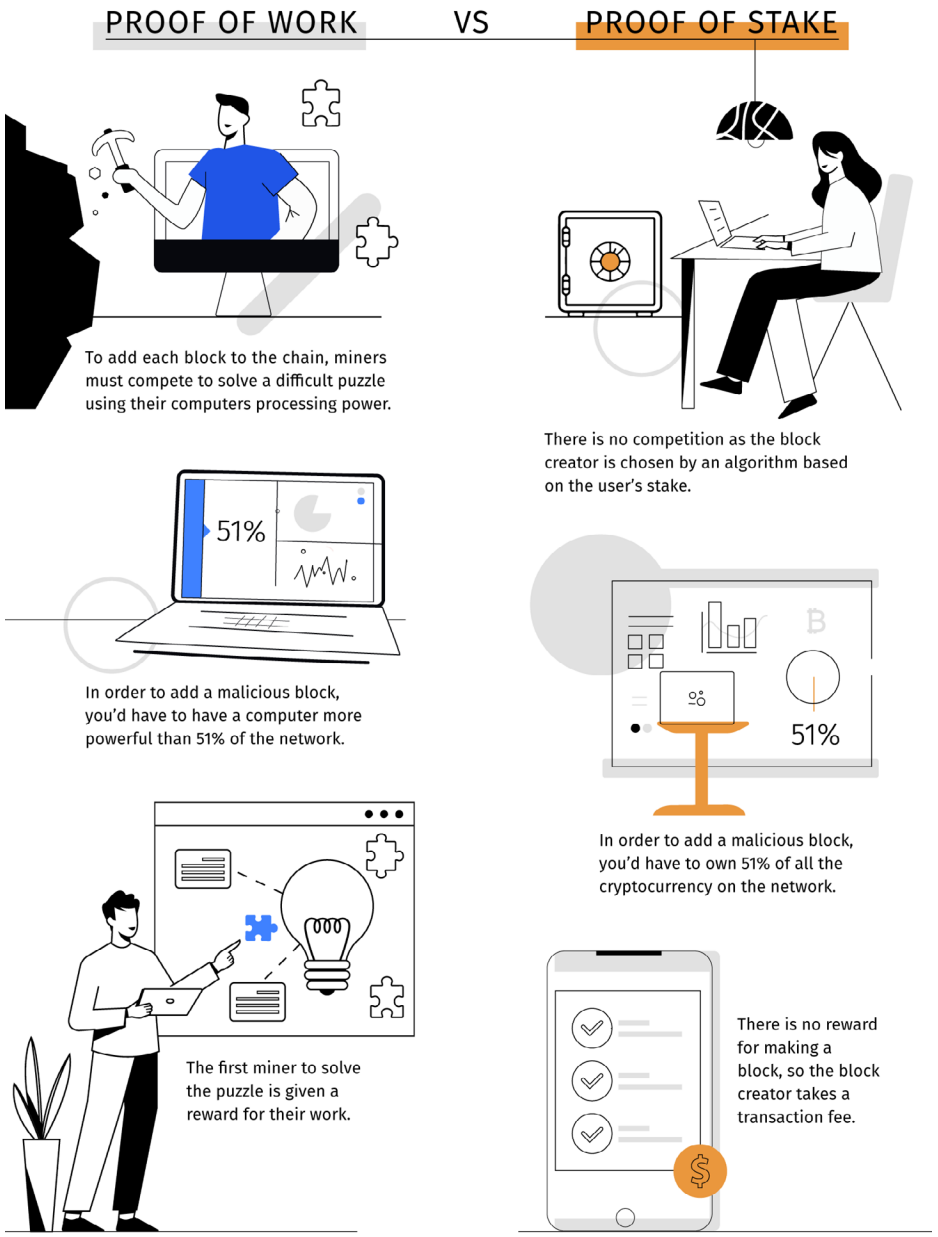


Figura 16

Grafica illustrativa che pone in risalto le principali differenze tra i sitemi PoW e PoS.

(fonte: cult of money)

2 - TECNOLOGIA

Wallet e Indirizzi

Il sistema della blockchain non comprende profili utente, esistono indirizzi che prendono parte a transazioni e si possono gestire tramite strumenti digitali chiamati **Wallet**.

Un indirizzo prevede **due chiavi crittografiche**, una che deve rimanere privata e una pubblica, utile all'invio di denaro, queste costituiscono la **firma digitale** e vengono gestite dal Wallet.

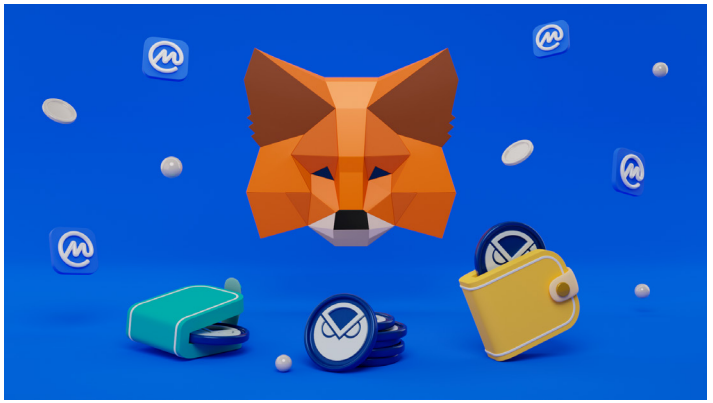


Figura 17

Illustrazione 3d di Metamask uno dei principali e più utilizzati wallet.

Per creare un indirizzo nuovo viene generata una chiave privata a partire da un numero casuale, in seguito viene generata la chiave pubblica dalla chiave privata tramite una funzione matematica e in fine essa viene criptata con una funzione di hashing, il risultato è l'indirizzo sulla blockchain.

