LUISS

CORSO DI LAUREA IN ECONOMIA E MANAGEMENT

Cattedra: Informatica

« I DBMS e la Blockchain: un futuro cristallino»

Relatore
Prof. Laura Luigi

Candidato
Samuel Dammicco
253611

Anno accademico 2022/2023

Indice

1. Introduzione

In Italia le transazioni digitali stanno diventando sempre più comuni, arrivando a rappresentare il 40% delle spese degli italiani. Ciò ha portato a una media di 1,2 miliardi di Euro scambiati ogni giorno attraverso i mezzi di pagamento digitali, rappresentando una forte crescita che sta portando alla progressiva riduzione del denaro contante utilizzato.

Questo aumento della popolarità dei pagamenti digitali è dovuto all'introduzione e all'evoluzione di tecnologie e mezzi di pagamento come le carte di credito, i bonifici bancari, i pagamenti tramite home banking, con smartphone e con applicazioni via mobile dedicate. Questi strumenti hanno reso gli acquisti e le transazioni finanziarie più semplici e convenienti per le persone, aumentando la velocità di circolazione della moneta e migliorando l'efficienza degli scambi di denaro.

Nonostante la crescente popolarità dei pagamenti digitali, il denaro contante rimane ancora il principale mezzo di pagamento per molte persone, soprattutto per gli anziani che si sentono più a loro agio con il semplice foglio di carta che rappresenta, in alcune situazioni, l'unica opzione, come ad esempio nei mercati all'aperto o nei piccoli negozi che ancora non accettano pagamenti digitali.

Ci sono anche alcune preoccupazioni sulla sicurezza dei pagamenti digitali. Molti temono che i pagamenti digitali possano essere più vulnerabili agli hacker e ai criminali informatici rispetto alle transazioni in contanti. Inoltre, alcune persone hanno paura di perdere il controllo dei propri soldi quando li depositano in una banca o li usano per fare acquisti online.

Tuttavia, nonostante queste preoccupazioni, i pagamenti digitali diventeranno sempre più popolari in futuro.

Ciò significa che le banche e le altre istituzioni finanziarie dovranno adattarsi alle mutevoli esigenze dei loro clienti e sviluppare nuovi servizi per soddisfare queste esigenze. Ad esempio, molte banche stanno investendo in tecnologie di sicurezza per proteggere i loro clienti da frodi e crimini informatici, mentre altre stanno sviluppando

nuovi servizi di pagamento mobile per semplificare ulteriormente le transazioni finanziarie.

Tra queste, una tecnologia di spicco, per le sue caratteristiche di sicurezza, trasparenza, scalabilità e efficienza è quella della Blockchain, dotata di caratteristiche avanguardistiche in termini tecnologici. Si tratta di un nuovo concetto di database in cui i dati sono potenzialmente a disposizione di tutti, ma non sono di nessuno. Una situazione di reale democrazia in cui nessuno può arrogarsi il diritto di prendere una decisione piuttosto che un'altra, non permettendo manipolazioni di dati di nessun tipo, grazie alla crittografia.

Prima dell'avvento dei pagamenti digitali, le transazioni richiedevano l'uso di contante o di assegni bancari, che erano soggetti a limitazioni evidenti, quali i costi di emissione, la necessità di avere fisicamente l'assegno a portata di mano e i rischi di smarrimento e furto che ne conseguono, oltre a limitazioni di carattere temporale rappresentate dall'impiego di tempo necessario per l'esecuzione di un pagamento.

Quest'ultima limitazione si identifica a tutti gli effetti con un costo che prende il nome di "costo delle suole" e rappresenta appunto la scomodità e il tempo perso per recarsi in banca più spesso, alludendo al fatto che per lo spostamento in sé, vengano consumate le scarpe.

In generale, a limitazioni di questo tipo corrispondono sempre dei costi, evitabili tramite l'implementazione di tecnologie più all'avanguardia.

L'integrazione dei mezzi digitali per effettuare spostamenti di denaro ha quindi reso questi ultimi molto più rapidi, efficienti e sicuri, aumentandone l'utilizzo e modificando profondamente la concezione della spesa e tutti i meccanismi mentali che ne conseguono.

Spendere moneta ora è molto più semplice, a tal punto da far sembrare più abbordabile e leggera l'uscita di denaro, facendo aumentare le spese più trascurabili e inutili, rendendole meno trascurabili sul bilancio personale annuale.

Ogni transazione che viene effettuata porta con sé dei dati che vengono collezionati in appositi database, o "registri contabili", che possono essere di diverso tipo in base alla tecnologia su cui si fondano. Questi database possono essere utilizzati per vari scopi, come l'analisi dei dati, la statistica sulle ricerche relative alle spese dei consumatori, la profilazione a scopo lucrativo da parte delle grandi aziende e la prevenzione di alcune frodi.

Inoltre, l'utilizzo dei pagamenti digitali può portare a un aumento dell'efficienza delle transazioni finanziarie, poiché le transazioni possono essere eseguite in tempo reale da qualsiasi luogo e non richiedono la presenza fisica di una persona.

Tuttavia, l'introduzione dei pagamenti digitali ha anche sollevato alcune preoccupazioni per la sicurezza dei dati personali e finanziari degli utenti, dal momento che i possessori di alcuni tipi di dati sono incredibilmente favoriti e si trovano in una posizione nettamente dominante rispetto agli altri.

2. I dati

Forse non tutti si sono soffermati almeno una volta a pensare intensamente ai dati di cui ogni giorno lasciamo traccia in rete, che vengono immediatamente salvati in appositi database, con fini più o meno nobili. E soprattutto al potere che si cela dietro al possesso di queste informazioni.

Se un tempo si poteva parlare di economia del petrolio, in cui i proprietari di giacimenti si posizionavano automaticamente sopra chiunque altro per potere e influenza, ora non è più esclusivamente così.

Infatti, il petrolio della nostra era, quella digitale, è rappresentato dai dati che ogni giorno le grandi aziende del mondo Tech collezionano da tutti gli utenti sparsi per il mondo, in base al loro utilizzo quotidiano.

Grazie a questi dati, aziende come Amazon sono in grado di stabilire con facilità se un prodotto crea interesse sul mercato, in quale segmento si posiziona più efficacemente, e addirittura in quale momento il potenziale cliente è più propenso all'acquisto.

Immaginiamo la raccolta di questi dati come un'immensa analisi di mercato, svolta in corso d'opera sui reali clienti, ottenendo uno storico globale sui comportamenti dei consumatori in ogni fase del processo di acquisto, che permette quindi all'azienda proprietaria di sfruttare queste importanti informazioni per poter soddisfare al meglio i bisogni dei consumatori e abbattere quindi i rischi e le incertezze legati al commercio di nuovi prodotti.

Ora moltiplichiamo questo effetto innumerevoli volte, per innumerevoli tratti comportamentali che possono essere analizzati e compresi dalle aziende attraverso i dati raccolti presso il pubblico, e otteniamo un mercato mai visto prima, in cui chi detiene la nuova materia prima preziosa, i dati, è in una posizione nettamente dominante rispetto ai *competitors*.

Come Amazon, sono presenti altre famose aziende che ogni giorno raccolgono dati su scala globale in grado di controllare i comportamenti dei consumatori: Google, Meta,

Apple o Microsoft, per citarne alcune, che si posizionano tutte quante tra le Big Tech mondiale, grazie alla loro capacità di sfruttare tutte le informazioni che hanno a disposizione per ottenere utili da record.

I dati che lasciamo in rete, quindi, sono dotati di un valore immenso, in grado di renderci vulnerabili o addirittura indifesi davanti alle attente strategie dei colossi mondiali che ne fanno uso.

Non bisogna prendere alla leggera questo concetto, perché essenzialmente è come se ogni giorno lasciassimo informazioni private, intime e potenzialmente in grado di condizionare le nostre decisioni nelle mani di entità che non le terranno al sicuro, ma anzi le sfrutteranno proprio per raggiungere i propri obiettivi finanziari, posizionando chi non detiene questi dati in una posizione di netto svantaggio.

Le aziende che raccolgono i dati dai propri clienti e dai propri prodotti lo fanno tramite diversi canali come ad esempio i loro siti web, le applicazioni, i sondaggi o le interazioni dirette con i clienti.

Questi dati, che possono includere informazioni personali come nome, cognome, indirizzo e-mail, indirizzo di residenza e persino dati sensibili come informazioni finanziarie o di salute, devono essere organizzati in modo da essere facilmente recuperabili, gestibili e aggiornati.

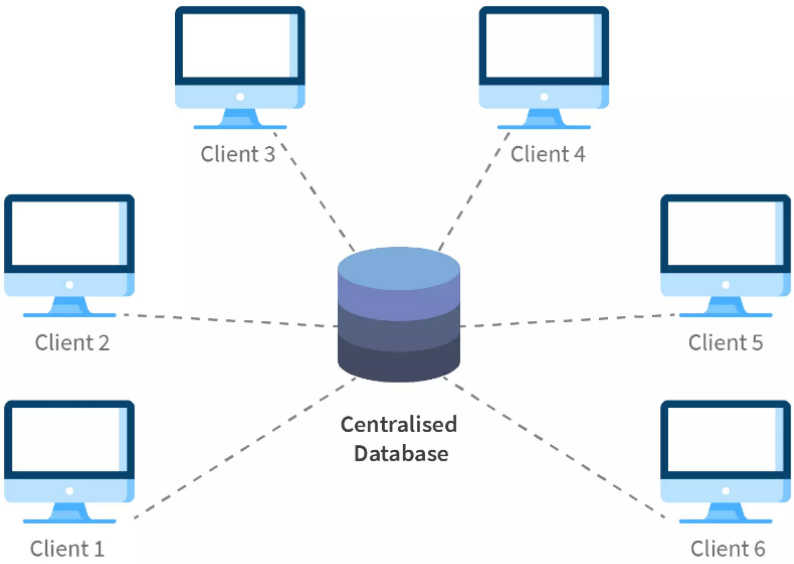
Per fare questo, le aziende utilizzano un sistema di gestione di database, ovvero una collezione dei dati strutturati in modo da poter essere facilmente manipolati.

Il tipo di database può variare in base alle necessità e soprattutto alla grandezza dell'azienda, tra i più importanti, tuttavia, figurano il Database centralizzato, il Database distribuito e il Cloud, oltre alle moderne tecnologie DLT tra cui vi è anche la Blockchain.

2.1 Il database centralizzato

Il database centralizzato è un tipo di database che utilizza un server centrale per archiviare, gestire e fornire accesso ai dati. In questo modello, tutti i dati vengono archiviati su un unico server e gli utenti accedono ai dati tramite applicazioni client.

Figura 1 - Il database centralizzato



Fonte: *https://www.scaler.com/topics/dbms/types-of-database/*

Questo modello di database offre diversi vantaggi, tra cui la semplicità di gestione e la maggiore sicurezza dei dati. In particolare, un sistema centralizzato semplifica notevolmente la gestione dei dati, poiché tutti i dati vengono gestiti in un unico luogo.

Inoltre, poiché tutti i dati sono archiviati in un unico server centrale, il controllo degli accessi e la sicurezza dei dati possono essere più facili da gestire.

Tuttavia, il database centralizzato presenta anche alcune limitazioni. In primo luogo, l'accesso ai dati è limitato all'applicazione client associata, il che significa che i dati possono essere accessibili solo a un gruppo limitato di utenti o applicazioni.

In secondo luogo, il server centrale rappresenta un singolo punto di fallimento, quindi se il server non è disponibile, tutti gli utenti non possono accedere ai dati. Questo può rappresentare un grande problema per le applicazioni in cui l'accesso ai dati è fondamentale e non può essere interrotto. Questa forte centralità enfatizza un altro problema, quello della disponibilità intesa come potere di disporre dei dati a proprio piacimento, e quindi di eliminarli, modificarli o "inventarli", che è reso possibile al proprietario degli stessi.

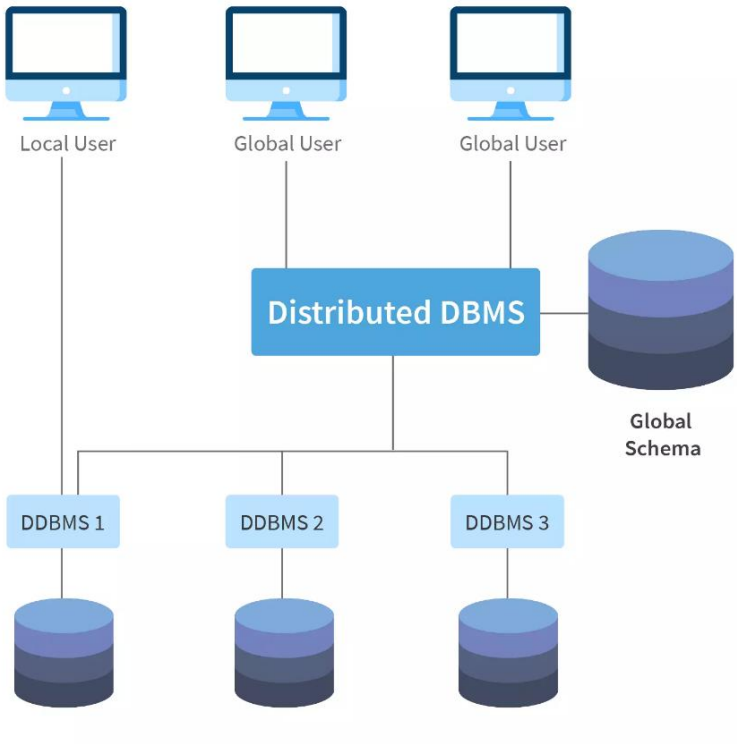
Questo tipo di database si espone anche ad una forte vulnerabilità alla frode e alla manipolazione di dati essendo il server centrale un punto critico di attacco per eventuali *hacker*, che in caso di violazione possono compromettere, divulgare, o manipolare i dati contenuti al suo interno.
Infine, il database centralizzato può rappresentare un problema in termini di scalabilità. Poiché tutti i dati sono archiviati su un unico server, può diventare difficile gestire grandi quantità di dati o un grande numero di utenti che accedono simultaneamente ai dati. In questo caso, può essere necessario aggiungere ulteriori server per gestire la crescita del database e l'aumento del traffico di dati.

In generale, il database centralizzato è una scelta appropriata per le applicazioni in cui la gestione dei dati è relativamente semplice e la sicurezza è una priorità. Tuttavia, per le applicazioni che richiedono la gestione di grandi quantità di dati o la scalabilità, potrebbe essere necessario considerare altre opzioni di database, come il database distribuito.

2.2 Il database distribuito

Il database distribuito rappresenta una soluzione innovativa che affronta le sfide sempre crescenti che le aziende devono affrontare nella gestione di grandi quantità di dati. Questo tipo di database presenta una struttura più decentralizzata rispetto al precedente, in cui i dati sono memorizzati su diversi computer (o nodi) all'interno di una stessa rete, invece di essere salvati su un singolo server centrale.

Figura 2 - Il database distribuito



Fonte: *https://www.scaler.com/topics/dbms/types-of-database/*

Questa struttura consente ai diversi nodi all'interno della rete di collaborare tra di loro per gestire e condividere i dati, rendendoli disponibili per essere utilizzati da applicazioni e utenti diversi nella rete. Questo è particolarmente utile per le aziende che operano su scala globale e hanno la necessità di accedere rapidamente ai dati ovunque essi si trovino.

Rispetto al database centralizzato, il database distribuito presenta maggiori livelli di sicurezza, poiché eventuali dati persi da un nodo compromesso o fallito possono essere recuperati attraverso gli altri nodi che costituiscono la rete. Ciò significa che il rischio di perdita di dati è notevolmente ridotto, migliorando la sicurezza complessiva del sistema.

La scalabilità è un'altra caratteristica distintiva del database distribuito. I dati e gli utenti possono essere facilmente distribuiti sui diversi nodi che possono essere modificati e incrementati in base alla forza lavoro necessaria per sostenere il carico di lavoro. Ciò consente un aumento della velocità con cui vengono processate, memorizzate e condivise tutte le informazioni, migliorando notevolmente l'efficienza del sistema.

