POLITECNICO DI TORINO

Corso di Laurea Magistrale in Ingegneria della Produzione Industriale e dell'Innovazione Tecnologica

Tesi di Laurea Magistrale

La Blockchain e le sue applicazioni

RELATORE:
Ch.mo Prof.
Danilo Bazzanella

CANDIDATO:
Vincenzo Abruzzese
Matr. S280168

ANNO ACCADEMICO 2020/2021

Indice

Abstract 4
Introduzione 5
Rivoluzione tecnologica nel campo della blockchain 6
Introduzione alla crittografia 8
Che cos'è la crittografia? 8
Firma digitale 11
La funzione Hash 13
Introduzione alla Blockchain 15
Evoluzione della Blockchain 15
Che Cos'è la Blockchain? 18
Problema dei generali Bizantini e Blockchain 18
Caratteristiche della Blockchain 22
Distributed Ledger Technology 22
Come funziona la Blockchain? 24
Proof of Work e Miners 26
Wallet ed esempio di transazione 31
Fork 32
Vantaggi e Svantaggi della Blockchain 34
Protocolli di validazioni, uno sguardo alla Proof of Stake 36
Proof of Work e Proof of Stake a confronto 37
Blockchain: pubblica, privata ed ibrida 39
La Blockchain per il mondo delle criptomonete 40
Smart Contracts 45
Vantaggi degli Smart Contracts 49
Token 49
Not Fungible Tokens 52
Blockchain, una tecnologia dirompente 54
Blockchain, una medicina per tutto? 55
La Blockchain e le altre tecnologie 58
Internet of Things e Blockchain 58
Artificial Intelligence e Blockchain 59
Big Data e Blockchain 60
La Blockchain e le sue applicazioni nei principali settori 62

Blockchain per il settore finanziario 62
Blockchain per le Assicurazioni 64
Blockchain per il Voto elettronico 65
Blockchain per il Settore energetico 67
Blockchain per il settore Farmaceutico 69
Blockchain per la supply chain 70
Blockchain per la pianificazione degli approvvigionamenti e della domanda 70
Gestione dei flussi logistici 72
Gestione della produzione 72
Benefici della Blockchain nella supply chain 74
Conclusioni 75
Bibliografia 76

Indice delle Figure

Figura 1: Processo di cifratura e decifratura simmetrica 9
Figura 2: Processo di cifratura e decifratura asimmetrico 10
Figura 3: Processo di cifratura e decifratura applicando l'algoritmo della firma digitale 12
Figura 4: Esempio illustrativo di un Merkle Tree. 17
Figura 5: Rappresentazione della manomissione del blocco 2 e conseguente incompatibilità con l'hash del blocco successivo 25
Figura 6: Esempio di una catena di blocchi, dove ognuno è collegato a quello successivo mediante codice hash. 25
Figura 7: Schema semplificato del processo di PoW. 28
Figura 8: Esempio di rete decentralizzata Peer to Peer. 30

Indice dei Grafici

Grafico 1: Variazione del prezzo di Bitcoin da ottobre 2013 a settembre 2021 42
Grafico 2: Capitalizzazione del mercato dal 2013 al 2021. 43
Grafico 3: Dimensione della blockchain bitcoin 43
Grafico 4: Implementazione della blockchain (in percentuale) nei diversi settori 55
Grafico 5: Implementazione della blockchain (in percentuale) nei diversi processi 56
Grafico 6: Numero totale di users che utilizzano piattaforme DeFi 63

Abstract

L'obiettivo principale di questa tesi è quello di permettere al lettore di conoscere il funzionamento della tecnologia **Blockchain**. Si porrà attenzione alla crittografia e successivamente ci si soffermerà sui vari strumenti che possono essere utilizzati mediante la blockchain. Si darà uno sguardo più da vicino alle **criptomonete**, gli **smart contracts**, i **tokens** e gli **NFTs**.

Successivamente, sarà fatta un'analisi relativa alle differenti applicazioni della blockchain nei vari settori, da quello bancario a quello farmaceutico. Infine, si porrà l'attenzione alla blockchain applicata nei processi principali della supply chain.