Esistono **tre tipi di wallet**, hardware, software e cartacei che a loro volta sono divisibili in **hot storage** e **cold storage**.

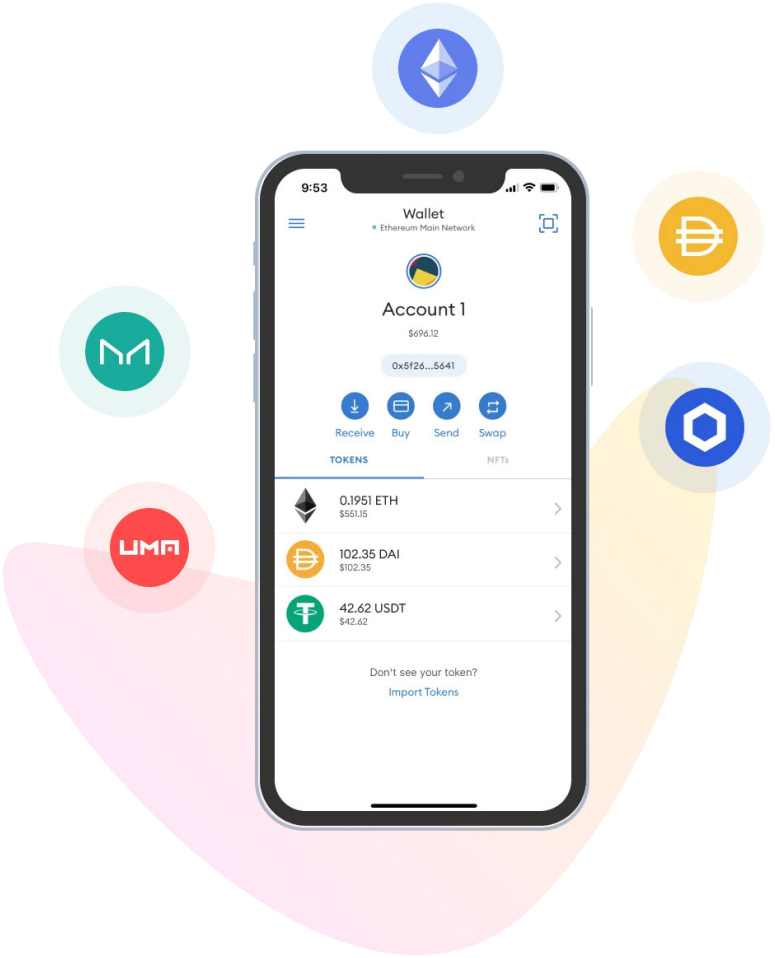


Figura 18

Interfaccia smartphone principale di Metamask, riportante nome del wallet, il suo contenuto e le principali azioni che si possono svolgere .

Hot e Cold storage

Il termine **hot storage** indica un wallet **connesso a internet**, quindi le chiavi private sono salvate sulla rete, al contrario un wallet **cold storage** non è connesso alla rete e per questo motivo è **più sicuro**.

- Il **paper wallet** o wallet cartaceo è una tipologia di wallet a cold storage molto semplice, consiste banalmente nella chiave privata e nell'indirizzo stampati su un foglio di carta.
- Con **software wallet** si intende un'app installata su smartphone o su computer che, tramite un accesso protetto da password, memorizza chiave privata e indirizzo. I vantaggi sono sicuramente la rapidità e semplicità di utilizzo, ma lo svantaggio principale è il fatto che, se il sistema sul quale è installato venisse hackerato, la chiave potrebbe essere rubata.
- Gli **hardware wallet** sono il compromesso perfetto tra sicurezza e facilità d'uso, sono contraddistinti da un hardware esterno che memorizza chiave privata e indirizzo, ogni transazione viene verificata all'interno dell'hardware stesso, in un'area sicura.

Il contenuto di un wallet

I wallet memorizzano le chiavi ma **non contengono cripto valute**, esse infatti non esistono nemmeno digitalmente, ciò che avviene in una transazione non è altro che **un'operazione matematica** e i wallet contengono il risultato di essa.

Figura 19

Semplice esempio di un paper wallet, per conervare off line le proprie chiavi d'accesso private.


Ledger
Choose PIN
with 4 to 8 digits
ethereum
ethereum

2 - TECNOLOGIA

UTXO

L'**Unspent Transaction Output** è uno dei modelli contabili con cui si tiene traccia delle transazioni in blockchain. Oltre a verificare la validità delle transazioni effettuate, consentono anche di calcolare la quantità di token posseduti in un preciso momento da un indirizzo.

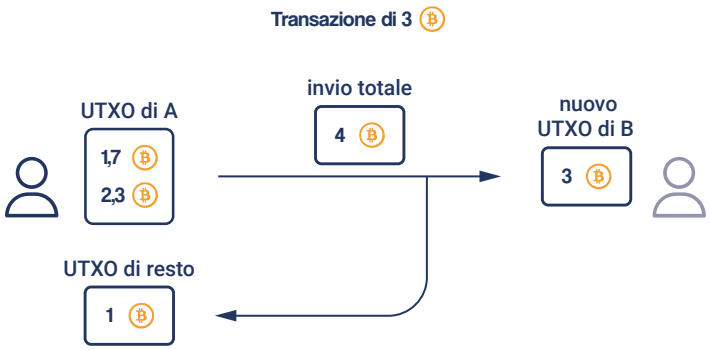
Definizione UTXO

L'UTXO è la rappresentazione di una determinata **somma che si è ricevuta** da terzi, ma che in quel momento **non si è ancora provveduti a spendere**. I wallet registrano tutti gli UTXO che vengono ricevuti o spesi da un indirizzo, gestendoli come fossero assegni in quanto **non frazionabili**.