Nonostante i grandi passi avanti fatti in termini di efficienza e sicurezza rispetto al primo tipo di database che abbiamo visto, rimane un problema non trascurabile, ossia permane l'esistenza di un possessore di dati unico, o al limite di un "oligarchia dei dati" che rende ancora possibile la figura del servo-padrone in funzione del loro dominio.

In sintesi, il database distribuito rappresenta una soluzione flessibile e altamente scalabile per le aziende che vogliono gestire grandi quantità di dati in modo efficiente e sicuro. La sua struttura decentralizzata, la maggiore sicurezza e la scalabilità consentono alle aziende di ottenere un vantaggio competitivo, migliorando l'efficienza operativa e la velocità delle operazioni complessive. Ma sempre rinunciando alla parità in forza del possesso di dati da parte dei pochi, che non viene meno rispetto al database centralizzato

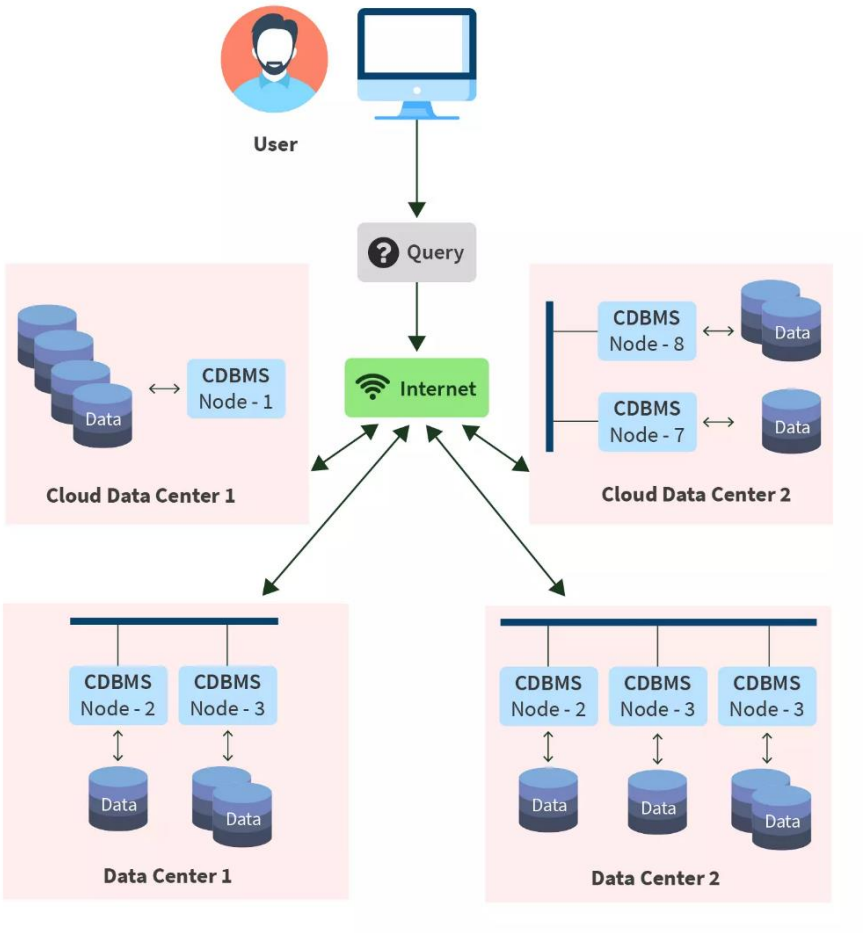
2.3 Il Cloud

Un database cloud raccoglie, gestisce e organizza i dati in un sistema IT, che risiede su una piattaforma di cloud computing pubblica, privata o ibrida.

Dal punto di vista del modello generale e delle funzionalità, un database cloud non è poi tanto diverso da un database locale che viene eseguito sui sistemi del data center di un'organizzazione.
La differenza maggiore risiede nel modo in cui il database viene distribuito e gestito.

Ad esempio, lo stesso database appare identico agli utenti finali e alle applicazioni, sia che si trovi in locale che nel cloud.A seconda del software di database utilizzato, i database cloud possono memorizzare dati strutturati, non strutturati o semi strutturati, proprio come le loro controparti locali.

Figura 3 - Il cloud



Fonte: *https://www.scaler.com/topics/dbms/types-of-database/*

Sul piano personale l'utilizzo di un database nel cloud cambia drasticamente le responsabilità dei team IT e di gestione dei dati. I fornitori di cloud installano e gestiscono l'infrastruttura di sistema sottostante e, in alcuni casi anche la piattaforma di database.

Questo riduce il lavoro tradizionalmente svolto dagli addetti alle operazioni IT e dagli amministratori di database (DBA), permettendogli quindi di occuparsi di altri compiti, come l'ottimizzazione dei database per le applicazioni e il monitoraggio dell'utilizzo e dei costi dei sistemi di database cloud.

Come in molti altri contesti, la tendenza è quella di abbracciare il progresso tecnologico, e già in molti stanno implementando DBMS di questo tipo.

Le organizzazioni che implementano i database nel cloud pubblico possono scegliere tra due principali modelli di implementazione:

- modello tradizionale, molto simile ad un database locale proprietario, per cui l'organizzazione paga un fornitore di servizi cloud terzo e sviluppa su di esso il suo database;
- approccio DBaaS, ossia Database as a service. Si tratta di un servizio offerto simile al precedente ma in questo caso il fornitore del cloud, che lo "affitta", si occupa anche di tutte le fasi di manutenzione, aggiornamento e pulizia che necessita, in cambio ovviamente di una commissione.

2.4 Le Tecnologie DLT

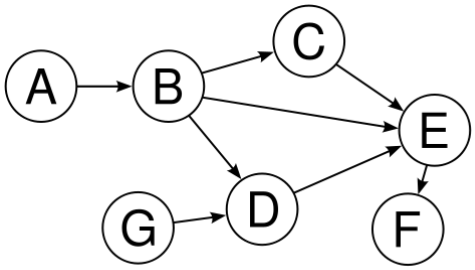
Le tecnologie Distributed Ledger sono una famiglia di tecnologie che si basa su un registro distribuito di informazioni, condiviso e replicato da tutti i nodi della rete.

Questo registro, noto anche come Ledger, registra tutte le transazioni effettuate sulla rete e garantisce la sicurezza, la trasparenza e l'immancabilità delle informazioni registrate.

La tecnologia più famosa basata su un registro distribuito è la blockchain, che vedremo tra poco, su cui già sono in movimento diversi protocolli più o meno efficienti.

Oltre alla blockchain, ci sono anche altre tecnologie a registro distribuito, come ad esempio la Directed Acyclic Graph (DAG), che si basa su un digrafo aciclico invece di un registro lineare come nel caso della blockchain.

Figura 4 - La forma in cui si dispongono i nodi in una tecnologia DAG



Fonte: https://commons.wikimedia.org/wiki/File:Directed_acyclic_graph.svg

Le tecnologie Distributed Ledger stanno cambiando radicalmente il modo in cui le organizzazioni gestiscono e condividono le informazioni. Ad esempio, nel settore finanziario diverse realtà stanno portando un modo tutto nuovo di gestire e archiviare le transazioni, garantendo maggiore sicurezza e soprattutto una trasparenza unica.

La vera forza di queste tecnologie sta infatti nell'omissione della figura del proprietario dei dati che su di essa vengono salvati, garantendo una parità non indifferente tra tutti gli utilizzatori, e rendendola estremamente più sicura e a prova di manipolazioni.

3. La Blockchain

3.1 Un po' di storia

L'idea alla base della tecnologia blockchain ha origine già nel 1991, quando i ricercatori Stuart Haber e W. Scott Stornetta introducono una soluzione più efficiente per la marcatura temporale dei documenti digitali, in modo da garantire con sicurezza l'impossibilità di manipolarne o alterarne le informazioni.

Nel 1992 vengono integrati nel sistema gli alberi di Merkle, che lo rendono ancora più efficiente consentendo di raccogliere più documenti in un unico blocco.

Nel 2004, l'esperto informatico Hal Finney (Harold Thomas Finney II) ha introdotto un protocollo considerabile il primo passo verso una valuta veramente digitale, ossia il Reusable Proof of Work.

Il concetto alla base del RPoW prevede un riutilizzo del lavoro computazionale impiegato da un hardware specifico per risolvere gli hash crittografati.

3.1.1 Bitcoin

Circa 4 anni dopo lo scadere del brevetto, nel 2008 è stato pubblicato su una mailing list di appassionati un white paper anonimo, che introduce un nuovo concetto di moneta P2P che nono vede il bisogno di un'autorità centrale, essendo decentralizzata. Questo modello prende il nome di Bitcoin, e il suo (o i suoi) sviluppatore ha mantenuto fino ad ora l'alias di Satoshi Nakamoto.

Il protocollo si basa sull'algoritmo di Proof of Work Hashcash, che a differenza della precedente RPoW omette la necessità di un hardware di riferimento, facendo gli stessi partecipanti da garanti per la sicurezza, impedendo la pratica del double spending o dell'indebitamento. In poche parole, chiunque ne sia in grado può eseguire la funzione di *miner*, verificando la transazione e ricevendo una commissione per il suo lavoro svolto.

3.1.2 Ethereum

Nel 2013, Vitalik Buterin, programmatore e co-fondatore di Bitcoin Magazine, dichiara che Bitcoin ha bisogno di un linguaggio di *scripting* per la creazione di applicazioni decentralizzate. Non riuscendo a convincere la comunità, inizia a sviluppare insieme ai successivi fondatori di Cardano e Polkadot, una nuova piattaforma informatica distribuita basata su una nuova blockchain, Ethereum, la quale introduce i c.d. "smart contracts", che svolgono la funzionalità di scripting.

3.1.3 Polkadot e la Parachain

Nella seconda metà del 2016 viene pubblicata la bozza del white paper di Polkadot da Gavin Wood, che dovrà però attendere un anno prima di effettuare la prima vendita dei token DOT. L'intento di Wood è di ampliare la compatibilità tra diverse blockchain autonome, utilizzando il sistema di Parachain (Parallelized Chain), ossia un sistema interconnesso, in cui i partecipanti possono mantenere la loro chain autonoma pur conversando attraverso il sistema della Parachain con tutti gli altri.

3.2 La Tecnologia

Partendo dalle caratteristiche di una Blockchain, essa intende soddisfare delle esigenze specifiche grazie alle sue peculiarità, ossia:

- sicurezza;
- trasparenza;
- disponibilità (o pubblicità);
- decentralizzazione.

Questa tecnologia è essenzialmente rappresentata da una rete di nodi che ci possiamo immaginare come molteplici database, i quali contengono al loro interno la storia della Blockchain sempre aggiornata e identica l'un l'altro, e sono distribuiti nel globo in modo tale da raggiungere la tanto decantata decentralizzazione nel senso più stretto e meno

fantasioso possibile (chiunque sia dotato di un hardware in grado di svolgere questo lavoro potrebbe istituire un nodo proprio).
Il registro condiviso delle transazioni, sempre disponibile on-line, prende il nome di *ledger*, ossia un libro mastro in cui, come detto, viene registrata dai nodi validatori ogni transazione effettuata, in modo permanente, all'interno di un blocco.

Il blocco possiamo immaginarlo come uno *storage* dotato di scadenza temporale in cui vengono contenute le transazioni validate in quella specifica era, che nel caso di Bitcoin è rappresentata da circa 10 minuti.

Al suo termine viene validato l'intero blocco e collegato al successivo, che conterrà l'*hash* dell'intero blocco al suo interno, incatenandoli l'un l'altro in serie e poi propagando il nuovo blocco a tutti i nodi che si sincronizzeranno con esso.

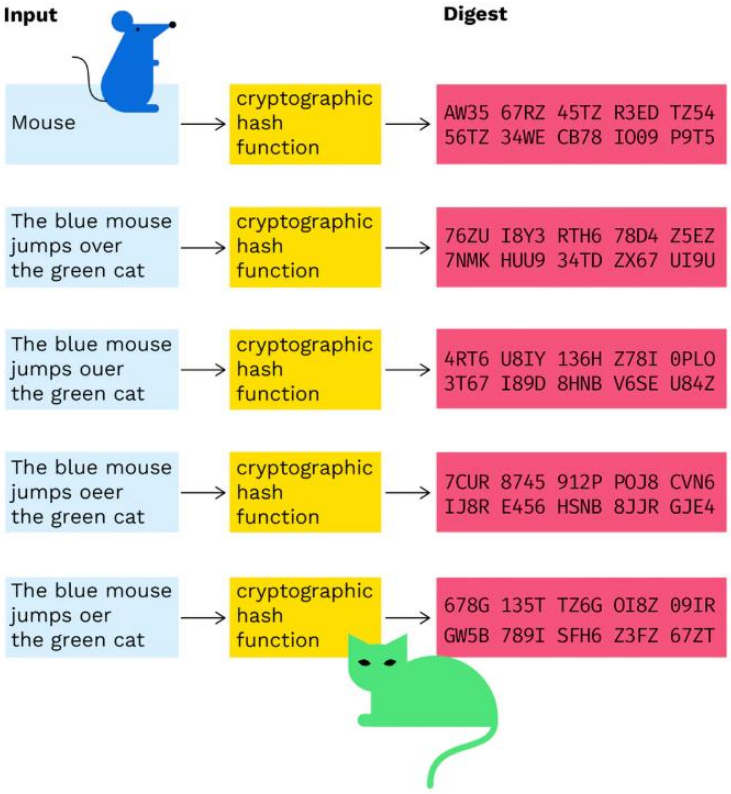
3.2.1 La funzione di Hash

Il legame tra un blocco e il successivo avviene attraverso una catena di *hash* crittografici, ossia algoritmi matematici che mappano dei dati in una stringa binaria di dimensione fissa (valore di *hash*), progettati per essere unidirezionali e quindi difficili da invertire, e caratterizzati da alcune proprietà fondamentali.

Tra le proprietà fondamentali della funzione crittografica di *hash* ci sono:

- identificazione univoca, che non permette a due messaggi differenti di avere lo stesso valore;
- natura deterministica, nel senso che lo stesso messaggio si tradurrà sempre nello stesso *hash*, e tale *hash* deve essere veloce e semplice da calcolare a partire da un qualsiasi tipo di dato;
- difficoltà, se non impossibilità, di generare un messaggio dal suo *hash*, a meno che non si provino tutti i messaggi possibili.

Figura 5 - Esempi di Hashing



Fonte: https://www.bitpanda.com/academy/en/lessons/what-is-a-hash-function-in-a-blockchain-transaction/

L'input di questa funzione può essere qualsiasi tipo di messaggio o di file, e l'output della funzione sarà una stringa binaria di lunghezza fissata, ad esempio 256 bit, che prende appunto il nome di "hash" o "digest".

L'output restituito è sempre lo stesso, per lo stesso input, ma basta cambiare l'input di un solo carattere e l'output restituito cambierà completamente.

Essendo crittografata, l'azione inversa, che parte dall'output e cerca di ricostruire l'input, è praticamente impossibile.