Inoltre, durante le varie fasi si cercherà di analizzare in maniera critica l'utilizzo di questo strumento, evidenziando quanto possa essere utile l'implementazione della blockchain.

Introduzione

Con il passare degli anni, soprattutto nel periodo successivo alla grande crisi finanziaria del 2008, è nata, in alcune parti della società, l'esigenza di cambiare il sistema centrale che attualmente è presente. L'obiettivo fin da subito è stato quello di creare una rete decentralizzata che possa essere funzionale, anche se priva di un ente centrale. Infatti, oggigiorno, grazie alla tecnologia della **Blockchain** ci si allontana sempre di più da organizzazioni o istituzioni centrali. Il raggiungimento di tale obiettivo ha permesso di sfruttare questa tecnologia non solo in ambito finanziario, ma un po' in tutti i campi del nostro sistema economico.

Questa tecnologia, dal grande potenziale, sta apportando riscontri positivi in vari ambiti aziendali, tanto da poterla classificare come tecnologia appartenente all'industria 4.0. Per questo motivo ci sono sempre più aggiornamenti a riguardo e si sente sempre di più la necessità di interfacciarsi a questa nuova tecnologia, che potrà stravolgere completamente il modo di fare impresa e di vivere delle persone.

Rivoluzione tecnologica nel campo della blockchain

La **Blockchain** nel corso degli anni è stata modifica per renderla più efficiente e veloce nel suo utilizzo, grazie all'uso dell'applicazione di nuove logiche e algoritmi. Prima di parlare dell'*evoluzione della blockchain* sarà illustrata la trasformazione della blockchain, partendo dalla blockchain 1.0 arrivando fino alla versione 3.0.

La ***blockchain 1.0*** nasce per le applicazioni di tipo finanziario, infatti, essa viene applicata per gestire quelle che sono le transazioni finanziare delle criptomonete. In particolare, la prima blockchain è stata ideata per permettere lo scambio della famosa criptomoneta Bitcoin; infatti, questa consente di effettuare le transazioni tra le persone che possiedono una determinata moneta e farle depositare all'interno di un wallet.

La ***blockchain 2.0*** si distingue perché risulta avere un linguaggio di programmazione user-friendly e, soprattutto, Turing completo, per poter eseguire qualsiasi algoritmo. Questa flessibilità rende possibile l'impiego della blockchain in ambiti quali la realizzazione di sistemi end-to-end. La blockchain 2.0 estende questa tecnologia a differenti settori, mediante la creazione e lo sviluppo degli **smart contracts**. Inoltre, rientrano nella blockchain 2.0 anche le **decentralized applications (Dapp)**. Le Dapp sono una specie di auto compilazione delle applicazioni già esistenti, senza nessun intervento da parte degli utilizzatori di queste ultime. In questo caso, le applicazioni non si appoggiano su una rete centralizzata, bensì sfruttano la piattaforma blockchain e la rete distribuita, rendendo così le app meno dipendenti da marketplace come Apple Store e Google Play. In questo modo si potrebbero evitare di pagare delle tasse alle piattaforme e un altro beneficio sarebbe che l'utente possa utilizzare le proprie chiavi crittografiche legate alla propria blockchain, invece dei dati personali. Al momento però questa blockchain, non presenta dei protocolli efficienti che ne possano permettere il funzionamento come lo si desidera.

Oggigiorno, si sta introducendo il concetto di ***blockchain 3.0***. L'obiettivo di questo tipo di blockchain è principalmente quello di poter dare la possibilità di far parlare più blockchain tra di loro. Una connessione tra varie blockchain che permette un'interoperatività tra di loro (definita Cross Chain); oppure la creazione di stratificazioni legate a singole blockchain però gestite al di fuori di esse (definita Side chain). Queste soluzioni permetterebbero di creare un network di blockchain che visto

in una diversa prospettiva può apparire come un'unica grande blockchain. Questo concetto sta diventando sempre più importante nei vari campi dove si sta applicando questa tecnologia e permette di migliorare in maniera più efficiente i vari settori che ne fanno utilizzo.