Quando si effettua una transazione verranno quindi **spesi per intero uno o più UTXO** posseduti, anche se si supera l'importo che intendiamo inviare. I token in eccesso non finiscono perduti ma vengono riconsegnati come resto attraverso un altro UTXO all'indirizzo mittente.

Figura 20

Schematizzazione di una transazione effettuata tramite multipli UTXO.



Questo sistema risulta un' efficace soluzione al problema del **double spending** (truffa che consiste nello **spendere lo stesso titolo valutario due o più volte**), dal momento che viene ceduto il titolo, ovvero l'UTXO, per intero nel momento in cui si effettua una transazione e non è quindi possibile eseguire una seconda transazione con esso.

Il resto

Nella **necessità di un resto**, se per esempio non esiste una combinazione di UTXO in nostro possesso pari alla quota che vogliamo trasferire, ne verrà generato uno di ritorno che riceveremo successivamente alla convalida della transazione, affinché questa venga correttamente registrata su blockchain e non risulti più modificabile da parte di terzi nel caso si tentasse una frode.

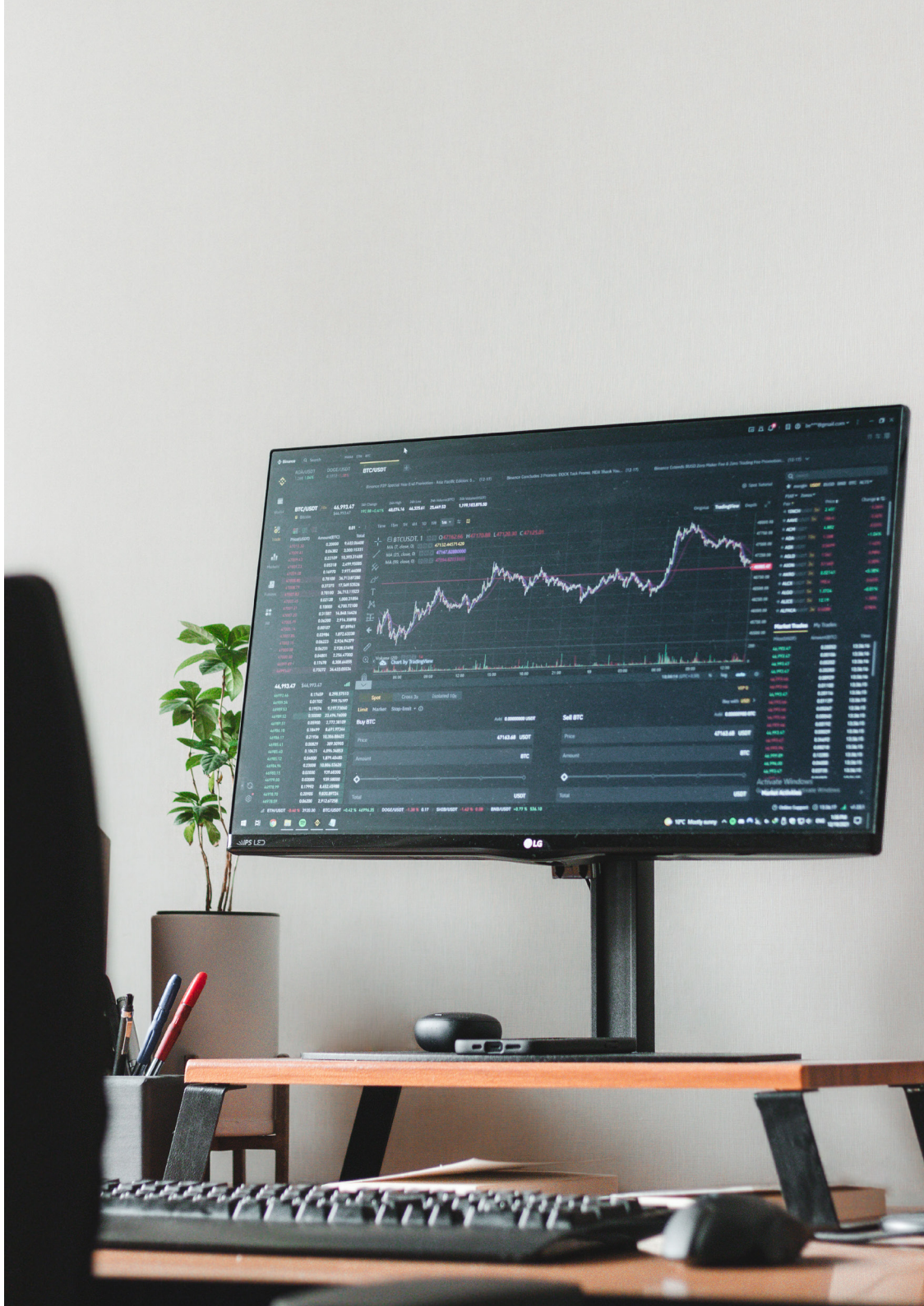
Applicazioni

Blockchain, Applicazioni

Analogamente al mondo dello sviluppo dei software, si potrebbe affermare che la tecnologia della blockchain si trovi ancora in uno **stadio di Beta**, nome che si assegna alla fase in cui gli utenti usufruiscono dell'applicazione e svolgono dei **test** per mettere alla prova la solidità del software.

Inoltre, come spesso accade per nuove scoperte tecnologiche, la tendenza iniziale è quella di utilizzarle per compiti obsoleti. Le potenzialità che questo nuovo strumento offre sono in larga parte ancora da scoprire.

La blockchain viene però già utilizzata in diversi settori, per **ridurre costi** e **ottimizzare processi**, nelle prossime pagine vedremo alcuni esempi.