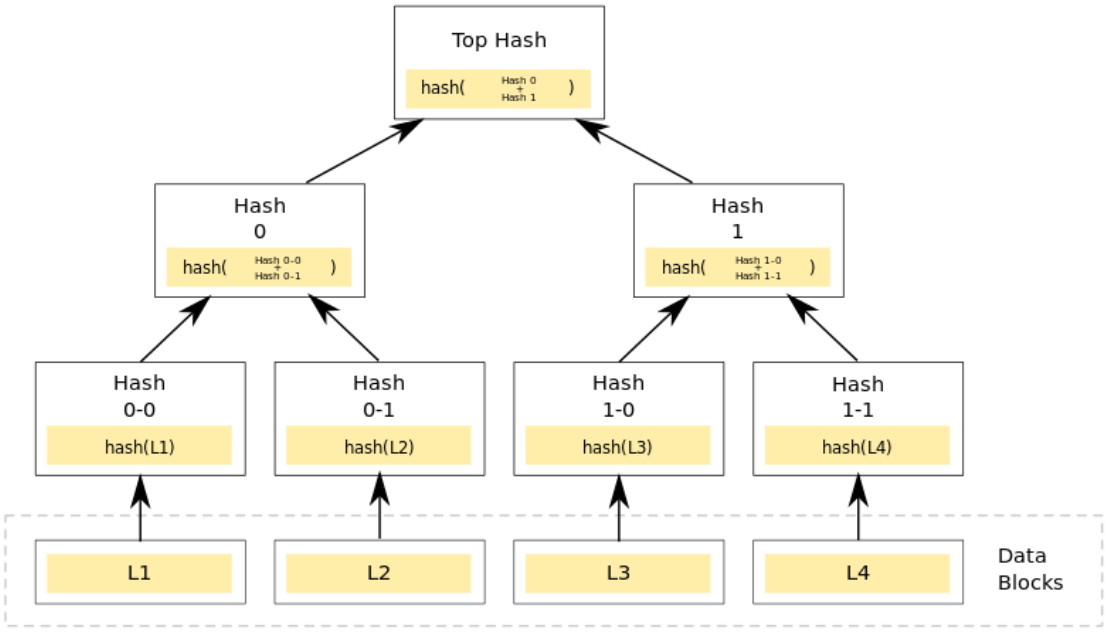
L'unico metodo plausibile è quello di tentare di indovinare in modo casuale tra 2^{256} possibili combinazioni nel caso preso.

3.2.2 Gli alberi di Merkle

Anche chiamato albero di Hash, La struttura ad albero, che prende il nome dal crittografo statunitense Ralph Merkle, porta con sé enormi potenzialità e vantaggi che permettono un miglioramento non indifferente dell'efficienza della blockchain.

Essenzialmente l'albero è rappresentato dai nodi iniziali (foglie) che devono essere identificati con un identificatore univoco come l'hash, i quali si collegano ai nodi superiori (rami), detti anche nodi padre, che presentano un identificatore univoco risultante dall'hash dei suoi nodi figli.
La concatenazione prosegue fino al nodo radice, la cui impronta è presente in tutti i nodi dell'albero.

Figura 6 - Il Merkle Tree



Fonte: https://en.wikipedia.org/wiki/Merkle_tree#/media/File:Hash_Tree.svg

Immaginiamo quindi un blocco di dati che apponga un'impronta (hash) unica e irripetibile. Ogni blocco di dati è organizzato nell'insieme a formare una sorta di piramide, e sono collegati l'un l'altro attraverso catene di *hash*.

Così facendo i blocchi superiori e i blocchi inferiori sono collegati, mantenendo invariata la struttura man mano che si scala e si aggiungono nuovi blocchi.

L'invariabilità si raggiunge grazie al fatto che, se venisse modificato l'*hash* di un blocco, si invaliderebbero gli *hash* di tutti gli altri blocchi (poiché contenevano le informazioni del blocco ormai invalidato).

Questo meccanismo ha permesso la risoluzione del grande problema rappresentato dalla possibilità di manomettere i dati, oltre a migliorare l'efficienza in quanto semplifica la verifica dei blocchi di dati.

3.2.3 Gli Smart Contracts

Gli *smart contracts* non sono altro che protocolli informatici in grado di facilitare e rendere più scorrevole l'operazione e l'esecuzione di un contratto su blockchain.
Rappresentano l'elemento chiave del rapporto tra contraenti, quell'elemento in grado di far venire meno la fiducia tra le parti, che nel sistema tradizionale è rappresentato dagli enti intermediari.
Non sono tanto diversi dai contratti legalmente validi che conosciamo, in quanto la funzione che svolgono è essenzialmente la stessa, con l'aggiunta del fatto che essendo sviluppati su blockchain, ed essendo quindi regolati da un codice crittografico di tipo "if/then", non permettono a nessuna delle parti di violare i termini pattuiti nel rapporto.

3.3 Da cosa è rappresentata la vita di una transazione?

Per mostrare con chiarezza in che modo l'insieme di tecnologie mostrato finora interagisce e si applica, prenderò l'esempio di una transazione sulla blockchain di Bitcoin. Una transazione su Bitcoin rappresenta il trasferimento di una certa quantità di valuta (BTC), da un indirizzo Bitcoin ad un altro.

Tutto ha inizio con il desiderio di un soggetto (Che chiameremo A), di inviare una somma di denaro ad un altro soggetto (B).

Per fare ciò A genera una nuova transazione, attraverso l'inserimento di un messaggio di transazione con i necessari input e output.

3.3.1 Gli Input

Nello specifico gli input sono rappresentati dall'indirizzo di A e dal suo valore di transazioni ricevute e non spese (Unspent Transaction Output o UTXO).
La funzione del UTXO consiste in una sorta di bilancio proprio di chi intende effettuare la transazione in grado di garantire che esso detenga la proprietà della somma che intende inviare, oltre ad un'autenticità dell'input stesso.
Tra gli altri dati vengono inserite le *fees*, ossia le commissioni da pagare ai *miners* per il lavoro svolto al fine di processare le transazioni, che possono essere aumentate per dare maggiore priorità, e quindi impiegare maggiore potenza di calcolo per la verifica della propria transazione.

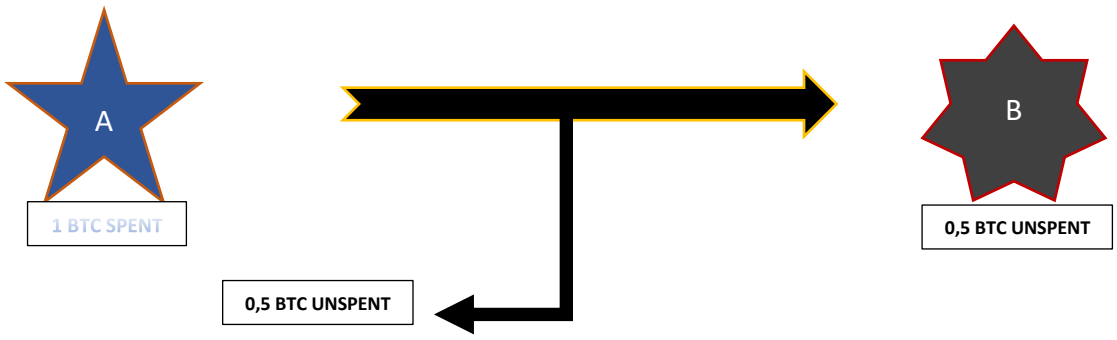
3.3.2 Gli Output

La restante parte del messaggio di transazione è rappresentata dagli *output*, i quali contengono in primo luogo l'indirizzo di B, ossia il *wallet* in favore del quale sono indirizzati i fondi.

In secondo luogo, viene specificata ovviamente la somma di denaro che A intende inviare. Infine viene specificato il *change*, ossia l'eccedenza dell'input rimandata al mittente, nel caso esso non spenda tutto ciò che detiene.

Volendo spiegare meglio il *change* bisogna immaginare che A detenga in portafoglio 1 BTC e intende inviarne la metà (0,5 BTC) al nostro destinatario B.
In questo caso la transazione avrà come somma "spent" l'intero Bitcoin, ma proprio come funziona con il resto ad esempio quando paghiamo il caffè con una banconota, attraverso la funzione di *change*, l'ammontare speso durante il suo viaggio incontrerà un bivio, al quale 0,5 BTC verranno effettivamente inviati a B, mentre la restante parte ritornerà all'indirizzo da cui è stata inviata la transazione, cioè quello di A.

Figura 7 - Il meccanismo del *change*



Fonte: Elaborazione propria

Questo processo addizionale non è affatto inutile, anzi serve per automatizzare il controllo sulla disponibilità degli utilizzatori, massimizzare la sicurezza e mantenere la coerenza con la blockchain.
Infatti l'ammontare che torna al mittente tornerà sotto forma di Unspent, e sarà quindi utilizzabile in seguito rientrando nell'UTXO (Unspent Transaction Output) che si era visto in precedenza.

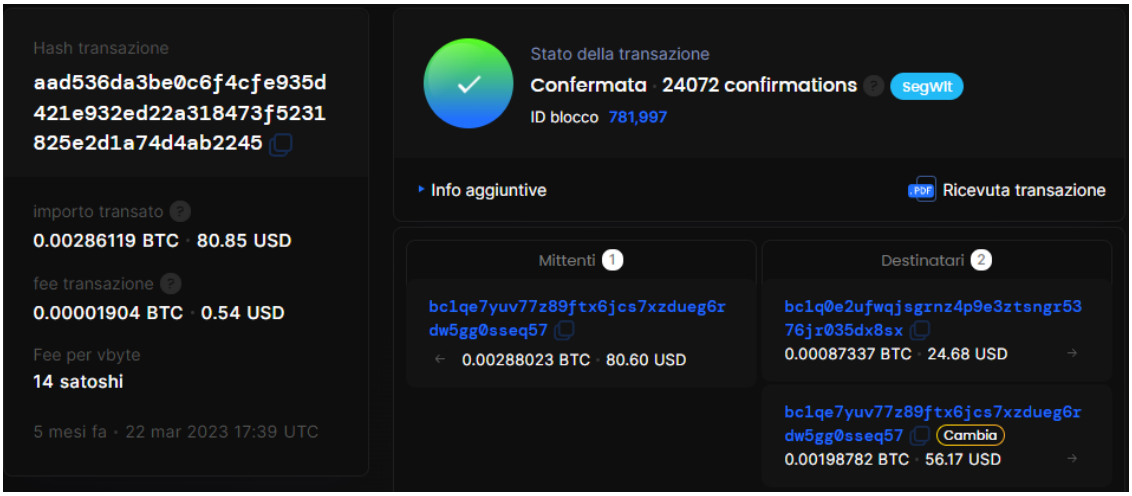
3.3.3 La firma

Dopo aver inserito Input e Output, A ha ultimato il suo messaggio di transazione. L'inserimento di Input e Output ovviamente non risulta essere complesso come abbiamo appena visto, grazie a molteplici applicazioni *user friendly* che richiedono semplicemente l'indirizzo del destinatario e la somma da inviare, automatizzando tutto il resto.

Arrivati a questo punto non gli resta che firmare la transazione con la sua chiave privata, che è univoca e garantisce che la transazione sia stata inviata da A.

Una volta firmata la transazione, viene generato l'hash corrispondente e inviato sulla BlockChain, dove il lavoro passa in mano ai nodi validatori, che dovranno confermare la transazione.

Figura 8 - Un esempio di transazione presa dall'explorer Blockchain



Fonte:https://blockchair.com/it/bitcoin/transaction/aad536da3be0c6f4cfe935d421e932ed22a318473f5231825e2d1a74d4ab2245

In questo caso specifico, preso casualmente, vediamo che A invia il corrispettivo di 80,60 USD (al momento della transazione). Di questi, solamente 24,68 USD finirà nelle mani di B, il resto infatti, come si può notare dalla specificazione "cambia", tornerà al mittente sotto forma di UTXO.

Se vediamo lo stato della transazione, notiamo che in quel momento aveva ottenuto solo 1 delle 6 conferme (minime) necessarie perché la transazione potesse diventare valida sulla BlockChain a tutti gli effetti.

3.4 Meccanismi di consenso

Facendo un richiamo al problema dei generali bizantini, analizzeremo in che modo questa tecnologia intende risolvere la questione del consenso.
Il famoso problema informatico ipotizza una situazione in cui tre o più generali bizantini devono decidere se attaccare o ritirarsi in seguito a un ordine di un comandante superiore. Uno o più generali potrebbero essere traditori, con l'intenzione di confondere gli altri;
si potrebbe quindi verificare il caso in cui uno dei generali comunichi ai suoi colleghi un ordine diverso da quello impartito dal comandante.

La soluzione al problema permette ai generali leali di evitare queste trappole.

Il parallelo della storia è quello dei nodi di un sistema distribuito, che. Vanno messi in contatto per ottenere un accordo su un'unica versione della blockchain, evitando così il fallimento della stessa.

Innanzitutto, un metodo di consenso è un algoritmo che viene utilizzato per raggiungere un accordo sulla validità delle transazioni e dei blocchi, progettato in modo tale da garantire l'accuratezza e la non manipolabilità dei dati conservati nella blockchain.

I principali metodi di consenso utilizzati, che vedremo in maniera più approfondita sono il Proof of Work e il Proof of Stake.
Esistono comunque altri metodi ampiamente validi, anche se meno utilizzati, tra cui il Proof of Authority, il Proof of History e il Proof of Capacity.

3.4.1 Proof of Work

La Proof of Work è il meccanismo alla base di Bitcoin ed è il meccanismo di consenso più dispendioso, in quanto la prova è effettivamente data da lavoro e quindi dalla fatica impiegata nella verifica.

La Proof of Work richiede che un *miner* risolva un problema matematico per poter aggiungere un blocco alla blockchain

Il problema matematico richiede la ricerca di un *hash* che soddisfi determinati requisiti, ovvero deve essere inferiore a un determinato valore.

La difficoltà del problema come sappiamo viene regolata in base alla potenza di calcolo della rete, in modo da mantenere il tempo tra la creazione di un blocco e l'altro costante, e il *miner* che risolve il problema per primo viene premiato con una quantità di BTC. In questo modo si offre un incentivo ai *miner* affinchè continuino a dedicare le loro risorse alla risoluzione dei problemi e quindi alla protezione della rete.

Per esplodere più nel dettaglio il problema matematico che i *miner* devono risolvere, l'output che a loro arriva, ossia l'hash, è dotato di un parametro fondamentale, la difficoltà.

Questa è collegata al numero di zeri iniziali nella stringa ottenuta, infatti essendo il lavoro di un *miner* trovare tra un'infinità di numeri, un numero inferiore a quello dell'hash per poi verificarlo, al variare degli zeri iniziali dell'hash varia anche la difficoltà, in modo lineare.

Una volta che il *miner* individua, in questa infinita ampolla, un numero inferiore all'*hash* che aveva ricevuto, deve procedere con la verifica.

Deve estrapolare il Nonce dall'hash, ossia la parte variabile che viene dopo gli 0 iniziali, che se dovesse coincidere con l'input della stringa che aveva ricevuto, può facilmente verificarlo essendo l'output sempre uguale per lo stesso input.

Se il Nonce è verificato, viene validato il blocco, altrimenti la richiesta è invalidata.

Tutto ciò al fine di renderlo effettivamente un lavoro di fatica in senso di impiego di TH/s (Thera Hash per secondo)

Volendo rendere l'idea in senso metaforico, la Proof of Work funziona come un enorme puzzle che deve essere risolto da tutti i *miner* che intendono farlo per poter aggiungere un pezzo alla volta.

La difficoltà del puzzle viene regolata in modo da mantenere costante il tempo con cui vengono aggiunti i pezzi al puzzle, nel caso di Bitcoin viene automaticamente reimpostato dal codice il parametro difficoltà.

Questo sistema è stato ideato per proteggere la rete e motivare i *miner* a dedicare le loro essenziali risorse alla risoluzione dei problemi.

Senza queste risorse infatti, l'intero sistema verrebbe messo in pericolo e sarebbe esposto agli attacchi malevoli.

3.4.2 51% Attack

Se un nodo malevolo, il generale bizantino traditore, volesse prendere il controllo della blockchain, gli basterebbe ottenere il 51% dell'Hash Rate totale impiegato, per diventare statisticamente il proprietario della *chain*.

Volendo capire se sia fattibile o meno ottenere il controllo di un sistema come Bitcoin, bisognerebbe ottenere una potenza di più di circa 220 mln TH/S, che al prezzo di circa 45/50 USD per TH/s, equivarrebbero a 9.945.000.000 USD, ossia circa 10 miliardi di dollari statunitensi al secondo.

Costo che tende ovviamente a variare, al variare dell'HR totale, facendo sì che in un sistema grande e concentrato, effettuare un attacco del genere diventa quasi impossibile a meno che non si disponga di infinite risorse.