Introduzione alla crittografia

Prima di parlare esclusivamente della blockchain sarebbe utile cercare di capire alcune nozioni base per quanto concerne la crittografia. Che cos'è di fatto la crittografia e quali strumenti vengono utilizzati all'interno di una blockchain, potrebbe essere utile per permettere di capire meglio il funzionamento di quest'ultima più avanti. Le caratteristiche che si andranno ad analizzare, dopo aver fatto un overview generale sulla crittografia, sono:

- la chiave pubblica e privata
- la firma digitale
- la funzione Hash.

Che cos'è la crittografia?

"L'invenzione della crittografia risale a tempi molto antichi, infatti, essa è definita come la branca della crittologica che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo, garantendo, così, in chiave moderna, il requisito di confidenzialità o riservatezza tipico della sicurezza informatica. Un tale messaggio si chiama comunemente crittogramma e i metodi usati sono detti tecniche di cifratura." (Wikipedia. (2021). *Crittografia, Wikipedia, L'enciclopedia libera)*.

Oggigiorno, essa è di fondamentale importanza nel mondo dell'informatica per evitare degli attacchi hacker. Il messaggio che deve essere protetto viene definito come testo in chiaro, mentre quello non comprensibile è il testo cifrato che sarebbe il messaggio in chiaro trasformato, ovvero, che ha subito **l'algoritmo di cifratura**. Questa trasformazione è definita **cifratura** e a sua volta quando si va incontro al processo di trasformazione inversa viene definito processo di **decifratura**.

I simboli di base utilizzati in ambito crittografico sono:

- **P**: che sono un testo in chiaro, essi appartengono allo spazio P definito come spazio dei messaggi in chiaro
- **k**: che sta per key, chiave in italiano
- **pk**: chiave pubblica

- **sk**: chiave privata

In crittografia le chiavi sono generate da un algoritmo **Gen**.

Quando parliamo di chiave privata e chiave pubblica dobbiamo pensare a due chiavi che sono collegate tra di loro, possedute da una stessa persona, dove la prima è pubblica a chiunque e la seconda è privata.

Continuando con la simbologia si hanno:

- **Enc**: algoritmo di cifratura
- **C**: testo cifrato, crittogramma o crittotesto e questi appartengono allo spazio C dei messaggi cifrati.
- **Dec**: algoritmo di decifratura.

L'algoritmo di cifratura consente quindi di trasformare il messaggio chiaro in un messaggio cifrato attraverso una trasformazione di tipo parametrico. Il parametro in questo caso viene chiamato chiave. Quindi, nel momento di decifratura ci sarà bisogno di conoscere sia l'algoritmo che la chiave, la quale ci permette di decifrare.

La crittografia tradizionale si basa su un sistema per cui sia l'azione di cifratura che l'azione di decifratura possono essere fatte con la medesima chiave. In questo caso si parla di **crittografia simmetrica.** Quindi avremo il testo in chiaro che subirà il processo di cifratura attraverso una chiave; successivamente se un secondo interlocutore volesse decifrare quest'ultimo, utilizzerebbe la medesima chiave per poter decifrare il testo e avere il messaggio in chiaro. Schematicamente possiamo riassumerlo come segue:

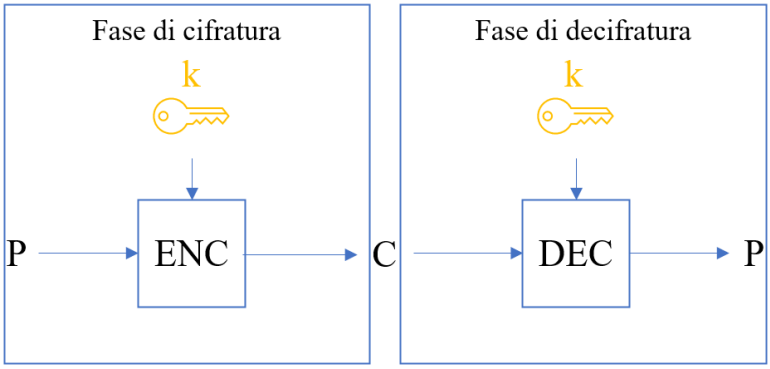

Figura 1: Processo di cifratura e decifratura simmetrica

"Per progettare un cifrario di tipo simmetrico serve f : K -> inv(P,C) dove inj(P,C) è l'insieme di funzioni iniettive f : P -> C. Dunque data una chiave k : $Enc_k := f_k$ e $Dec_k = f_k^{-1}$. Gli algoritmi usati per calolcare F_k da k, quello per cifrare cioè calcolare $f_k(P) = C$ e per decifrare $f_k^{-1}(C) = P$ sono efficienti. Perciò qualcuno che abbia la chiave k può cifrare e decifrare." (Bazzanella, D. (2021). C*orso Crittografia, Politecnico di Torino*).

La crittografia simmetrica è molto efficiente in termini di velocità e di semplicità del processo. Però, il difetto è che servono molte chiavi e soprattutto che queste devono essere scambiate con estrema sicurezza. Per evitare rischi di sicurezza, si utilizza un altro sistema crittografico più sicuro che prende il nome di **crittografia asimmetrica,** essa sfrutta l'utilizzo di due chiavi: la chiave pubblica e quella privata. Questo sistema è meno veloce però non ha bisogno di scambi di chiavi e quindi è più sicuro. In questo modo, quello che viene cifrato sarà fatto attraverso l'utilizzo della chiave pubblica, mentre l'operazione di decifratura avviene solo mediante una chiave privata corrispondente. Questa operazione è realizzabile solo dal proprietario della chiave e ciò garantisce che non ci sia bisogno di comunicazione tra le parti. In basso è presente uno schema di come avviene la fase di cifratura e decifratura mediante la crittografia asimmetrica.

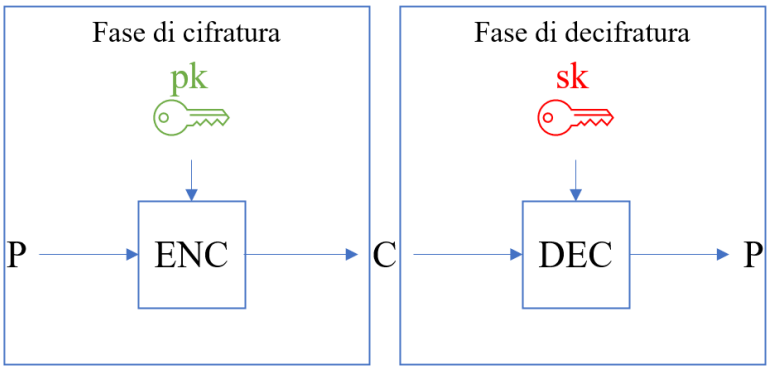

Figura 2: Processo di cifratura e decifratura asimmetrico

A differenza del cifrario simmetrico, nel cifrario asimmetrico ci sono due applicazioni:

- **f** : pubK -> inj(P, C)
- **g** : segk -> maps(C,P)

e coppie (sk, pk) tali che:

$$\boldsymbol{g}_{sk} \, o \, \boldsymbol{f}_{pk} = Id_P$$

Gli algoritmi per calcolare $\boldsymbol{g}_{sk}$ *e* $\boldsymbol{f}_{pk}$ *sono efficienti. Invece non dovrebbe essere computazionalmente fattibile calcolare sk conoscendo pk. cioè l'inversa della funzione* $\boldsymbol{f}_{pk}$ *dovrebbe essere computazionlmente "hard to compute".* (Bazzanella, D. (2021). *Corso Crittografia, Politecnico di Torino*).

Firma digitale

Per consentire gli scambi di informazioni anche all'interno di canali non protetti, la crittografia è un mezzo sicuro che permette la protezione di questi messaggi. Ovviamente però, non è solo importante che il messaggio arrivi integro, ma che esso arrivi dal mittente desiderato. Per poter fare in modo che questo si verifichi si utilizza la firma digitale.