Criptovalute

Grazie a tecnologie di ledger distribuiti, come la blockchain, per la prima volta nella storia è possibile effettuare transazioni di beni o denaro senza la presenza di un garante, come ad esempio una banca.

Grazie a questo tipo di tecnologia infatti **non si incorre nel rischio di controparte**, ovvero che lino dei due facenti parte dello scambio non rispetti le condizioni stabilitein comune accordo.

Vantaggi

Esse non hanno una valuta fisica, non hanno confini geopolitici ed ereditano le proprietà della tecnologia sulla quale si basano, come trasparenza, sicurezza e immutabilità.

Le cripto valute sono l'applicazione della blockchain di maggior successo, il Bitcoin, ideato nel 2008 da **Satoshi Nakamoto** (pseudonimo, la vera identità è ignota), è stato il precursore e possiede ancora il primato di cripto valuta di maggior valore.

Figura 21

Principali criptovalute, il loro valore come qualsiasi valuta nazionale è monitorabile nel mercato azionario.

Smart Contract

Il termine smart contract viene utilizzato per la prima volta nel 1994 da **Nick Szabo**, che lo definisce come "**un protocollo di transazione digitale che esegue i termini di un contratto**".

Più semplicemente, uno smart contract è come un contratto tradizionale, con la differenza che non è scritto su carta e non viene gestito da persone, bensì è **scritto in codice informatico** per eliminare ogni equivoco e viene svolto da un computer.

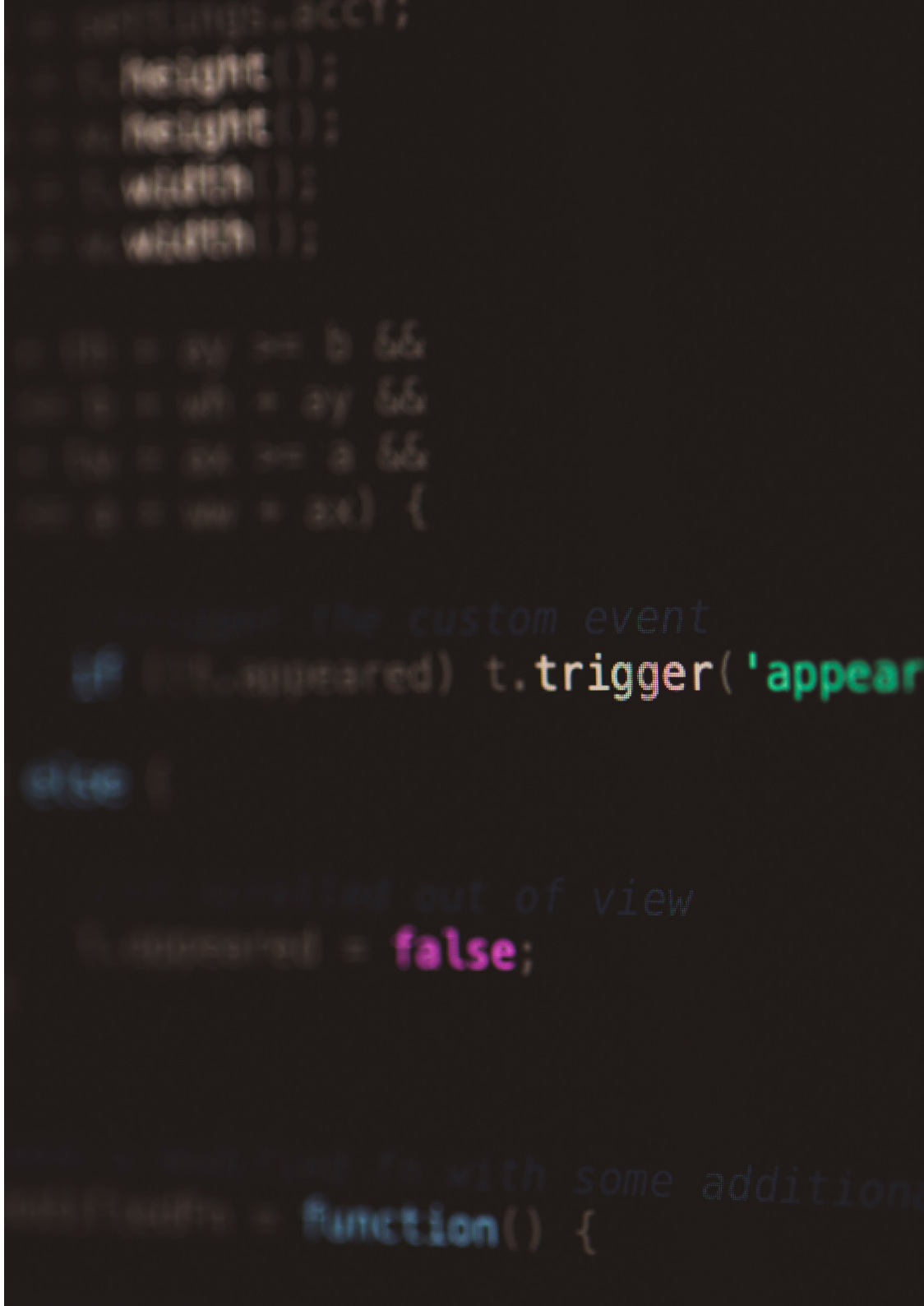
Funzionamento

Gli smart contract vengono scritti in **Solidity**, un software creato appositamente e sono semplificabili con la formula "**if this, then that**", ovvero quando si verifica la condizione concordata questo applica e svolge automaticamente i termini previsti dal contratto, senza che le parti debbano agire in prima persona per mantenere gli accordi.

Esso viene **registrato nella blockchain**, quindi una volta convalidato non può essere modificato e verrà eseguito quando si verificano condizioni prestabilite dall'accordo.