Risorse che rappresentano una notevole quantità di energia elettrica e quindi di coinvolgimento economico e di inquinamento, tanto che ha fatto recentemente muovere numerose critiche anche per la crescente spinta verso un'economia più green, dando peraltro la possibilità ad altri metodi di consenso di acquisire maggiore importanza e appoggio presso il pubblico, primo tra tutti quello della Proof of Stake.

3.4.3 Proof of Stake

Questa richiede ai partecipanti della blockchain di "bloccare" una certa quantità di moneta, o più precisamente criptovaluta, a garanzia della convalida delle transazioni. La quantità di moneta bloccata determina il potere di voto del partecipante, rendendolo a tutti gli effetti un nodo validatore, in grado fra le altre cose di ricevere le commissioni pagate da chi intende effettuare transazioni su tale blockchain.

Un sistema del genere è inevitabilmente meno inquinante e dispendioso, ma porta con sé anche effetti negativi, ad esempio una resistenza minorata al famoso 51% Attack data dalla minore decentralizzazione, per cui un malintenzionato potrebbe acquisire la maggioranza del potere di voto dell'intera rete e comprometterne il funzionamento, ad un prezzo più vantaggioso rispetto ad acquisire la maggioranza in un sistema di PoW.
Proprio per rimediare a questo deficit, per aumentare l'efficienza e la sicurezza delle *chain*, sono comuni appositi Pool di Staking, a cui i piccoli staker decidono se aderire o meno, depositando collettivamente i fondi in modo da bloccarli. Il creatore del pool non ha incentivi a comportarsi in modo dannoso, i quanto i piccoli *staker* possono decidere di andare a conferire il loro potere di voto altrove

La scelta del metodo di consenso dipende meramente dalle esigenze di chi intende dare vita alla Block Chain e della sua community di utilizzatori, ed è fondamentale in termini di sicurezza e di dispendio energetico, infatti tutti i metodi esistenti, come del resto in altri ambiti, hanno i propri vantaggi e svantaggi rispetto alle alternative.

3.5 I limiti della Blockchain

Questa tecnologia, come abbiamo visto, è in grado di ottenere grandissimi risultati in molteplici casi di applicazione, e addirittura ha la potenzialità di stravolgere interi settori, ma ha ovviamente anche degli svantaggi intrinsechi nella sua natura.
Come qualsiasi tecnologia, all'inizio non tutto performa come dovrebbe e ci sono dei limiti fisiologici che con il tempo vengono superati grazie a diverse implementazioni.
Per la valutazione di una Blockchain si tengono in considerazione diversi parametri, al di sotto dei quali la stessa non è pienamente efficiente, e quindi questi parametri consistono in limiti della Blockchain stessa. I parametri/limiti si identificano in:

- scalabilità;
- costi;
- *privacy*;
- interoperabilità.

3.6 Scalabilità della Blockchain

Il primo punto chiave su cui soffermarsi quando si valuta una tecnologia di questo tipo è quello della sua scalabilità.
Partiamo innanzitutto con la definizione di scalabilità, che in informatica rappresenta la capacità di un software (o hardware) di adattarsi a un aumento di domanda o del carico di lavoro.

Di scalabilità ne esistono essenzialmente due tipi:

- la scalabilità (*scale-up*) che aumenta la capacità dell'hardware o del software aggiungendo risorse a un sistema fisico, ad esempio aggiungendo potenza di elaborazione a un server per renderlo più veloce. Per l'archiviazione scalabile, ciò significa aggiungere più dispositivi, come le unità disco, a un sistema esistente quando è necessaria più capacità;

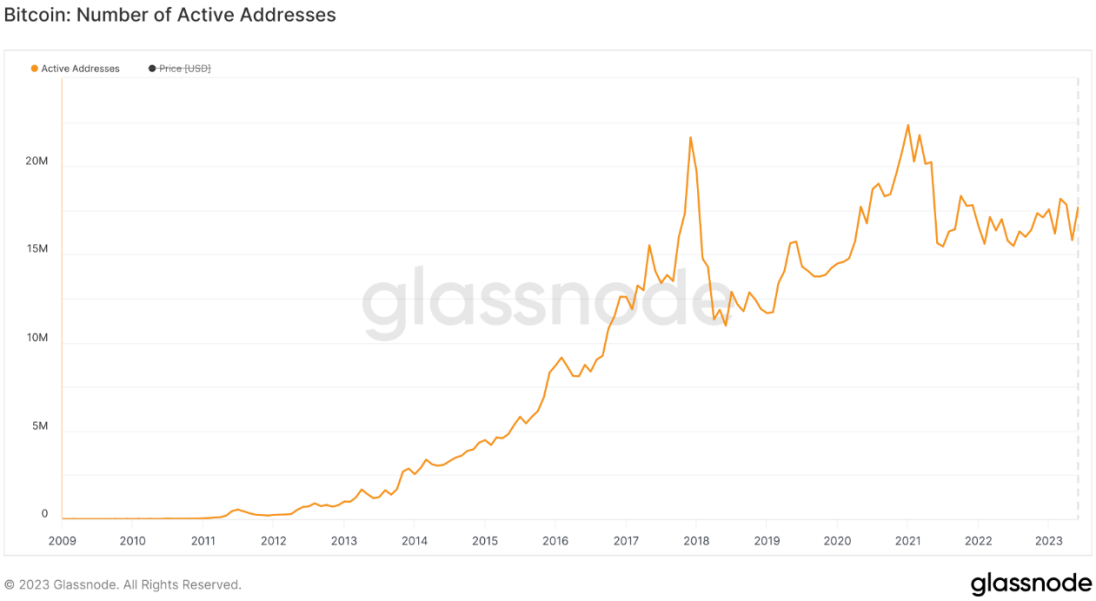
- la scalabilità orizzontale (*scale-out*) che collega più elementi per lavorare come un'unità logica. Per l'archiviazione con scalabilità orizzontale, ciò significa aggiungere dispositivi in array o cluster connessi. Ogni cluster può avere molti nodi (dispositivi) e i nodi possono essere separati geograficamente. Grazie a un'architettura scale-out, l'investimento iniziale in storage è ridotto perché è possibile aggiungere storage futuro in base alle esigenze.

Nel caso della Blockchain notiamo che la scalabilità, soprattutto quella orizzontale, gioca un ruolo cruciale ai fini dell'effettivo buon funzionamento e della velocità di esecuzione delle azioni nonostante la crescente quantità di dati da elaborare o di traffico generale sulla rete.

È però proprio in essa che risiede uno dei principali limiti di alcune blockchain; infatti, se si prende in considerazione la rete di Bitcoin, il suo codice è rimasto invariato dalla data della creazione, portandosi dietro inevitabili limiti legati a tale periodo in

contrapposizione con lo sviluppo odierno, sebbene comunque molti sviluppatori abbiano apportato alcuni miglioramenti alla sua blockchain.

Figura 9 - Il grafico degli Indirizzi Attivi su BTC preso da Glassnode



Fonte:https://studio.glassnode.com/metrics?a=BTC&m=addresses.ActiveCount&mScl=lin&pScl=log&resolution=1 month

Il problema sorge dal momento che l'ecosistema attuale si trova in una situazione molto più avanzata rispetto alla sua nascita, arrivando a contare più di 10 milioni di utenti giornalieri, che portano inevitabilmente un enorme volume di scambi in grado di affaticare non poco il network nei momenti di traffico intenso.

3.6.1 Le Transazioni per secondo

L'adozione fa fisiologicamente crescere il numero di transazioni quotidiane giorno per giorno, affaticando sempre di più la rete di Bitcoin che, al suo stato attuale, non è in grado di processare una tale mole di transazioni ad una velocità adeguata, arrivando soltanto a picchi di n.7 transazioni per secondo.

Figura 10 - TPS da Set ’22 a Ago ’23

Fonte: https://bitcoinvisuals.com/chain-tx-second

Per rendere un’idea di quanto questa metrica non sia trascurabile ma anzi fondamentale, il sistema di pagamenti più famoso ed impiegato al mondo, VISA, raramente eccede le 2.000 TPS, sebbene l’azienda dichiari di essere in grado di processare fino a più di 65.000 transazioni per secondo, un numero immenso rispetto alle sole 7 TPS massime di Bitcoin.

Proprio per questo motivo sono state più recentemente create altre soluzioni indipendenti da Bitcoin, che puntano molto di più su un elevata scalabilità delle transazioni, arrivando a numeri quasi folli, come nel caso di Solana, per citarne uno, che ha già dimostrato in fase di test di raggiungere le 65.000 TPS ma punta a raggiungere il limite massimo di 710.000 TPS con sviluppi e aggiornamenti futuri.
Numeri che diventano veramente importanti, rendendo molto più che attuabile l’idea di una piena adozione di un sistema basato su Block Chain.

È quindi scansato in linea teorica il problema della scalabilità della blockchain, poiché esso non risiede nella tecnologia in sé, ma più nel modo in cui essa viene sviluppata, e vista la velocità del progresso tecnologico non è impensabile arrivare a protocolli in grado di gestire numeri di transazioni per secondo vicine al milione.

3.6.2 L'attenzione

Per quanto riguarda questo limite, ci riferiamo ad un limite causato più dal comportamento umano che dalla tecnologia, infatti è identificabile anche come un costo derivato dall'applicazione della Blockchain.
È bene ricordare che i meccanismi transattivi all'interno di un network di Blockchain richiedono che ciascun attore disponga non soltanto di un chiave pubblica visibile ad altri utenti, ma anche di una chiave privata destinata a rimanere riservata.
Nel caso in cui una private key dovesse andare perduta non vi sarà alcuna possibilità di recuperarla, così come non sarà più possibile accedere ai fondi gestiti da essa.
Per comprendere meglio, pensiamo ad un caso assurdo in cui perdiamo tutti i documenti di identità e non riusciamo più a provare agli altri di essere veramente noi stessi.
Questo è il costo/limite dell'attenzione, che quindi richiede indubbiamente una maggiore attenzione alla conservazione della proprietà delle proprie finanze, andando ad annullare la comodità di affidarsi ad un ente terzo che le detenga e gestisca per te, mantenendo però la reale proprietà di esse.

3.6.3 L'inquinamento

Un secondo limite ha a che fare con la situazione relativa all'inquinamento ambientale e il dispendio energetico necessari, affinché i nodi possano validare le transazioni.
Un tema molto caldo, che viene spesso esagerato per distogliere l'attenzione da dati ben più allarmanti riguardo ai consumi.

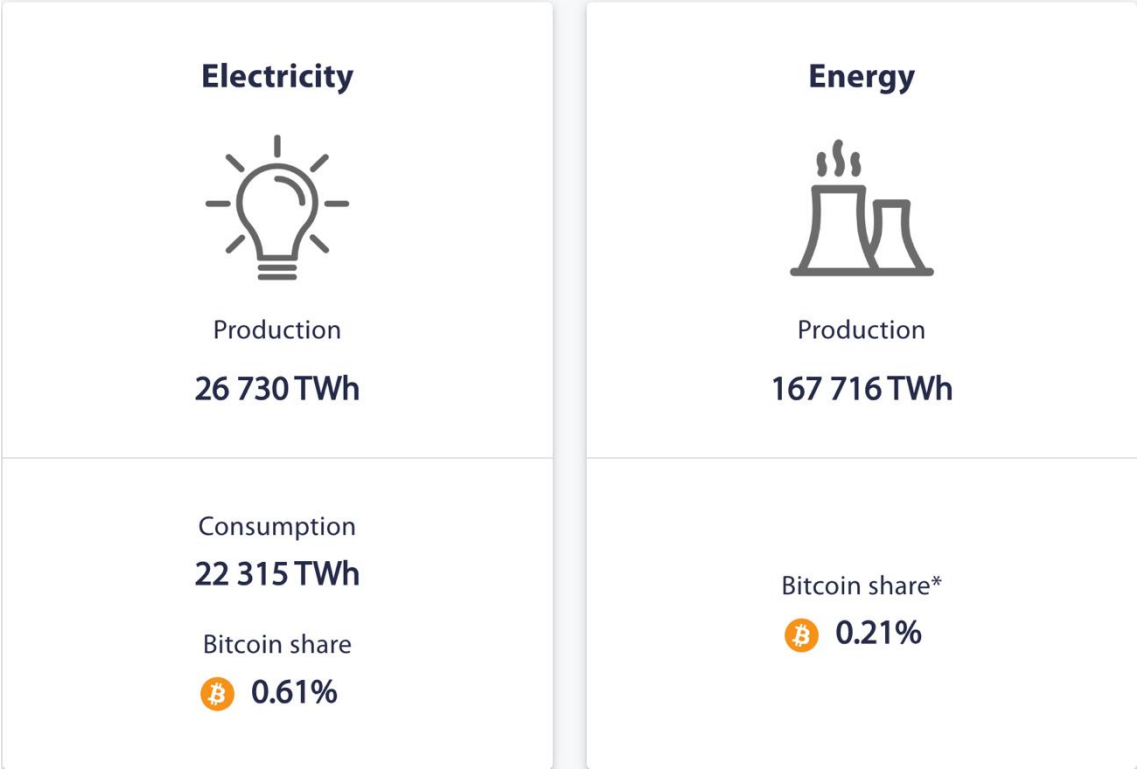
Infatti, sono stati svolti numerosi studi e paragoni sulle emissioni tanto acclamate del mining sulla rete di Bitcoin, la Blockchain più famosa e chiacchierata al mondo, e i risultati lasciano abbastanza perplessi.

L'università di Cambridge si è fatta pioniera di questo tema e ha creato il Cambridge Bitcoin Electricity Consumption Index (CBECI), ossia uno spazio interamente dedicato all'analisi e stime dei consumi di Bitcoin ed Ethereum, ricerche scientifiche e

aggiornamenti quotidiani, oltre ai paragoni con le emissioni di altre attività dispendiose, industriali e non.

Per prima cosa, vediamo in che misura l'attività su Bitcoin contribuisce al dispendio energetico e elettrico, rispetto al totale globale, notando che il peso è molto più trascurabile di quanto si possa pensare.
Successivamente si mettono a confronto attività come il mining di Bitcoin e di oro fisico, o i consumi di questo immenso network con i consumi domestici di ogni tipo, dimostrando il reale peso di questa demonizzata Proof of Work.

Figura 11 - Il paragone con il totale dei consumi di elettricità e energia



Fonte: *https://ccaf.io/cbnsi/cbeci/comparisons*

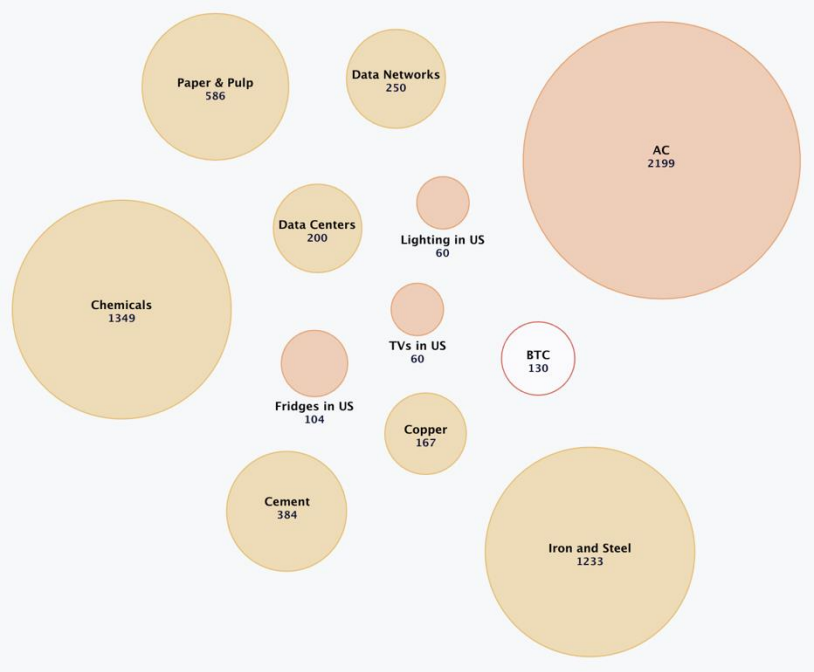
In questa prima parte del confronto i dati sono espressi in consumo energetico, e quindi in TWh.