La **Firma digitale** non è altro che una "firma" elettronica basata su un sistema di chiavi asimmetriche a coppia. La coppia è composta da una chiave pubblica e una privata, che tramite un algoritmo consentono di verificare la provenienza e l'integrità di uno o più documenti informatici.

Attraverso la crittografia asimmetrica il passaggio di informazioni tra due persone avviene attraverso l'utilizzo della chiave pubblica per cifrare il messaggio e una chiave privata per decifrare il messaggio. Chiave pubblica e privata di una determinata persona sono collegate tra di loro.

In generale, senza utilizzare la firma digitale, il processo sarebbe molto lineare. Infatti, se considerassimo due persone A e B, dove A vuole inviare un documento a B.

Se A fosse in possesso della chiave pubblica di B, a questo punto, A potrebbe utilizzare la chiave pubblica per cifrare il messaggio che desidera inviare a B.

Dopo che il messaggio è stato inviato a B, quest'ultimo, tramite la sua chiave privata (che è collegata alla sua chiave pubblica) potrà decifrare il messaggio ricevuto da A.

Ciò rende impossibile ad una terza persona di decifrare il messaggio, in quanto è in possesso al massimo solo della chiave pubblica, che è quella utilizzata per il processo di cifratura. Siccome però tutti conoscono la chiave pubblica, allora, tutti possono cifrare e quindi l'identità del mittente nei sistemi a chiave pubblica non è garantito. Per questo

motivo si utilizza un altro sistema, per fare in modo che il messaggio sia protetto e allo stesso tempo si abbia la certezza della provenienza del messaggio.

Nel caso si utilizzasse la firma digitale il processo degli scambi dei dati sarà sicuramente differente. In questo caso la chiave privata è utilizzata per l'azione di cifratura, mentre la pubblica per l'attività di decifratura. In questo modo si riuscirà sicuramente a essere sicuri che un determinato messaggio sia inviato da una determinata persona. Infatti, tornando all'esempio, se considerassimo sempre due persone A e B, con A colui che vuole inviare un messaggio a B, in questo caso si verificherebbe un processo differente:

A, attraverso la propria chiave privata, cifra il messaggio che vuole inviare a B (questo è il momento in cui avviene la firma digitale da parte del mittente) e successivamente cifra ulteriormente il messaggio utilizzando la chiave pubblica di B.

Nel momento in cui B voglia leggere il messaggio, dovrà decifrarlo. Allora B utilizzerà la sua chiave privata per decifrare il messaggio cifrato da A (dove A aveva utilizzato la chiave pubblica di B) e successivamente avverrà un secondo processo di decifratura, dove B utilizzerà la chiave pubblica di A (per decifrare il messaggio che A aveva cifrato inizialmente con la sua chiave privata).

In questo modo si ha la sicurezza che il messaggio è cifrato agli occhi di persone esterne e sicuri che esso sia firmato da una persona precisa, in quanto ha utilizzato la propria chiave privata a monte del processo di cifratura. Di seguito è presente un'illustrazione schematica del processo che rende più facile e comprensibile il passaggio di informazioni mediante questa logica.

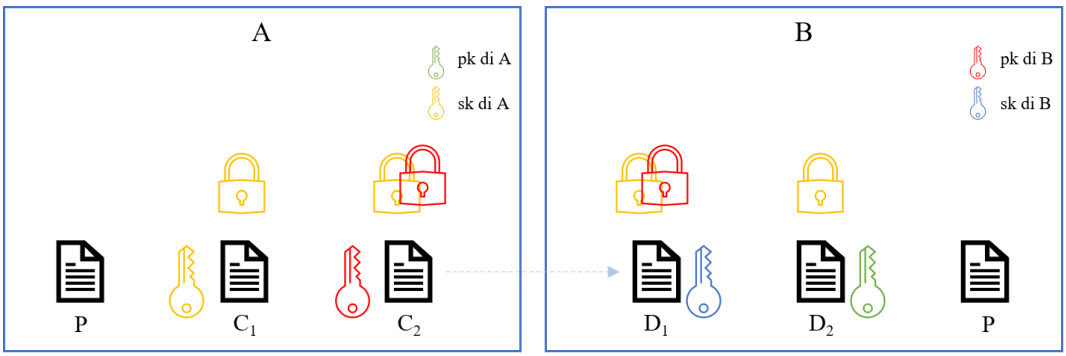

Figura 3: Processo di cifratura e decifratura applicando l'algoritmo della firma digitale