Liberarsi degli intermediari

Ciò permette di **ridurre costi e inefficienze** che si verificano nel mondo reale quando ci si affida a delle autorità centralizzate o a un garante esterno. Questi vantaggi rendono gli smart contract utili in molte situazioni, come nell'ambito delle transazioni finanziare senza bisogno d'intermediari, nella **gestione di proprietà** (smart property) e anche nel settore delle assicurazioni.



Industria 4.0 e IoT

La blockchain trova grande utilità nelle supply chain, ovvero nella f**iliera di produzione e logistica** di un qualsiasi bene. Al giorno d'oggi le filiere sono molto complesse, suddivise in **molteplici fasi** che spesso avvengono in luoghi differenti.

Tracciamento

Grazie alla blockchain è possibile tener traccia della **grossa mole d'informazioni** derivata dai vari step, **ridurre le inefficienze**, **tracciare merci** lungo le fasi di lavorazione e **aumentare la trasparenza** dell'intero processo. Ciò comporta una maggiore qualità del prodotto finale, diminuizione del costo, dei tempi di trasporto e stoccaggio e diminuzione degli sprechi lungo la filiera.

IoT

Per **Internet of Things** si intende un'insieme di dispositivi fisici interconnessi e capaci di raccogliere e scambiare informazioni. Ad esempio la domotica, che fa largo uso di sensori ed elettrodomestici, è in grado di gestire e automatizzare diversi processi interni a un nucleo abitativo.

Allo stesso modo anche l'industria dell'automotive sta producendo sempre più smart car, vetture con capacità di connettersi, raccogliere dati, stimoli e comunicare in un network.

È dunque chiaro come la blockchain, supporti e aiuti a gestire una filiera industriale di questo tipo, destinata a crescere esponenzialmente, con grossi scambi di dati e processi da gestire.

Figura 22

Carrefour, catena di supermercati è una delle prime grandi aziende ad aver implementato nella sua filiera la blockchain, viene utilizzata per tracciare la filiera dei suoi prodotti per garantirne la qualità e sostenibilità.

Peroni e EY Opschain

Recentemente, anche Peroni, noto marchio di birra italiano, ha deciso di sfruttare la tecnologia della blockchain a suo favore, portando trasparenza e **tracciabilità** all'interno della sua filiera di produzione tramite la **piattaforma EY Opschain.** Essa consente di autenticare le informazioni e **tokenizzare i beni venduti** come NFTs sulla blockchain pubblica di Ethereum.

Tokenizzare

Con il termine tokenizzazione si intende il processo di **conversione dei dati** sensibili in simboli d'identificazione univoci che conservano le informazioni essenziali senza comprometterne la sicurezza. Questo processo è molto utile per ridurre al minimo la quantità di dati sensibili che un'azienda deve gestire, o per certificare il rispettarsi di certi **standard di qualità.**

Tracciamento

Grazie a questa tecnologia, i **consumatori** possono seguire il viaggio del malto, la materia prima, dal campo alla bottiglia, scoprendo informazioni come la data della raccolta, la località e molto altro.

La piattaforma di tracciabilità EY Opschain permette alle aziende di utilizzare la blockchain come **estensione del loro ERP**(pianificazione delle risorse d'impresa), **semplificando la gestione** della supply chain, dalla produzione alla vendita.

Il brand guadagna anche credibilità, potendo supportare con dati il suoe legame con la filiera agricola e la qualità del malto 100% made in Italy.

Figura 23

Una bottiglia in vetro di birra Peroni

Ambito Governativo

La blockchain, che può essere condivisa su reti pubbliche o private, risulta un grande strumento anche nella **gestione di questioni burocratiche**, da sempre afflitte da ritardi e inefficienze. Già diversi paesi nel mondo stanno testando questa tecnologia per semplificare processi in **ambito di sanità**, **pagamento delle imposte**, istruzione e in generale **snellire la burocrazia**.

Identità digitale ▶

Ad esempio, tramite la blockchain, l'identità digitale potrebbe essere riconosciuta in tutto il mondo in maniera univoca, slegandola da ogni apparato governativo.

Una diretta applicazione di ciò potrebbe essere il **voto digitale**, dove ogni cittadino riconosciuto digitalmente può votare in maniera remota, senza incombere in rischi come corruzione e modifica delle schede elettorali. La votazione si svolgerebbe come una normale transazione registrata sulla blockchain, in totale **trasparenza e sicurezza**.

Nel settore della sanità invece la blockchain potrebbe trovare grande utilizzo nella **gestione delle cartelle cliniche**.
La tecnologia aiuterebbe di certo a controllare la grande mole di dati in costante aggiornamento, in questo modo sarebbe possibile avere un quadro clinico più completo del paziente in diverse regioni e anche all'estero, in modo da garantire le cure più idonee al paziente.

Figura 24

L'introduzione di blockchain per l'archiviazione delle cartelle cliniche consentirebbe ai medici ovunque nel mondo di conoscere i dettagli rilevanti sul paziente, utile soprattutto nei casi di emergenza. ▶▶

Fizzy di Axa Insurance

Esistono interessanti casi studio riguardanti gli smart contract, ad esempio **Fizzy di Axa assicurazioni**, un gruppo assicurativo di rilievo.

Si tratta di un esperimento operato nel settore dei viaggi in aereo e consentiva di acquistare un'**assicurazione per ritardi e cancellazioni** dei viaggi prima della partenza, il tutto in maniera sicura, trasparente e automatica, sfruttando proprio le potenzialità degli smart contract.

Registrazione

Al momento della registrazione il customer inserisce i dati del suo volo e il costo della polizza deriva direttamente dal rischio di cancellazione. Nel caso in cui il volo venisse cancellato o subisse un ritardo maggiore di due ore i clienti riceveranno il **rimborso in maniera automatica**, **senza alcuna azione richiesta da parte loro**.