Possiamo notare che su questi dati, al 2020, Bitcoin incideva all'incirca per meno dell'1% sul consumo dell'energia elettrica prodotta globalmente, e ancora meno per quanto riguarda l'energia utilizzata a livello industriale.

Infatti, anche in un confronto diretto con l'asset non digitale più simile a Bitcoin per caratteristiche fondamentali, l'oro, vediamo valori di consumo abbastanza in linea, che non rendono certamente giustizia alle critiche mosse contro il mining su block chain.

Se volessimo dare uno sguardo alle attività nel loro insieme, sarebbe ancor più evidente la contribuzione quasi irrisoria di Bitcoin al complesso dei consumi.

Figura 12: Grafico a bolle sui consumi annuali



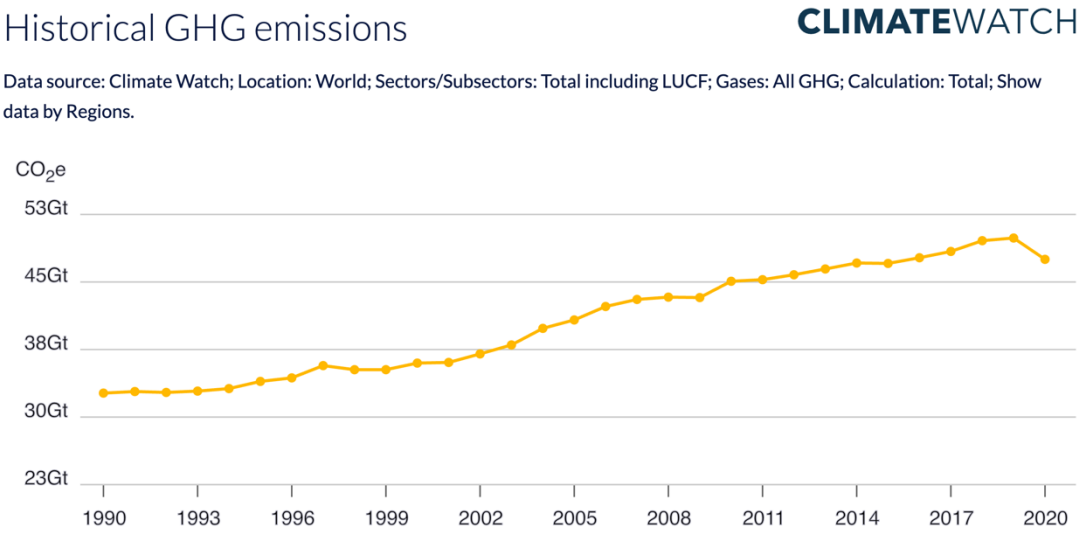
Fonte: https://ccaf.io/cbnsi/cbeci/comparisons

È sorprendente notare che il peso totale del consumo di questo tipo di *mining* è inferiore al consumo energetico congiunto di due semplici elettrodomestici presenti nelle case di tutti gli americani, la TV e il frigorifero.
Il dato che veramente fa preoccupare qui in questo grafico è quello sull'aria condizionata e il suo abuso, anche se non di certo quello che fa più scalpore.

Passando in secondo luogo ai dati sulle emissioni vere e proprie, è doveroso precisare che i dati sono presentati in $MtCO_2e$, ossia i Milioni di Tonnellate di CO_2 equivalente emessa, ovvero una misura che esprime l'impatto sul riscaldamento globale di una certa quantità di gas serra, rispetto alla stessa quantità di anidride carbonica (CO_2).

Il primo dato che salta all'occhio è quello della contribuzione del mining al totale delle emissioni globali nel 2019, che si è attestata a livelli record secondo Climate Watch Data:

Figura 13 - Grafico sulle emissioni globali da ClimateWatch

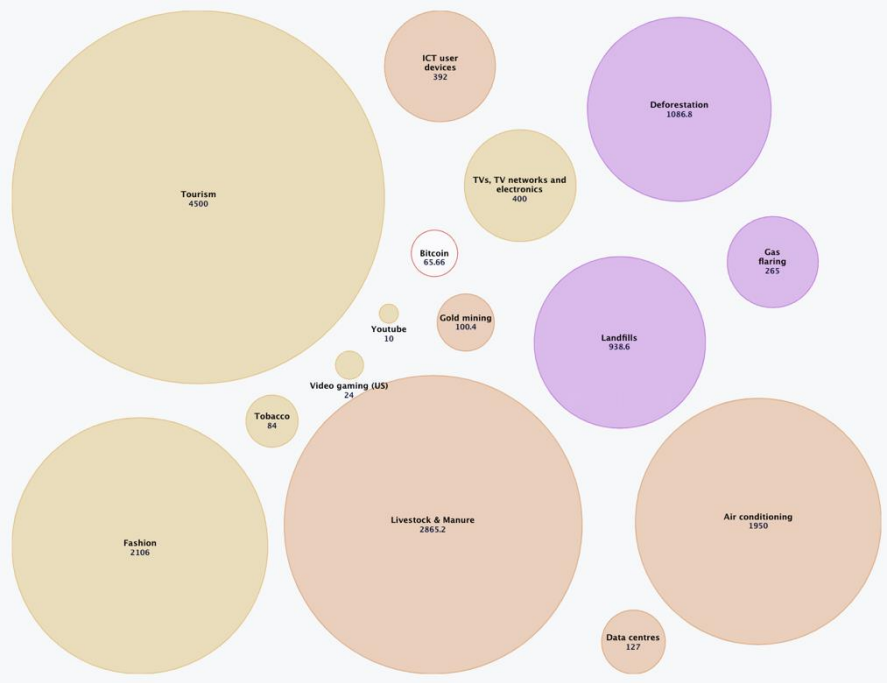


Fonte: https://www.climatewatchdata.org/ghg-emissions?breakBy=regions&end_year=2020&start_year=1990

Numeri come vediamo in costante crescita, da più di 20 anni, per motivi purtroppo naturali legati al processo di sviluppo del genere umano, che sempre di più stanno destando preoccupazioni e favorendo la ricerca di alternative altrettanto valide ma con un netto abbattimento dei danni apportati all'ecosistema.

Ebbene, la contribuzione totale di Bitcoin pesa circa lo 0,13% (65,66 $MtCO_2e$), un tasso di contribuzione tale da non giustificare l'allarmismo che si è venuto a creare attorno a questa attività.

Figura 14 – Grafico a bolle sulle emissioni annuali in MtCO2e



Fonte: https://ccaf.io/cbnsi/cbeci/ghg/comparisons

Ecco alcuni dei dati presentati in $MtCO_2e$, che fanno intendere meglio la grandezza dei danni ambientali apportati da alcune delle più ovvie attività che, solo perché considerate indispensabili, sono "giustificate" anche nei loro astronomici dati sull'impatto ambientale.

È interessante soffermarsi sul paragone con l'asset più vicino a Bitcoin come concetto, l'oro, che restando sul piano materiale, non digitale, condivide con esso molti aspetti utilitari e tra le altre la caratteristica di poter essere considerato come una riserva di valore grazie alla loro scarsità, e al loro costo di estrazione.

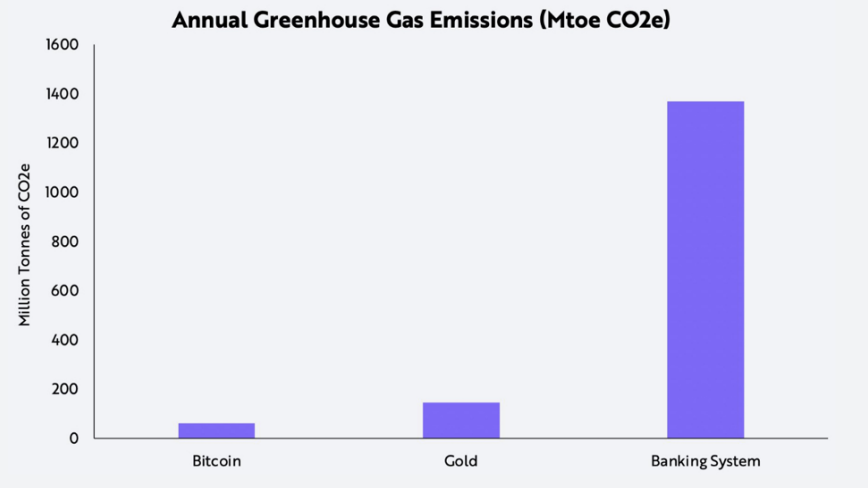
Ebbene, vediamo come l'oro sovrasta anche in questo caso il dato sull'emissione di Bitcoin di più del 65%.

L'inquinamento apportato dal *mining* della rete PoW più importante al mondo è certamente elevato, ovviamente soluzioni green sarebbero da preferire per cercare di contenere i danni apportati dalle emissioni, ma d'altra parte è scorretto additare questa

tecnologia come altamente colpevole in mezzo a tante altre ben peggiori per quanto riguarda l'apporto di inquinamento globale.

Un altro studio svolto da ARK Invest riguarda le differenze tra Bitcoin e il sistema bancario tradizionale, sia sotto un punto di vista più ambientale sia etico, in quanto come vedremo si sofferma sull'utilizzo del Bitcoin come mezzo di scambio e sul paragone con il contante per il contributo allo svolgimento di attività illecite.

Figura 15 - Il paragone con i sistemi tradizionali sulle emissioni



Fonte: *https://ark-invest.com/articles/analyst-research/bitcoin-myths/*

Nel grafico si nota la maggior contribuzione dell'oro all'inquinamento globale, come visto in precedenza, ma con un'aggiunta a dir poco spaventosa, ossia quella dei tradizionali sistemi a cui siamo abituati e del loro apporto relativo misurato, pari a circa 1.368 $MtCO_2$.
Visto in questi grafici, un sistema come quello basato sul concetto di Proof of Work di Bitcoin, sembra quasi *green*, essendo microscopico a confronto con i giganti sistemi istituzionali.

3.6.4 I costi

Come possono facilmente suggerire i limiti relativi all'inquinamento, e più in particolare nei sistemi Proof of Work come abbiamo visto nell'analisi del caso di 51% Attack, i costi relativi al mantenimento di una Blockchain sono ingenti, proprio a causa dell'enorme consumo di energia impiegata nelle azioni di mining.

Cifre che possono facilmente costituire causa di barriera all'ingresso per nuove aziende competitors, e ancor di più per singoli privati.

Oltre al punto di vista dei *miner* però bisogna tenere in conto anche quello dell'utente, che intende risparmiare più costi possibili relativi alle tasse da pagare per ogni transazione. Chain più efficienti e dense di attività di mining o staking diventano assolutamente più efficienti e scalabili rispetto a chain affaticate come quella presa in analisi (Bitcoin), richiedendo agli utenti costi trascurabili, vicini allo zero.

Già esistono numerose *chain* i cui costi sono stati abbattuti incredibilmente, o perché sviluppate come layer2 su altre chain proprio per migliorarne l'efficienza, o perché concepite dalla nascita con meccanismi alternativi in grado di far risparmiare i costi di mantenimento e messa in sicurezza dell'intero ecosistema.

3.6.5 Le attività illecite

Un altro argomento di cui spesso si sente parlare, utilizzato in sfavore di Bitcoin e altre Criptovalute è quello degli utilizzi illeciti a cui ti aprono le porte, dimenticandosi probabilmente del fatto che la nostra economia si è basata fino a pochissimo tempo fa quasi esclusivamente sul denaro in forma cartacea, oltremodo preferibile nel processo di svolgimento di attività illecite di qualsiasi genere.

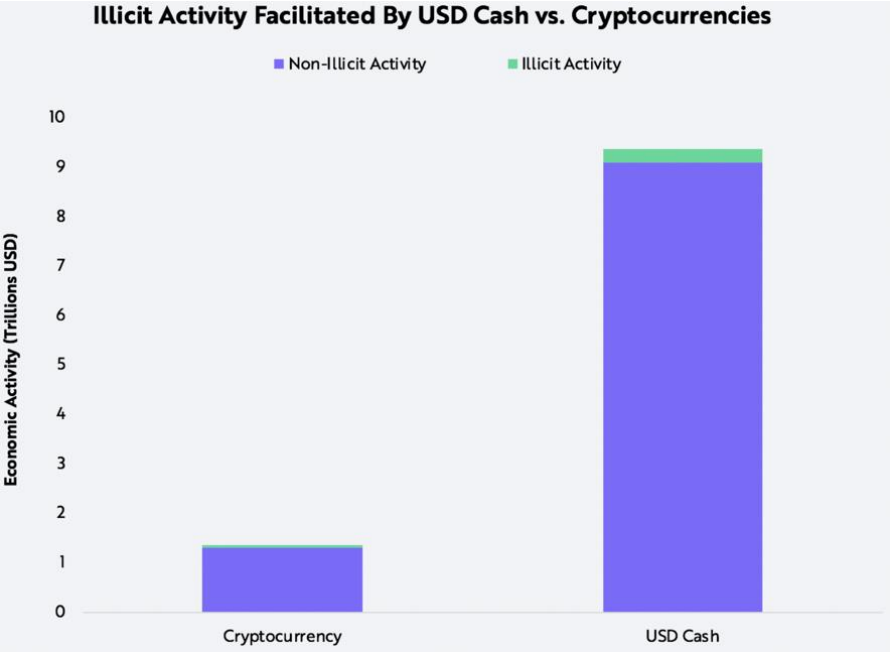
Questo è dovuto all'evento di Silk Road in particolare, una sorta di mercato nero online, che ha facilitato la vendita di droghe, armi e altri servizi illeciti, e che utilizzava come moneta per gli scambi Bitcoin, nei suoi primi anni.

Come tecnologia neutrale, Bitcoin consente a chiunque di effettuare transazioni e non può identificare ed escludere i "criminali".

Al contrario dei sistemi basati su identità o indirizzo IP, Bitcoin distingue i suoi utilizzatori tramite chiavi digitali crittografiche, rendendo difficile per le autorità censurare le transazioni o identificare i criminali.

La natura resistente alla censura di Bitcoin consente a chiunque di scambiare valore a livello globale e senza autorizzazioni, il che è una delle sue maggiori forze, e non va assolutamente scambiata con una predisposizione intrinseca allo svolgimento di attività illecite.

Figura 16 - La misura assoluta e relativa con cui le attività illecite vengono favorite da due diversi sistemi



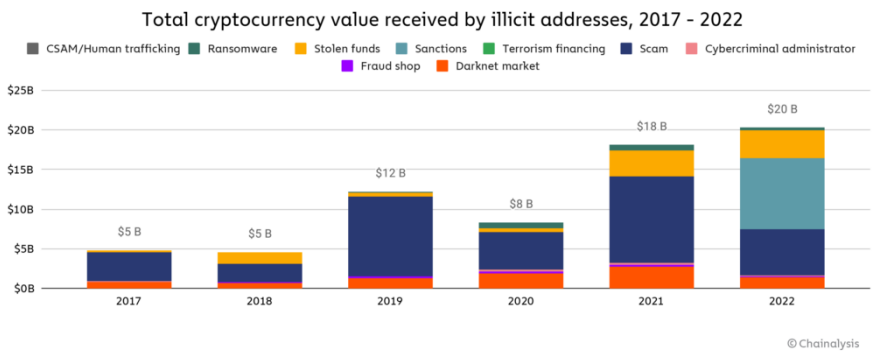
Fonte:https://ark-invest.com/articles/analyst-research/bitcoin-myths/

Secondo Chainalysis, un'azienda con sede a New York di analisi su Block Chain, solo una piccola percentuale delle transazioni con Criptovaluta è per scopi illeciti (al di sotto dell'1% delle transazioni totali).

L'azienda ci tiene a presentare annualmente un report di analisi sulle transazioni effettuate in favore di indirizzi illeciti, proprio per far leva sul punto di forza della trasparenza della

blockchain. Nel report sono anche suddivise per tipologia i diversi atti illeciti compiuti attraverso l'uso di valute digitali.