La funzione Hash

Nel campo informatico e matematico la funzione **Hash** rientra in quelle funzioni di tipo non invertibili. Essa è capace di trasformare un messaggio di lunghezza arbitraria in un codice alfanumerico di lunghezza prefissata, detto **digest**. La parola Hash in italiano è traducibile come impronta, infatti da qui si può intendere come una procedura volta alla trasformazione di un messaggio in un codice corrispondente.

Definito con $\sum$ l'alfabeto e $\sum^*$ l'insieme di tutte le parole (di lunghezza arbitraria) ottenibili da $\sum$, si definisce funzione Hash, una funzione h: $\sum^* \rightarrow \sum$ n, con n fissato. Nei calcolatori avendo la relazione $\sum = \{0,1\}$ ha senso fissare n, che sarebbe la lunghezza del digest, con un multiplo di 8 bit, facendo assumere ad n un valore di solito uguale a 160, 256, 384 e 512 bit. A causa del fatto che il dominio della funzione Hash è uno spazio più grande dello spazio immagine, la funzione non potrà essere iniettiva; dunque esistono più coppie (a,b) tali che $h(a)=h(b)$. In crittografia è fondamentale che queste inevitabili collisioni siano difficili da determinare.

Data una funzione $h(x)$, è fortemente priva di collisioni se determinare una qualsiasi collisione (a,b) è un problema computazionalmente intrattabile. Se questo non si verificasse, allora la funzione Hash dovrà essere debolmente priva di collisioni per avere un utilizzo crittografico; In questo caso, una funzione $h(x)$, è debolmente priva di collisioni se $a \in \sum^*$ fissato, determinare b tale che $h(a)=h(b)$ è un problema computazionalmente intrattabile. (Bazzanella, D. (2021). *Strumenti, Slide del corso Blockchain e criptoeconomia, Politecnico di Torino.)*

Le caratteristiche che rendono la funzione Hash di fondamentale importanza nel mondo della crittografia sono *l'unidirezionalità e l'effetto valanga*.

Per quanto riguarda *l'unidirezionalità*, una funzione $h(x)$ è definita tale se, data un'impronta z, è un problema computazionalmente intrattabile ricavare $x / h(x) = z$. Allora si può definire una funzione unidirezionale nel momento in cui si è in grado di calcolare la funzione $h(x)$ in tempo polinomiale ed al contempo non è noto nessun algoritmo polinomiale che sia capace di calcolare la contro immagine di $h(x)$, ovvero $h^{-1}(x)$, a meno di una probabilità trascurabile. In questo modo, il sistema è reso molto sicuro.

Per quanto concerne *l'effetto valanga;* la funzione Hash, cambiando anche solo un carattere o un valore in input, genererà un output completamente differente. Questo consente di complicare enormemente il lavoro di malintenzionati che cambiando i dati in input, genererebbero un output differente che tutti potrebbero scoprire.

Introduzione alla Blockchain

Spesse volte la blockchain viene collegata alle criptomonete come se fossero la stessa cosa, ma effettivamente sono due cose completamente diverse. Ogni blockchain ha la sua criptomoneta, ma non è detto che la funzione principale di ogni blockchain sia solo quello di trasferire in sicurezza le criptomonete da un utente all'altro. La blockchain offre più applicazioni dei semplici trasferimenti di valore.