Questo poiché Fizzy riceve le informazioni di base sul volo e **lo smart contract esegue il rimborso** nel caso si verifichino le condizioni sufficienti.

Blockchain a supporto del progetto

Tali contratti si basano sulla blockchain di **Ethereum**, seconda criptovaluta per importanza dopo Bitcoin, consultabile da chiunque, famosa per la sua praticità riguardo smart contract e NFT.

Chiunque può programmare un contratto per poi salvarlo sulla catena, possono in seguito venir richiamati con un evento trigger e svolgere in questo modo la loro funzione. Sia il file di codice che la transazione sono **consultabili liberamente**.

Fizzy prevede **diversi tipi di azioni**, quindi diversi codici, ognuno per una **funzione diversa**, ad esempio "addNewInsurance" per registrare un nuovo cliente, oppure "triggerCondition", per controllare lo stato di un volo, nel caso venisse cancellato o subisse un ritardo. Lo smart contract viene quindi utilizzato due volte, alla sottoscrizione e all' arrivo del volo. In qualsiasi momento il customer può disdire la polizza.

Le **informazioni personali** riguardanti il volo vengono inoltre **criptate** prima di essere inserite nella blockchain, così da mantenere la privacy.

Esiti del progetto

Il progetto risale al 2017 ed è stato chiuso dopo due anni circa a causa della **scarsità di domanda**, poiché ancora poche persone usufruiscono di tale tecnologia. Tuttavia ha riportato **esiti positivi** ed è stato un **progetto avanguardistico** per ciò che riguarda l'applicazione delle potenzialità degli smart contract nelle situazioni di vita quotidiana.

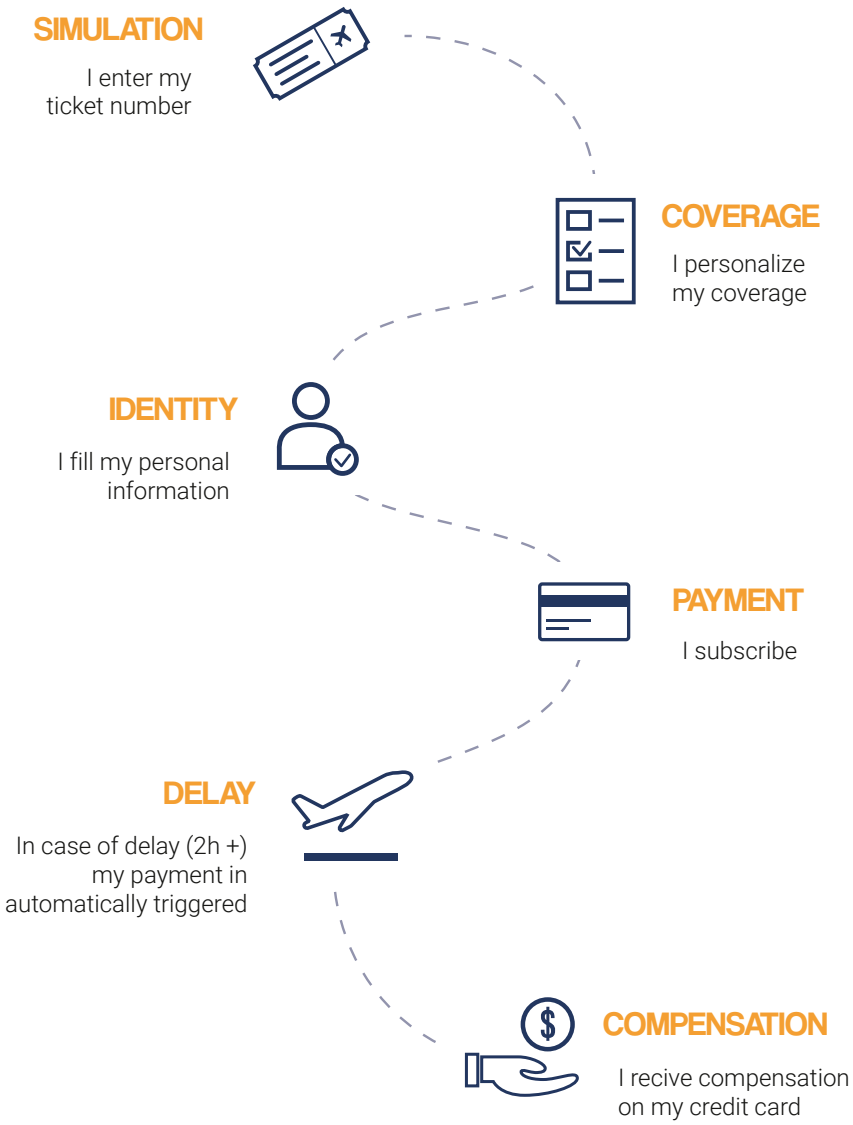


Figura 25

Schema rappresentante i principali passaggi per usufruire del servizio assicurativo smart progettato da Axa per i ritardi aerei.

Super Chair

Tra le diverse novità proposte nel 2023 al Salone del mobile di Milano spicca il progetto **Super Chair**, presentato da Damiano Latini in collaborazione con il designer newyorchese Nicholas Baker.

Nicholas Baker

Progettare in VR

Oltre al processo produttivo la Super Chair risalta per la sua particolare progettazione, Nicholas Baker è un designer particolarmente attento alle nuove tecnologie e novità progettuali che non teme di sperimentare, questa seduta è infatti stata modellata in 3d ma in **realtà virtuale** tramite un visore e due controller che consentono di mettere direttamente le "mani" sul modello, interagendo con volumi e assottigliando la barriera che ancora separa realtà e metodi convenzionali di progettazione, tale metodo di modellazione 3d in realtà virtuale è possibile attraverso il software **Gravity Sketch VR.**

Figura 26
Damiano Latini, a sinistra, e Nicholas Baker, al centro, al salone del mobile di Milano 2023.