Figura 17 - Panoramica sul totale dei movimenti illeciti di Criptovaluta dal 2017 al 2022

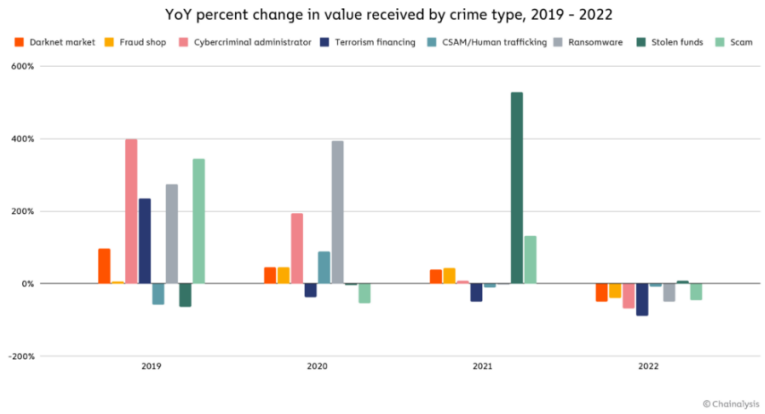


Fonte: https://www.chainalysis.com/blog/2022-crypto-crime-report-introduction/

Sono indubbiamente tutte azioni immorali e ingiuste, ma sono quasi tutte radicate nella "cultura" dell'uomo da diversi anni prima che nascesse la tecnologia della Blockchain, che quindi non le ha favorite in nessun modo, anzi.

Se analizziamo l'ampiezza dei volumi tra gli anni 2021 e 2022, si può notare con facilità grazie al tipo di grafico, che la tendenza è stata per tutte le attività quella della diminuzione in termini percentuali, con l'unica eccezione delle sanzioni che pesano più del 40% del totale, in un anno particolarmente insidioso sotto il punto di vista politico e dei rapporti tra le diverse giurisdizioni.

Figura 18 - La variazione percentuale dei movimenti illeciti, divisi per tipologia



Fonte: https://www.chainalysis.com/blog/2022-crypto-crime-report-introduction/

Infatti, il valore del volume è aumentato a dismisura specialmente dopo il piano attuato dall'OFAC (Office of Foreign Asset Control) per cercare di controllare e sanzionare le aziende che si sono servite delle Criptovalute per fini illeciti, come riciclaggio di denaro o vendita di stupefacenti, impiegando cifre ben al di sopra delle possibilità di clienti retail.

La trasparenza della rete Bitcoin consente a qualsiasi utente di visualizzare l'intera storia delle transazioni, il che suggerisce che il contante fisico sia un mezzo migliore per l'attività illecita. Infatti, nonostante la maggiore difficoltà a determinare il luogo o l'identità di chi effettua le transazioni, la blockchain offre sicuramente uno storico più trasparente e preciso rispetto a quello dei contanti, che non a caso rappresentano una quota maggiore di attività illecite rispetto alle transazioni con criptovalute, sia in termini assoluti sia relativi.

3.6.6 La Compatibilità tra piattaforme

La scarsa, se non in alcuni casi inesistente interoperabilità tra diverse blockchain rappresenta il primo vero ostacolo significativo della tecnologia, per l'adozione e l'utilizzo su larga scala delle criptovalute. La mancanza di una comunicazione efficiente tra le diverse blockchain rende difficile per gli utenti gestire e trasferire le proprie criptovalute da una rete all'altra, limitando così la loro portata e la loro utilità.

Infatti, se per esempio volessi inviare dei BTC su rete diversa da quella nativa (Bitcoin), come ad esempio la rete Ethereum, questa operazione non sarebbe possibile per un problema di incompatibilità tra le due Blockchain.
Conflitto irrisolvibile, che nasce dal linguaggio di scrittura delle due piattaforme, e che è un problema ricorrente in considerazione del limitato sviluppo e impiego di queste tecnologie.

Tuttavia, ci sono alcune soluzioni in fase di sviluppo che promettono di risolvere questo problema in modo semplice ne mantenendo un elevato livello di sicurezza.

Ad esempio, il concetto di "cross-chain" sta guadagnando terreno nell'industria delle criptovalute e rappresenta un'alternativa potenziale alle soluzioni esistenti.

La tecnologia cross-chain consente agli utenti di trasferire criptovalute tra diverse blockchain senza dover passare attraverso un intermediario o una piattaforma di scambio centralizzata. Questo è possibile grazie all'uso di ponti (o "bridges") che consentono la comunicazione tra le diverse blockchain, consentendo così anche il trasferimento di asset tra le diverse reti.

Inoltre, alcune aziende stanno lavorando su nuove soluzioni di interoperabilità ben più sofisticate e complesse rispetto al concetto di “cross-chain”, come Polkadot e Cosmos.

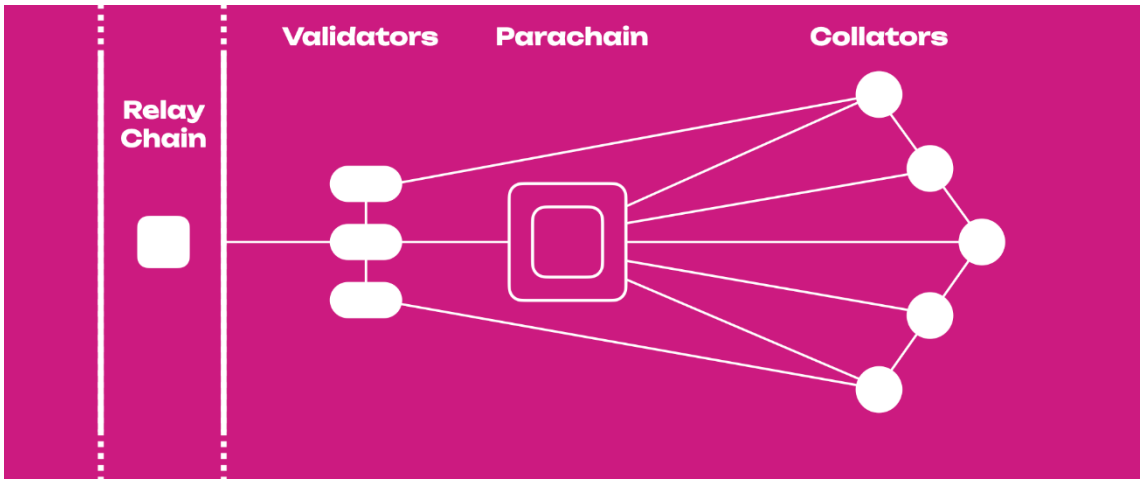
3.6.7 Le Para Chain

Già esistono i primi progetti che puntano a colmare questo tipo di mancanza basandosi su modelli di tipo Parachain, come Polkadot, che intendono risolvere simultaneamente i problemi di scalabilità e interrelazione tra chain.
Per fare ciò si basa il sistema su un modulo un po' alterato rispetto alla normale BlockChain, in cui troviamo al centro la Relay Chain, ossia la chain principale, il cuore dell'ecosistema, su cui gira il token nativo della Chain.
È quindi questa la principale responsabile delle votazioni e della sicurezza dell'intero ecosistema.
Accanto a questa Relaychain si possono sviluppare diverse Parachain, che si identificano in Blockchain a sé stanti, dotate di un Token proprio e quindi di un'indipendenza operativa.
Tutte le Parachain sono messe in relazione tra loro grazie alla Relaychain permettendo a diversi protocolli di interagire.
Inoltre, all'interno di questo tipo di modello è presente un'altra figura essenziale, quella dei "Collators".

Il Collator svolge all'interno della parachain il ruolo di manutentore, in quanto le transazioni vengono spezzettate nel processo di "sharding" per migliorare l'efficienza e la scalabilità dell'intero ecosistema.

La sua funzione è quella di recuperare i vari shards delle transazioni, le elaborano per produrre le prove e passarle in un secondo momento ai validatori per la validazione.

Figura 19: Il modello Parachain di Polkadot



Fonte: https://wiki.polkadot.network/docs/learn-parachains

Polkadot è un esempio lampante di una piattaforma che mira proprio a fornire questa interoperabilità tra diverse blockchain.

In altre parole, Polkadot vuole mettere diverse blockchain in condizione di comunicare tra loro in modo fluido e di scambiare informazioni senza problemi grazie all'utilizzo di un modello basato sulla Parachain.

Polkadot, che svolge nel suo ecosistema il ruolo di Relay chain, quindi il ruolo della chain principale, è stata fondata da Gavin Wood, uno dei co-fondatori di Ethereum, ed è supportata da una immensa comunità di sviluppatori altamente competenti e appassionati.

È proprio grazie a soluzioni di questo tipo che, anche il limite della scarsa interoperabilità tra diverse chain, viene abbattuto con facilità, grazie al naturale processo di sviluppo della tecnologia, che si evolve per soddisfare le esigenze sempre crescenti.

4. Teorie ed applicazioni

4.1 Le applicazioni della Blockchain

La Blockchain risulta essere una tecnologia versatile, che può essere utilizzata in molte diverse applicazioni, migliorandone l'efficienza.
Troviamo infatti applicazioni alla sfera contrattuale, con gli Smart Contracts, che sono programmi autonomi in grado di utilizzare la blockchain per registrare, gestire e convalidare accordi tra parti, proprio svolgendo la classica funzione dei contratti come tutti la conosciamo, ma rendendola più veloce e sicura grazie all'utilizzo di questa tecnologia.
Sempre per aumentare la velocità, la sicurezza e la disponibilità di dati, altre importanti applicazioni della blockchain sono rappresentate da:

- identità digitale, per cui ci si potrebbe appoggiare a questa tecnologia per il controllo dei propri dati personali e della loro condivisione;
- votazioni politiche, da non sottovalutare in quanto grazie alla blockchain si potrebbero creare sistemi di votazione sicuri e trasparenti, pressoché impossibili da manipolare;
- registri immobiliari, capaci di contenere tutti i dati relativi, riducendo il rischio di frodi e i tempi di transazione;
- tracciabilità delle catene di approvvigionamento, per cui attraverso questa tecnologia può essere utilizzata in modo da tracciare la provenienza e il percorso delle merci garantendone l'autenticità e la qualità.

Arriviamo poi alla più conosciuta fra tutte le applicazioni della blockchain, ossia le criptovalute.

In questo caso attraverso di essa si regolano tutti i rapporti di natura economica tra gli individui, rendendo possibili gli spostamenti di denaro senza la necessità di un'intermediazione classica come può essere quella di una banca.

Dopo aver compreso il funzionamento della Blockchain da un punto di vista più tecnico, ed aver quindi compreso i suoi vantaggi e svantaggi, passiamo ad analizzare le sue possibili applicazioni, estremamente utili e proficue, in diversi ambiti o processi che necessitano di uno svecchiamento in favore di metodi più efficienti e sicuri.
Alcune di queste applicazioni risulteranno utopiche, forse proprio a causa dell'enorme avanguardia della tecnologia, o forse a causa dei modelli cui siamo abituati, dove sempre più raramente esiste una vera parità di trattamento, anche tra singoli cittadini.

In ambito finanziario, il fallimento del genere umano e la conseguente perdita di fiducia verso il prossimo, ha fatto sì che un ente terzo si potesse intromettere negli scambi tra privati, per poterli regolare e per fungere da "garante di fiducia".
Così facendo, non solo si è rallentato il processo dello scambio, ma si è anche permesso a questi enti di sfruttarlo per ottenere un crescente potere economico e generare grossi introiti, detenendo la centralità del potere nelle sue mani.

Le possibili digressioni filosofiche in materia sarebbero infinite, ma un concetto in particolare esprime al meglio il punto centrale del discorso.
Questo è il concetto espresso dal proverbio pessimistico "Homo homini lupus", assunto dal filosofo Thomas Hobbes, ispirandosi all'Asinaria di Plauto, per alludere all'egoismo umano.
Hobbes, infatti, se ne serve nell'opera De cive, per descrivere lo stato di natura in cui si trovano gli uomini, schiavi dell'egoismo, che si combattono l'un l'altro per sopravvivere.
Dalle parole utilizzate traspare con estrema forza la sfiducia verso l'intero genere umano e i suoi sentimenti, tanto che il filosofo non si fa scrupoli ad affermare che l'amicizia, le buone azioni e i sentimenti benevoli non siano altro che atti di finzione nati dalla convenienza.
L'uomo infatti trarrebbe vantaggio dalla pacifica convivenza piuttosto che dalla guerra eterna e, cosciente di ciò, avrebbe fondato lo stato per impedire a tutti di uccidersi a vicenda.

Traslandolo e adattandolo, questo concetto dimostra di essere perfettamente applicabile alla quotidianità.

La società, dall'alba dei tempi, si è basata su suddivisioni in base alla disponibilità materiale e allo status sociale dell'individuo (basti ricordare il feudalesimo).

Il raggiungimento di un determinato status o l'arricchimento economico, con il passare degli anni sono diventate sempre di più cause determinanti circa il benessere e il piacere di vivere, tanto da divenire obiettivi principali nella vita della maggioranza delle persone, creando una competizione malata per cui, senza ovviamente generalizzare, chi si trova in una posizione sfavorevole è disposto a tutto, o quasi, pur di salire qualche gradino e avvicinarsi al suo obiettivo.
In alcuni casi estremi, si toglie a chi ha, per il solo gusto di farlo, per il gusto di vedere chi si trova in una posizione dominante scendere di uno o due gradini, senza trarne alcun beneficio.
Ebbene, questa è la perfetta incarnazione del proverbio latino sopra citato.

È proprio questa mancanza di fiducia, spesso giustificata, che rende la blockchain un mezzo utilissimo, poiché al posto di fidarsi della parola di qualcun altro, si potrebbe verificare autonomamente e in prima persona la realtà dei fatti.

4.2 La Finanza "Pubblica"

Immaginiamo una possibile applicazione di questo mezzo in grado di omettere la necessità di fiducia nei rapporti, specialmente in un rapporto che è causa di innumerevoli dissidi, ossia il rapporto cittadino-ente pubblico.

Come si è appreso in precedenza, chiunque grazie alla blockchain può verificare in proprio tutto ciò che su di essa accade.
Ora pensiamo alla gestione delle casse dello stato, i finanziamenti di opere pubbliche, gli incentivi, i bonus statali, e tutte quelle attività che comprendono la gestione da parte di un gruppo ristretto delle finanze pubbliche, ossia di un capitale potenzialmente utile a tutti.

Se questa gestione finanziaria venisse caricata e salvata sulla Blockchain, episodi di mala gestione del denaro, danni erariali o di furbi escamotage finanziari sarebbero molto più difficili da mettere in atto, se non addirittura impossibili nel giro di pochi anni, con la molto probabile nascita di squadre speciali o intelligence atte al controllo dei dati e delle transazioni che passano su questo nuovo database.

Purtroppo, episodi del genere non sono rari, tanto che solamente in Italia più volte si sono presentate problematiche relative a esenzioni illecite dal ticket sanitario (circa il 90% secondo ilSole24Ore), o di altre agevolazioni.
Oltre a questi, vicende di appalto illecito, evasione fiscale, riciclaggio e danni erariali in generale turbano il nostro paese ogni anno, che a partire dal vertice si impoverisce fino alle fondamenta.

I danni erariali per definizione sono i danni sofferti dallo stato o da un altro ente pubblico a causa dell'azione o dell'omissione di uno o più soggetti che agiscono per conto della pubblica amministrazione in veste di funzionario, dipendente o, comunque, inserito in un suo apparato organizzativo.

Il danno non è aleatorio, è stimabile, e a farlo è stata proprio la Guardia di Finanza, che ha identificato la cifra in circa 6 miliardi di euro di danni erariali e 2 miliardi di danni da appalti illeciti solamente nel periodo tra il 2018 e il 2019.
Le cifre sono molto probabilmente sottostimate, in quanto rappresentano solamente gli illeciti di cui la Guardia di Finanza è venuta a conoscenza, tralasciando tutto ciò che si trova più in profondità.

Non ci vuole molto a comprendere che cifre del genere non sono trascurabili quando si parla della gestione di un paese che ha fin troppe problematiche a carico relative alle sue finanze e alla loro gestione.
Ne consegue che, se si risolvesse, o almeno arginasse il problema, non solo in Italia ma in tutto il mondo, il beneficio sarebbe inestimabile.

In questo modo non si sta mirando all'utopico e anarchico mondo in cui non esista uno stato, inteso come ente centrale, in grado di prendere decisioni per la vita dei suoi cittadini.
Molto più realisticamente si sta dando il diritto ai cittadini di tracciare l'operato dell'ente cui sono sottoposti, come garanzia di protezione.

Non solo diventa così uno strumento di tutela per i cittadini, ma potrebbe diventare anche uno strumento di ricerca utile all'ente stesso.
Infatti, se molti più cervelli avessero accesso a questo tipo di dati, chiunque ne sia in grado potrebbe impegnarsi per capire quali sono i punti di forza e soprattutto i punti carenti della gestione, e proprio tutta questa forza lavoro sarebbe in grado di proiettare teorie e rimedi volti a risolverli, o quantomeno contenerli, migliorando indubbiamente l'efficienza di tale gestione.

Volendoci addentrare ancor di più in questo tema di pubblicità, si potrebbe addirittura fantasticare (purtroppo) di inserire nella blockchain anche gli stipendi e gli scambi di denaro di qualsiasi genere riguardanti opere di interesse pubblico, un altro tema molto caldo che crea non pochi scompensi.

Essendo funzionari pubblici, il loro operato dovrebbe essere rivolto al bene pubblico, così come la loro persona dovrebbe impegnarsi per raggiungere più obiettivi possibili nell'interesse del pubblico generale composto dai cittadini.
Essi dovrebbero quindi accettare di essere pubblicamente tracciabili durante tutto il periodo di carica, rinunciando a un po' di privacy per poter svolgere a pieno il loro incarico in un rapporto paritario con il pubblico.

Ovviamente questa ultima applicazione è molto e in linea di massima non è indispensabile; proprio per questo motivo potrebbe facilmente creare pareri contrastanti e diverse problematiche.

La questione della privacy, in questo caso dei funzionari pubblici, è infatti un tema delicato che richiede una soluzione bilanciata.

Da un lato, la trasparenza e la pubblicità dei loro spostamenti di denaro potrebbero essere viste da alcuni come un dovere verso la collettività e un modo per prevenire possibili casi di corruzione e di abuso di potere.
D'altro canto, il diritto alla privacy è un diritto fondamentale citato nella Costituzione, che va garantito a tutti i cittadini, compresi i funzionari pubblici, per proteggerli da possibili rischi e per garantire la loro sicurezza personale.
Essendo completamente tracciabili, infatti, essi sarebbero esposti a malintenzionati, mettendo la loro figura e quella dei loro familiari in grave pericolo.

Analizzando meglio la situazione si potrebbero effettuare degli aggiustamenti in modo da garantire quantomeno la privatezza di spostamenti di denaro identificabili come appartenenti alla sfera della vita privata di ognuno di essi, così da mantenere il loro diritto alla privacy in veste di cittadini per proteggerli dai rischi evitabili.

Un modo efficace di raggiungere questa situazione bilanciata sarebbe quello di adottare un sistema duale, in cui i funzionari pubblici mantengano pubblici gli spostamenti di interesse generale, avendo però anche a disposizione un conto privato secondario alle cui informazioni non si potrebbe accedere, dando loro modo di condurre la propria vita e fare le proprie spese in sicurezza come cittadini qualsiasi.
In questo modo si potrebbero consultare i dati relativi agli stipendi e gli effettivi spostamenti effettuati dai funzionari verso il proprio conto privato che rimarrà segreto.
Infatti, oltre ad essere lesivo per il diritto alla privacy risulterebbe addirittura inutile e oltremisura costoso tener traccia di tutti i movimenti di denaro privati dei funzionari.

4.3 Le elezioni politiche

L'uso della tecnologia blockchain potrebbe essere applicato ad un'altra importante attività di interesse generale che è causa di alcune incomprensioni date dalla sfiducia, ossia le elezioni politiche. Questa tecnologia avrebbe il potenziale per rivoluzionare il modo in

cui votiamo, creando un modo più sicuro ed efficiente di esprimere il proprio voto, che in ultima analisi potrebbe portare a un processo democratico più trasparente e affidabile.

Il vantaggio principale di un sistema di voto basato su blockchain è che fornisce una registrazione immutabile dei voti, che non può essere alterata o manomessa.
Infatti, una volta che il voto è stato espresso e registrato sulla blockchain, è impossibile modificarlo.
Questo garantisce l'integrità del processo di voto e riduce il rischio di frodi o di tentativi di ostruzione di un procedimento ufficiale del genere.

Un altro vantaggio di un sistema di voto basato sulla blockchain è che elimina la necessità di un conteggio manuale dei voti. La blockchain conteggia automaticamente i voti e fornisce risultati in tempo reale, riducendo in modo significativo il tempo e le risorse necessarie per il conteggio dei voti e la consegna dei risultati. Questo rende il processo più veloce, efficiente e affidabile.
Inoltre, la natura decentralizzata di un sistema di voto basato su blockchain garantisce che nessuna singola entità possa controllare il processo di voto rendendolo più trasparente e sicuro, in quanto nessuno può manipolare o influenzare l'esito delle elezioni.

La pratica di manipolazione dei voti o di sabotaggi atti a trarre vantaggi di qualsiasi tipo non sono pratiche abbandonate da anni, anzi.
Una recente vicenda, fra tutte, sta acquisendo sempre più interesse e seminando confusione. Si tratta della vicenda che ha visto protagonista l'ex Presidente degli Stati Uniti d'America Donald Trump, che è stato accusato e arrestato proprio per fatti relativi alla "storica" votazione del 2020 che lo vedeva come contendente principale di Joe Biden per il ruolo di presidente degli Stati Uniti d'America.

"*Il 4 marzo 2024 Donald Trump dovrà affrontare il suo primo processo penale. Lo ha deciso la giudice Tanya S. Chutkan, responsabile del processo contro l'ex presidente a Washington, dove è perseguito per l'assalto dei suoi seguaci al Congresso e per aver tentato di rovesciare l'esito delle elezioni presidenziali del 2020. L'ex presidente è accusato a Washington di quattro capi d'accusa: cospirazione per frodare gli Stati Uniti, cospirazione*

per ostacolare un procedimento ufficiale, ostruzione e tentativo di ostruzione di un procedimento ufficiale e cospirazione contro i diritti. […] Il primo capo d'accusa prevede una pena massima di cinque anni di carcere, il secondo e il terzo capo d'accusa prevedono rispettivamente una pena massima di 20 anni di carcere e il quarto capo d'accusa prevede una pena massima di 10 anni di carcere" ([1]).

Essendo la Blockchain caratterizzata da una personalità inequivocabile, poiché sappiamo che la firma per una qualsiasi transazione può essere apposta dal solo conoscente della chiave privata, e quindi il suo proprietario, eseguire processi come quello della votazione è di incredibile semplicità tramite questa tecnologia, ed episodi come quello dell'ex presidente americano o altre possibili cause di dubbiosità o confusione sarebbero pressoché impossibili da verificarsi.

Non a caso, molte blockchain già ora sono sviluppate come delle democrazie reali, in cui le decisioni più importanti, decisive per il loro futuro, vengono prese da tutti i possessori di diritti di voto, in maniera efficiente e veloce.

Sfruttando questa tecnologia si risparmierebbe notevolmente sul tempo richiesto per gli spostamenti verso le sedi istituite a seggio elettorale, oltre che sul conteggio dei voti che sarebbe immediato ed automatico.
Al tempo stesso si andrebbe a giovare di una maggiore affidabilità e sicurezza, che non lascerebbe spazio a episodi di sabotaggio di qualsiasi tipo.
Sembra assurdo che in un'epoca come la nostra, profondamente digitalizzata, ancora ci si esponga all'errore umano e all'imprecisione della votazione cartacea, quando adottando una semplice e digitale misura alternativa si guadagnerebbe in efficienza e comodità.

Tuttavia, ci sono ancora sfide da superare quando si tratta di implementare un sistema di voto basato su blockchain.
Una delle sfide principali è legata alla privacy degli elettori.

([1]) Fonte: Blanca Castro, Edizione italiana: Cristiano Tassinari – "Eletto presidente, ma condannato: cosa accadrebbe a Trump? Un evento senza precedenti negli USA" (https://it.euronews.com/2023/08/29/eletto-presidente-ma-condannato-cosa-accadrebbe-a-trump-evento-senza-precedenti-negli-usa).

Se da un lato la tecnologia blockchain garantisce l'anonimato degli elettori, dall'altro rende difficile assicurare la privacy dei loro voti.
Infatti, i voti sono essenzialmente espressi da stringhe alfanumeriche, che fanno mantenere l'anonimato agli elettori.
Il problema sorge nel momento in cui per qualche ragione dovesse diventare facilmente possibile ricollegare gli indirizzi alle persone fisiche che ne sono proprietarie, facendo così venire meno la caratteristica dell'anonimato del voto.

Un'altra sfida, sempre meno difficile da superare, è legata all'accessibilità, poiché non tutti dispongono di un accesso a Internet o alla tecnologia necessaria per votare sulla blockchain.

Infine, come sempre, la scalabilità è un'altra questione che deve essere affrontata, poiché i sistemi di voto basati su blockchain devono essere in grado di gestire un gran numero di elettori contemporaneamente.

Nonostante queste sfide, i potenziali vantaggi di un sistema di voto basato su blockchain lo rendono un'importante area di ricerca e sviluppo in corso nel campo delle elezioni politiche.
Con ulteriori progressi e aggiornamenti, un sistema di voto basato su blockchain potrebbe essere il futuro delle elezioni politiche, rendendo il processo più efficiente, trasparente e sicuro.
Ad esempio, i ricercatori stanno cercando di superare la sfida più ardua, lavorando allo sviluppo di un sistema di voto basato su blockchain che garantisca la privacy degli elettori, pur mantenendo l'integrità e la sicurezza del processo di voto.
Inoltre, si stanno compiendo sforzi per aumentare l'accessibilità e fare sì che tutti possano partecipare al processo elettivo utilizzando la tecnologia blockchain.

4.4 La proprietà privata

Il tema della proprietà privata è un tema fondamentale, in grado di far facilmente comprendere la grande utilità di una tecnologia così sicura anche nella vita quotidiana, senza andare a tirare in ballo grandi temi come la politica o la finanza pubblica, che sono sicuramente più complessi e lenti da aggiornare.

La proprietà di un oggetto fisico, che sia un'auto, un immobile, un orologio o un pezzo d'arte, è necessaria e fondamentale per legge, per poterne godere e disporre in modo pieno ed esclusivo.
Talvolta, come nel caso di una qualsiasi transazione, si presenta la situazione in cui è necessario dimostrare di essere legittimi proprietari di un bene, e non sempre risulta facile, destreggiandosi tra documenti di ogni tipo, ricomponendo il quadro completo e integrando in qualche caso alcuni pezzi essenziali mancanti.
Questo problema viene messo in risalto quando lo scambio ha ad oggetto beni di lusso. Immaginiamo un proprietario di un orologio di alta orologeria, o di un quadro di un certo valore, che intenda vendere il suo bene a un terzo.
In uno scambio di questo tipo non si possono lasciare spazi a incertezze, né dalla parte del venditore, tantomeno da quella dell'acquirente che intenderà sicuramente essere completamente al sicuro con riguardo allo scambio che sta per effettuare.

I principali problemi sono rappresentati da:

- dimostrazione dello storico degli scambi del bene in questione, in modo tale da poter risalire, nel migliore dei casi, al primissimo scambio, per potersi accertare dell'effettiva veridicità dell'oggetto in questione, evitando la trappola della contraffazione, ed anche per evitare di acquistare un bene il cui venditore non coincide con l'effettivo proprietario, ossia un bene sottratto illecitamente (rubato);

- trattandosi in certi casi di asset veri e propri, considerando la speculazione che si muove dietro a determinati beni di lusso, torna estremamente utile avere un report

minuzioso dei prezzi di tutti i precedenti scambi, per poter interpretare l'acquisto in modo più cosciente e informato, in un'ottica di conservazione o incremento del valore nel tempo.

Essenzialmente quando si compie un acquisto di beni durevoli, ci si deve porre una moltitudine di domande circa il chi, il dove, il quando, il come, il quanto e tutte le modalità, per sapere con esattezza tutto il percorso che tale bene ha compiuto nell'arco della sua vita utile.
Non sempre è possibile reperire queste informazioni, e spesso si compie l'acquisto "sulla fiducia" (tornando al tema iniziale) oppure presso enti (musei, boutique ecc.) che sono certamente in grado di fornire tutte queste informazioni, o comunque di dare una garanzia circa il bene in questione, ma che tendono quasi sempre a imporre prezzi maggiorati che gli garantiscano un certo margine, proprio a causa del valore di questa maggiore sicurezza che risulta essenziale per effettuare un acquisto consapevole.
Immaginiamo ora se lo storico di un bene fosse costantemente aggiornato e salvato su blockchain, permettendo a chiunque di informarsi sulla sua vita e sul suo storico degli scambi, garantendo la sicurezza dell'acquisto che si sta effettuando, indipendentemente da chi sia il venditore.
In tal modo si combatterebbe un mercato illecito che ogni anno tende a crescere, e rappresenta, solamente in Italia per il periodo 2008-2021, un giro di affari superiore a 5,9 miliardi di euro.
Questo è il mercato della contraffazione, che verrebbe messo in ginocchio dall'integrazione della blockchain, in quanto un bene il cui storico non dimostra con certezza la propria provenienza e veridicità perderebbe immediatamente tutto il valore.

Inoltre, si contrasterebbe in maniera evidente il furto, infatti basta pensare ad un orologio rubato, di cui si potrebbe immediatamente conoscere il legittimo proprietario, e quindi anche verificare che lo si stia acquistando da esso, omettendo tra l'altro ogni problema relativo ad uno degli istituti più dubbi della legislazione italiana, quello della buona fede.

4.5 Gli NFT

Per capire come è resa possibile la proprietà su blockchain bisogna comprendere correttamente cosa sia un Non Fungible Token (NFT).

Gli NFT sono una forma di token crittografico che ha recentemente preso d'assalto l'industria dell'arte digitale, consentendo ai creatori di opere d'arte di certificare l'autenticità delle proprie creazioni e di trasferirne la proprietà in modo sicuro e immutabile, essendo sviluppati sulla blockchain.

Essenzialmente, gli NFT rappresentano, come suggerisce il nome, un token non fungibile, ossia non spendibile.

Se pensiamo a una moneta, che sia un conio o una moneta digitale come Bitcoin, il valore di una unità di quella moneta avrà lo stesso valore di un'altra qualsiasi unità della stessa moneta. Questo non può dirsi per gli NFT, che rappresentano un bene unico e insostituibile e quindi senza un valore stabilito, proprio come può essere un quadro o un immobile.

In sostanza, prendendo come esempio un’opera d’arte, quando un qualsiasi quadro viene creato come NFT, viene coniata una copia digitale unica dell'opera stessa.

Questa copia digitale è poi registrata sulla blockchain, consentendo di identificare in modo univoco l'opera d'arte e di garantire che essa sia autentica, mostrandone anche lo storico degli scambi con i rispettivi valori di scambio.

In pratica, la blockchain funge da registro pubblico che tiene traccia di tutte le transazioni relative all'opera d'arte.

Gli NFT sono stati ampiamente implementati anche in altri ambiti, ad esempio quello videoludico, nel mondo dello sport o del collezionismo.

Un ultimo settore rilevante che potrà giovare in futuro di implementazioni sempre più efficaci è rappresentato dall’immobiliare.