Figura 27
Retro Superchair.

Possedere un oggetto oppure la sua idea

Ogni progetto o iterazione di prodotto che realizza viene **coniato come NFT** (tramite il minting), per **tutelare il diritto d'autore** e poiché possiede valore artistico. Ciò è considerabile al pari di comprare gli sketch o un brevetto di un designer famoso o di un progetto di successo.

Tuttavia, nella prospettiva di sviluppo del Metaverso e del concetto di **smart property**, è possibile ipotizzare un futuro in cui questi progetti 3D diventeranno la **controparte virtuale** dei beni fisici del mondo reale, come case, oggetti, mobili, indumenti e molto altro.

Da ciò si aprono infinite possibilità, come quella di **acquistare i diritti di produzione di un prodotto tramite il suo NFT** oppure di creare progetti d'interior design direttamente in realtà virtuale, sperimentando cosa si prova a navigare lo spazio come se fosse l'ambiente finito.

Tutela dei diritti d'autore

L'applicazione degli smart contract in ambiti simili andrebbe a risolvere questioni legali inerenti i diritti d'autore di vari ambiti, brevetti di progetti, brani musicali, attestati di proprietà, innumerevoli sarebbero i contesti dove l'applicazione di questi non solo semplificherebbe l'ipotetico acquisto di un bene ma allo stesso tempo tutelerebbe costantemente i diritti riservati al proprietario o all'autore originale.

Figura 28
Vista Superchair.

Bored Ape Yacht Club

Riconoscere i diritti dell'artista

Riguardo ai riconoscimenti dei diritti d'autore, il primo esempio applicato sono gli **NFT**, questi nascono come **opere d'arte digitali**, e sono un ottimo esempio in tal senso perché, oltre a rendere sempre nota l'originalità e l'autore dell'opera, nel momento in cui vengono messi in vendita l'autore tra vari fattori tra cui il numero di copie, può scegliere se riservarsi dei **diritti sulla compravendita** della sua opera e specificare nel caso la percentuale a lui riservata, così facendo se la sua opera venisse in futuro rivenduta lui **riceverà automaticamente una percentuale** sul prezzo a cui questa è stata scambiata in seguito al suo rilascio.

Ciò è possibile perché è scritto direttamente nel codice dell'NFT (che è a tutti gli effetti uno smart contract) l'attuale proprietario, l'autore originale, tutti i diritti a lui riservati e le transazioni che hanno coinvolto quello specifico NFT.

Diatriba tra Meta e la SIAE

Si immagini adesso un sistema così automatico e sicuro applicato a uno dei campi che più ha problemi inerenti ai diritti: la musica, l'ultimo esempio attuale è la diatriba tra Meta e la SIAE.

BAYC tra i primi progetti NFT

BAYC è uno dei primi progetti NFT nati e di sicuro quello di maggiore successo, in larga parte grazie alla visibilità mediatica che gli è stata offerta da personaggi dello spettacolo (in maniera più o meno involontaria) ma è innegabile che il progetto sia andato ben oltre al semplice collezionismo.

Figura 29
Logo di BAYC.

Grazie a iniziative sempre nuove e **coinvolgendo in prima persona gli utenti** è nata una vera e propria comunità, che dialoga e partecipa in prima persona ai progetti.

Ape Fest, NY

L'apice di tale concetto di comunità che si è sviluppato è l'**Ape Fest** nato nel 2021 e verificatosi in una seconda edizione nel 2022, sempre a New York, posso partecipare al festival solo i membri della community, cioè coloro in possesso di un NFT di BAYC, questo evento come altre iniziative hanno reso questo progetto un **club estremamente esclusivo**, dove è possibile incontrare anche molti personaggi famosi e imprenditori.

L'esclusività

Attualmente è anche in sviluppo **Apecoin** una criptomoneta che avrà una funzione di scambio solo all'interno della community di BAYC che potrà essere guadagnata contribuendo alla community stessa e darà anche potere di voto nelle scelte da intraprendere nei progetti futuri.

Figura 30

Installazione gonfiabile sul pier 17 a New York per l'evento dell'Ape Fest 2022.


APE
FEST

Conclusioni

Riflessione Conclusiva

Come si è dimostrato tramite questa ricerca, le potenzialità e i **campi di applicazione** di questa tecnologia sono innumerevoli. Esistono ancora degli **aspetti da perfezionare**, per citarne uno il consumo energetico, ma è indiscutibile che la tecnologia blockchain nel prossimo futuro porterà ad una **rivoluzione dei servizi** e di come ci rapportiamo in questo mondo globalizzato.

Tutte le barriere geopolitiche che attualmente impediscono un rapporto diretto tra individui saranno infrante dalla velocità e facilità di comunicare, è ipotizzabile inoltre che andranno a stravolgersi quelli che ad oggi vengono ritenuti i normali **rapporti di uso e fruizione** di un utente nei confronti di un prodotto.

Strumenti che ad oggi vengono ritenuti indispensabili **diventeranno inevitabilmente obsoleti**, primo su tutti il portafoglio. Attualmente, con servizi come ApplePay, è già possibile uscire di casa senza la versione fisica della carta di credito. In un futuro non molto lontano è possibile che anche bancomat, documenti e altri certificati **non esisteranno più**, ma verranno sostituiti da una piccola quantità di dati associati alla nostra **identità digitale** e salvata su una blockchain, diffusa nello stato o addirittura mondiale, in una visione utopistica.