Infatti, un immobile è per eccellenza un asset unico, irripetibile, e dotato di un valore deciso dai contraenti interessati. Proprio per questo motivo, sarebbe perfetto utilizzare un NFT per rappresentarlo e scambiarlo su Blockchain.

Già è una pratica utilizzata in alcuni paesi del mondo più aperti alle integrazioni su Blockchain, e sono state scambiate proprietà come immobili su Blockchain sotto forma di NFT. Essenzialmente, essendo l'NFT uno soltanto, come l'immobile a cui si riferisce, il possessore dell'NFT diventa anche possessore dell'immobile fisico. Lo storico degli scambi è sempre immediatamente disponibile sulla blockchain, e ciò permette una maggiore sicurezza e trasparenza in tutti quei processi legati al suo passaggio di proprietà.

4.6 Il furto d'identità, l'appropriazione indebita

Come si è visto con la proprietà privata, la blockchain permette un'identificazione univoca e immutabile di un bene unico. Questo la rende particolarmente adatta anche per la gestione di documenti e titoli di riconoscimento, dove la sicurezza e l'autenticità dei dati rappresentano elementi di fondamentale importanza.

Ad esempio, l'utilizzo della blockchain per la gestione dei documenti di identità potrebbe garantire un elevato livello di sicurezza e certezza nell'associazione tra un titolo qualsiasi, che possa essere la Laurea, l'abilitazione a determinati lavori, l'assegnazione di alcune agevolazioni speciali o addirittura il conseguimento di un premio come l'oro alle olimpiadi o un Nobel, e la persona fisica che ne è legittimamente in possesso.

In definitiva, sarebbe possibile prevenire crimini come il furto d'identità e l'appropriazione indebita molto semplicemente, grazie alla tracciabilità e all'autenticità dei documenti salvati sulla blockchain.

In particolare, l'utilizzo di questa tecnologia potrebbe tornare molto utile anche nella lotta alla contraffazione dei marchi e dei brevetti registrati. Grazie alla sua capacità di garantire l'autenticità dei marchi e dei brevetti, sarebbe più difficile per i contraffattori operare senza essere scoperti e più semplice invece per le autorità competenti individuare e perseguire tali reati.

In generale, l'implementazione della blockchain per la gestione di documenti e titoli di riconoscimento può portare a numerosi vantaggi, tra cui una maggiore efficienza, una riduzione dei costi e una maggiore sicurezza negli scambi.

Tuttavia, ancora una volta è importante valutare attentamente le implicazioni e le sfide che potrebbero sorgere nell'uso di questa tecnologia, al fine di garantire che sia utilizzata in modo responsabile e sostenibile.

4.7 La tassazione smart

Un’applicazione ben più lontana dall’attualità ma con un immenso potenziale è poi quella relativa alla tassazione.
Infatti, immaginiamo un commerciante che decida di implementare pagamenti su blockchain all’interno della sua attività.
Tutti quei processi di redazione del bilancio e dichiarazione dei redditi ai fini tassativi sarebbero non solo estremamente più veloci, ma anche renderebbero impossibile l’evasione fiscale.
Se infatti si abolisse il sistema di pagamenti non tracciabile per eccellenza, il contante, gli esercenti di attività che implementerebbero sistemi basati su Blockchain sarebbero dotati di un libro mastro sicuro e certo al cento per cento, che fornirebbe un valore esatto relativo al reddito dell’attività in questione, rendendo poi la tassazione veloce, sicura, e potenzialmente immediata.
Il tema della tassazione è un tema delicato, che ancora una volta apre la porta a pareri contrastanti.

Il vero valore aggiunto di questa implementazione si raggiungerebbe solo se tale tecnologia si rendesse uno standard. Così facendo infatti, tutti sarebbero tassati giustamente in proporzione al loro rendimento, e con il passare del tempo molto probabilmente si riuscirebbero a riportare entro margini ben più accettabili le percentuali di imposte, non essendo condizionate da chi tenta di sottrarsi a tale obbligo.

4.8 La supply chain

Uno dei settori che maggiormente sta esplorando i vantaggi della blockchain è quello della gestione della supply chain, specialmente in situazioni di complessi aziendali globali, che devono sopperire alle richieste di consumatori da tutto il mondo nel modo più veloce e efficiente possibile.

La tecnologia blockchain può essere utilizzata per creare un sistema di supply chain più sicuro e trasparente.
Utilizzando questa tecnologia, infatti, ogni passaggio nella catena di fornitura può essere registrato e verificato, creando un registro inalterabile di tutte le attività.
Ciò può contribuire a ridurre le frodi e ad aumentare la responsabilità nel settore della supply chain.

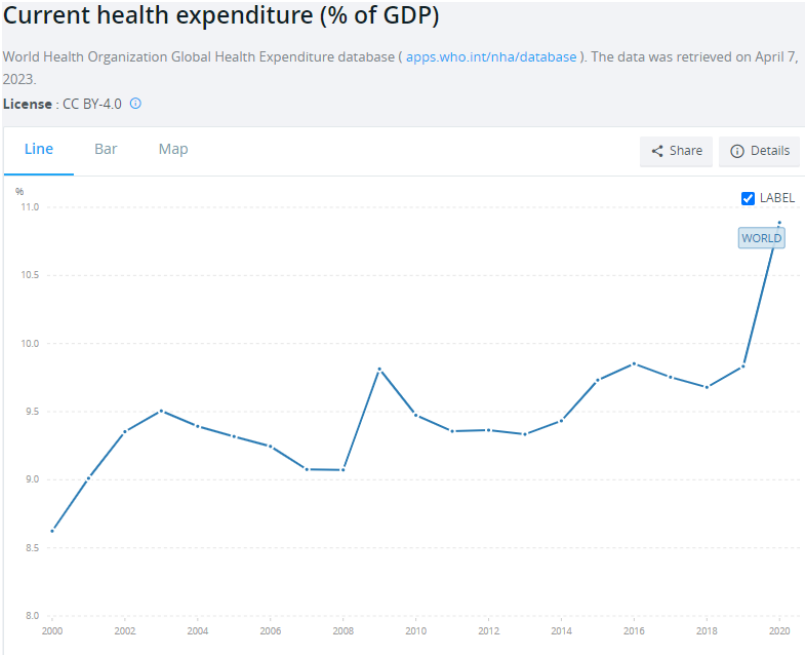
Il principale vantaggio che nasce dall'integrazione della blockchain nella catena di fornitura è la sua maggiore tracciabilità.
Utilizzando la blockchain, le aziende possono tracciare i prodotti dalla loro origine fino all'utente finale, indipendentemente dalla loro posizione.
Ciò può contribuire a migliorare la trasparenza della catena di approvvigionamento, particolarmente importante in settori come quello alimentare e farmaceutico, dove è fondamentale garantire che i prodotti siano sicuri e provengano da fonti etiche.
Con la blockchain, le aziende possono creare un registro a prova di manomissione dell'intera catena di fornitura, riducendo il rischio che i prodotti contraffatti entrino nella catena di fornitura e garantendo effettivamente per la provenienza dei prodotti.

Oltre a una maggiore tracciabilità, la blockchain nella catena di approvvigionamento può anche portare a una maggiore efficienza. Utilizzando gli smart contracts, infatti, le transazioni possono essere automatizzate, riducendo la necessità di intermediari e snellendo la catena di fornitura. Ciò può portare a transazioni più rapide ed economiche, migliorando ancor di più le prestazioni complessive della catena di approvvigionamento.

Una delle problematiche più grandi circa questo tipo di integrazione è la necessità di interoperabilità tra i diversi sistemi blockchain, oltre alla scalabilità e ai costi di implementazione della blockchain stessa.
Per superare le sfide associate all'integrazione della blockchain nella supply chain, le aziende dovrebbero considerare attentamente le proprie esigenze e i propri obiettivi e collaborare con esperti del settore per sviluppare una soluzione in grado di girare su una blockchain personalizzata.
In questo modo, possono sfruttare i vantaggi della tecnologia blockchain riducendo al minimo i rischi e i costi, che dipendono da altri, associati alla sua implementazione.

4.9 L'Health Care

Un settore trainante di questa tecnologia, che ogni anno muove sempre più denaro, è quello della sanità.
Il settore sanitario, infatti, specialmente dopo l'evento COVID-19 ha ricevuto un fortissimo impulso di crescita, che ha fatto aumentare le spese relative a questo settore facendole arrivare a rappresentare quasi l'11% del PIL mondiale (Gross Domestic Product).
Nel datato mondo dell'Health Care, ci sono alcuni processi facilmente velocizzabili e migliorabili in efficienza grazie all'integrazione della tecnologia della Blockchain.



Alcune possibili applicazioni sono rappresentate da:

- Autenticazione del farmaco. Come citato in precedenza nei riguardi della contraffazione, grazie all'implementazione di questa tecnologia si può ottenere un database immutabile in grado di fornire elevati standard di conformità e sicurezza. Con la blockchain, è possibile creare un registro digitale affidabile e immutabile per tracciare la provenienza e la storia di un farmaco, dalla produzione alla distribuzione. Ciò può aiutare a prevenire la contraffazione di farmaci e garantire che i pazienti ricevano farmaci sicuri ed efficaci;

- Registri medici. Poiché i pazienti vengono visitati da diversi medici o addirittura in diverse sedi e poiché le loro esigenze in termini sanitari variano in base alla loro condizione, le cartelle cliniche devono essere aggiornate e facilmente trasferibili tra le varie istituzioni sanitarie per garantire la precisione. Grazie alla blockchain, questo risultato è ottenibile con tutti i pregi che si porta dietro la tecnologia.
- Credenziali velocizzate. Per mantenere aggiornate la formazione e le certificazioni, la blockchain può accelerare la verifica delle qualifiche in campo

medico. Ciò riduce le frodi e le inesattezze e impedisce che si verifichino potenziali situazioni pericolose. Con la blockchain, i medici possono facilmente condividere le proprie credenziali con le istituzioni sanitarie e le compagnie di assicurazione. Ciò può aiutare a garantire che solo i medici qualificati possano esercitare la professione medica e migliorare la sicurezza dei pazienti.

- Rapporti assicurativi.Al sistema condiviso che traccia lo stato sanitario di un paziente si potrebbe affiancare quello assicurativo rendendo più efficaci i rapporti tra compagnie assicurative, ospedali e pazienti. Con la blockchain, le compagnie assicurative possono facilmente accedere alle informazioni sanitarie dei pazienti e valutare i rischi in modo più accurato. Ciò può aiutare a ridurre i costi dell'assicurazione e migliorare l'accessibilità alle cure mediche.
- Tracciabilità di organi. La blockchain può infine può avere un potenziale incredibile nel merito dei trapianti di organi. Potendo creare una rete condivisa su blockchain, i dati sui donatori e i pazienti che necessitano di un trapianto sarebbero facilmente ottenibili, velocizzando un processo essenzialmente vitale.

In sintesi, la tecnologia blockchain ha il potenziale per trasformare o, meglio, modernizzare il settore sanitario in molti modi, potenzialmente migliorandone l’efficienza, la rapidità e la qualità.

5. Conclusioni

Questa tesi ha esaminato il fondamentale ruolo che svolgono i database nel nostro contesto sociale e, in particolare, ha approfondito l'analisi di un nuovo tipo di database, più moderno ed efficiente dei precedenti, rappresentato dalla blockchain.

I temi trattati non sono limitati alla tecnologia informatica, ma spaziano e includono trasversalmente altri temi fondamentali per dare un contesto al trattato, come quello della fiducia nei rapporti uomo a uomo o ancora meglio nei rapporti uomo a istituzione.

Ci si sposta poi su temi di filosofia, di politica e di etica connessa al possesso di grandi quantità di un minerale prezioso, molto più dell'oro, ossia i dati sul pubblico dei consumatori.

Questa nuova tecnologia è in grado di fornire risultati impressionanti in termini di sicurezza e trasparenza, essendo rappresentata essenzialmente da un registro distribuito sempre disponibile a tutti, in qualsiasi momento.

Ciò che viene salvato sulla blockchain, inoltre, non può essere manipolato o modificato in un secondo momento, garantendo un elevato livello di sicurezza.

Questa tecnologia consente di registrare transazioni in modo permanente e immutabile, creando una catena di blocchi (blockchain) che può essere verificata e validata in modo distribuito da tutti i partecipanti della rete.

In questa tesi, si è visto come la tecnologia blockchain può essere applicata in diversi settori, come la sanità, la finanza e la logistica per citarne alcuni.

La tecnologia in sé è profondamente moderna e, diversamente da tante altre tecnologie nate per essere soltanto efficienti, è anche pregna di temi rilevanti in materia di etica e valori.

Infatti, questa è forse la prima tecnologia a portare con sé l'idea che la trasparenza e la tracciabilità da parte di tutti siano caratteristiche necessarie e fondamentali, in modo da posizionare tutti quanti sullo stesso livello, poiché nessuno si trova in una posizione favorevole in termini di disponibilità dei dati.

Se il potenziale di questa tecnologia non rimanesse inesploso ma, anzi, venisse sviluppato e aggiornato per integrarlo sempre più efficacemente con i tradizionali sistemi a cui siamo abituati, si potrebbero ottenere ottimi risultati sia in termini di efficienza che in termini di trasparenza e sicurezza, andando incontro peraltro a coloro che sono più diffidenti, e che quindi difficilmente si abbandonano alla guida istituzionale, sapendo che l'interesse principale di grandi istituzioni del genere non sia tanto il bene di tutti, quanto il bene per il proprio bilancio annuale, che come in ogni contesto rende il profitto padrone delle scelte.

Molti dei problemi che il nostro paese, l'Italia, deve affrontare ogni anno, sono causati dal modus operandi di soggetti che sembrano sempre meno in grado di ricoprire e gestire le cariche che ricoprono, mandando avanti una gestione del paese poco precisa e con troppi vuoti e contraddizioni. Non è un caso se il termine "all'italiana" viene ironicamente utilizzato per indicare un tipico comportamento leggero e superficiale.

L'Italia è un paese pregno di potenzialità, di storia, di arte e di qualsiasi tecnica che l'uomo abbia appreso nel corso del tempo. La sua guida è però affidata nelle mani di persone che quasi mai sono in grado di sfruttare tali potenzialità nel migliore dei modi, andando a tarpare le ali di questa imponente aquila che freme per spiccare il volo.

Ebbene, se si potesse sciogliere il lazzo che tiene legato questo sapiente rapace, si potrebbe forse raggiungere un risultato molto più alto rispetto al presente. Un modo per liberare il controllo di un paese dalla malagestione, diverso da quello di cambiare i suoi gestori, potrebbe essere quello di permettere a chiunque il controllo, sull'operato di gestori e non. Questo risultato, potrebbe essere raggiunto grazie all'utilizzo di una tecnologia come quella della Blockchain, la prima forma di database realmente democratica.

Indice delle figure:

Bibliografia:

https://coincodex.com/article/24666/solana-tps/

https://it.wikipedia.org/wiki/Problema_dei_generali_bizantini#cite_note-Coulouris_et_al-1

https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/

https://www.chainalysis.com/blog/how-2022-crypto-sanction-designations-affected-crypto-crime/

https://academy.binance.com/it/articles/history-of-blockchain

https://ark-invest.com/articles/analyst-research/bitcoin-myths/

https://amp24.ilsole24ore.com/pagina/AC3eX9S

https://www.climatewatchdata.org/ghg-emissions?breakBy=regions&end_year=2020&start_year=1990

https://ccaf.io/cbnsi/cbeci

https://shorturl.at/bGJVX

https://shorturl.at/fkIY0

https://shorturl.at/fpsyG

https://www.ilsole24ore.com/art/il-mercato-falsi-cresce-ma-aumentano-anche-sequestri-AEhmR2VD

https://www.cnbc.com/2023/08/24/donald-trump-to-be-arrested-in-georgia-live-updates.html#:~:text=Trump%20is%20one%20of%2019,of%20them%20have%20almost%20nothing.%E2%80%9D

https://it.euronews.com/2023/08/29/eletto-presidente-ma-condannato-cosa-accadrebbe-a-trump-evento-senza-precedenti-negli-usa