Risulta difficile immaginarsi una trasformazione del genere o prevedere cosa potrebbe succedere in futuro, ma a seguito della nascita d'Internet, è stato possibile osservare come l'**evoluzione** tecnologica segua una curva **esponenziale**, la rete è infatti ormai presente in quasi tutte le azioni che compiamo quotidianamente, senza nemmeno rendercene più conto.

Al contrario, altre tecnologie diventeranno **obsolete** ancor più rapidamente, basti pensare ai DVD, ormai scomparsi da anni anche se ci appaiono come uno strumento recente. Superati da **tecnologie più avanzate**, hanno perso la loro funzione: film, software e videogiochi vengono fruiti ormai solo tramite la rete. Il medesimo esempio si può fare per le chiavette USB, sostituite da servizi quali Drive o ICloud.

In tutti i casi sopra riportati, i consumatori hanno **mutato** radicalmente il loro concetto di **esperienza d'uso**, e solo nel giro di pochi anni. Questi esempi suggeriscono il modo in cui dobbiamo guardare alla blockchain, perché si tratta di un **progetto in sviluppo** che, anche se verrà inizialmente utilizzato per dei compiti obsoleti, sarà in grado di rivoluzionare ambiti che ancora non possiamo immaginare.

È quindi necessario **comprenderla e approfondirla**, per restare aggiornati con questa rivoluzione tecnologica e **fruirne in maniera attiva e consapevole**.

Indice

INTRODUZIONE p.05

- Perchè la Blockchain p. 08

TECNOLOGIA p. 10

- I Blocchi p. 16
- Blockchain Explorers p. 18
- Funzione di Hash p. 20
- La Crittografia p. 22
- Hash Rate p. 24
- Il Mining p. 26
- World State p. 30
- Proof of Work p. 32
- Proof of Stake p. 34
- Wallet e Indirizzi p. 36
- UTXO p. 42

APPLICAZIONI p. 44

- Criptovalute p. 48
- Smart Contract p. 50
- industria 4.0 e IoT p. 52
- Peroni e EY Opschain p. 54
- Ambito Governativo p. 56
- Fizzy di Axa Insurance p. 58
- Superchair p. 62
- Bored Ape Yacht Club p. 68

CONCLUSIONI p. 76

- Riflessioni Conclusive p. 78

Bibliografia

- Chiap G.; Ranalli J.; Bianchi R. - **Blockchain, Tecnologia e Applicazioni** - Hoepli, 2019
- Nakamoto S. - **Bitcoin: un sistema di moneta elettronica peer-to-peer** - Author's Rupublic
- Garavaglia R. - **Tutto su Blockchain. Capire la tecnologia e le nuove opportunità** - Hoepli, 2018
- Nuzzo A. - **Blockchain e Autonomia Privata** - 2021
- P. J. Owings - **Metaverso e NFT: la rivoluzione del play to earn e l'arte digitale su Blockchain** - 2022
- McClendon D. - **NFT: L'enciclopedia completa dei Non Fungible Token** - 2022
- CJ Bangah - **Blockchain in advertising - Is it the answer to digital advertising's trust and transparency gap?** - pwc, 2019
- M. J. Yuan - **Sviluppare applicazioni blockchain. Guida per creare sistemi decentralizzati su reti distribuite** - Apogeo, 2019
- Attico N. - **Enterprise blockchain. Legaltech e altri strumenti per professionisti e imprese** - Guerini Next, 2021

Sitografia

- **Coinbase:** Tutto quello che c'è da sapere sulla Fusione di Ethereum (ultima consultazione 13-06-2023)

  https://www.coinbase.com/it/ethereum-merge
- **Fizzy by Axa**: Ethereum smart contract in details (ultima consultazione 17-06-2023)

  https://medium.com/@humanGamepad/fizzy-by-axa-ethereum-smart-contract-in-details-40e140a9c1c0
- **Etherscan**, blockchain di Fizzy, smart contract (ultima consultazione 20-06-2023)

  https://etherscan.io/address/0xdc3d8fc2c41781b0259175bdc19516f7da11cba7#code
- **Case Study**: Walmart and Hyperledger Fabric (ultima consultazione 6-06-2023)

  https://www.hyperledger.org/learn/publications/walmart-case-study
- **Binance Academy** (ultima consultazione 22-06-2023)

  https://academy.binance.com/it
- **Techtarget:** la tokenizzazione (ultima consultazione 28-06-2023)

  https://www.techtarget.com/searchsecurity/definition/tokenization

Ringraziamenti

Emanuele

Un sentito ringraziamento va a tutti i miei amici e parenti che mi hanno accompagnato durante questo percorso.

In particolar modo ringrazio mio padre Mirto, che sin da piccolo mi ha fatto appassionare al disegno, mio nonno Benedetto, che io considero un proto-designer e segue ogni mio progetto e idea che mi vengano in mente, mio nonno Alfio che, nonostante i pochi anni trascorsi insieme, mi ha insegnato a pensare e ad avere curiosità, e Federica, che da un po' mi accompagna e mi sprona a dare il meglio di me.

Pier

Ringrazio tutti i compagni e amici incontrati in questi anni, che anche se per brevi periodi, hanno saputo non solo offrirmi un'ottima compagnia ma un diverso punto di vista.

Un doveroso grazie alla mia famiglia che non mi ha mai fatto mancare nulla e vuole il meglio per me e per il mio futuro.

Grazie a Ginger che con la sua sincera passione e dedizione al design è un punto di riferimento oltre che un'amica.

E un ringraziamento a tutte le persone importanti che hanno iniziato questo percorso con me, ma purtroppo non sono qui oggi, immagino sarebbero state orgogliose.

Ringraziamo il professor Monetti per la sua guida e disponibilità