In questi ultimi anni, la tecnologia blockchain, ha dimostrato la sua funzionalità come mezzo efficiente nello scambio di valore, ma è diventato anche molto di più con interessanti applicazioni da quelle mediche a quelle del settore industriale. Infatti, la blockchain sta influendo su diversi modelli di business andando a creare nuovi prodotti e servizi grazie alla sua nuova logica di funzionamento. Ciò che la caratterizza e la presenta come un sistema realmente funzionale è quello di essere un registro condiviso che la rende immutabile. È possibile attaccare un utente e cambiare la sua copia della blockchain ma è sostanzialmente impossibile attaccare migliaia o milioni di utenti e cambiare a tutti i dati della blockchain. Questo rende il sistema più resiliente agli attacchi, molto di più dei sistemi centralizzati.

Evoluzione della Blockchain

Nonostante la blockchain sia una delle tecnologie più innovative di quest'ultimo secolo, si può far risalire il concetto di blockchain al comune "libro mastro" che risale circa al periodo tra il 1300-1400. La peculiarità di questo strumento già in quegli anni, era quella di essere un "registro contabile dove riunire tutti i conti in dare e avere, definiti mastrini, che compongono un dato sistema contabile". (Wikipedia (2020). *Libro mastro, Wikipedia, L'enciclopedia libera*).

Con gli anni, i libri contabili hanno avuto sempre più rilievo all'interno della società fino a diventare uno strumento di obbligo per le attività imprenditoriali. Con il tempo, questo libro si è cercato di digitalizzarlo per evitare problemi fisici o facili manomissioni da parte delle persone. Oggigiorno, si può parlare di Blockchain come nuovo libro mastro del XXI secolo.

L’evoluzione di questa tecnologia innovativa che ha inizio durante la fine del XX secolo è riassumibile in tre passaggi: timestamp, Merkle trees e infine il periodo inerente al lancio della conosciuta blockchain bitcoin.

Una prima applicazione della blockchain avviene durante i primi anni ‘90 con Stuart Haber e Scott Stornetta. Il loro obiettivo era creare una marcatura temporale per i documenti digitali che potesse assicurarne l’autenticità. L’uso di questa tecnologia aveva la necessità di superare due questioni fondamentali. La prima era quella di fare in modo che i dati fossero contrassegnati con l’ora esatta e la seconda che il calendario non potesse essere modificato.

La soluzione definita dai due intellettuali era il ***naive*** che consisteva nell’utilizzare una digital safety deposit box. Ciò vuol dire che ogni momento in cui un client ha un file che deve essere contrassegnato con data e ora, esso trasmette il documento ad un servizio di marcatura temporale che registra la data e il momento in cui il documento stesso è stato ricevuto, conservandone anche una copia. Già in questa fase, ogni qualvolta l’integrità del documento del client viene messa in discussione, essa sarà confrontata alla copia archiviata dal timestamp. Nel momento in cui questi documenti sono uguali, allora, il documento si può definire integro, privo di manomissione.

Questa metodologia aveva delle criticità che erano legate principalmente alla privacy e alla difficoltà di archiviare dati, in quanto il tempo richiesto era in funzione della grandezza del documento stesso; quindi, per i documenti di grandi dimensioni sarebbe stata difficile l’archiviazione.

Dopo aver incontrato queste difficoltà, i due formularono un’idea alternativa, ovvero quella di utilizzare un algoritmo di hashing crittografico, producente un ID univoco per il documento. In questo modo un client invia il suo valore hash anziché il documento; così da poter risolvere entrambe le criticità, quella legata alla dimensione del documento e quella riguardo la privacy.

La seconda applicazione è quella del Merkle Tree. Questa idea è nata nel 1992 da parte di Dave Bayer, riprendendo quella che è la struttura già ideata da Haber e Stornetta. Merkle Tree, dall’anglosassone alberi di Merkle, l’obiettivo era raccogliere più documenti possibili all’interno di blocchi. L’albero è composto da nodi foglia, ognuno

contenente informazioni ed etichettati con il digest risultante dalla Hash dei dati che sono contenuti in esso. Invece, i nodi padre sono etichettati con il digest della Hash calcolati sulla concentrazione di etichette dei propri nodi figli. I nodi padre a loro volta sono collegati ad un nodo radice, chiamato radice di Merkle. Questo strumento avrebbe potuto permettere un'efficiente e sicura verifica delle informazioni che sono presenti all'interno dei blocchi.

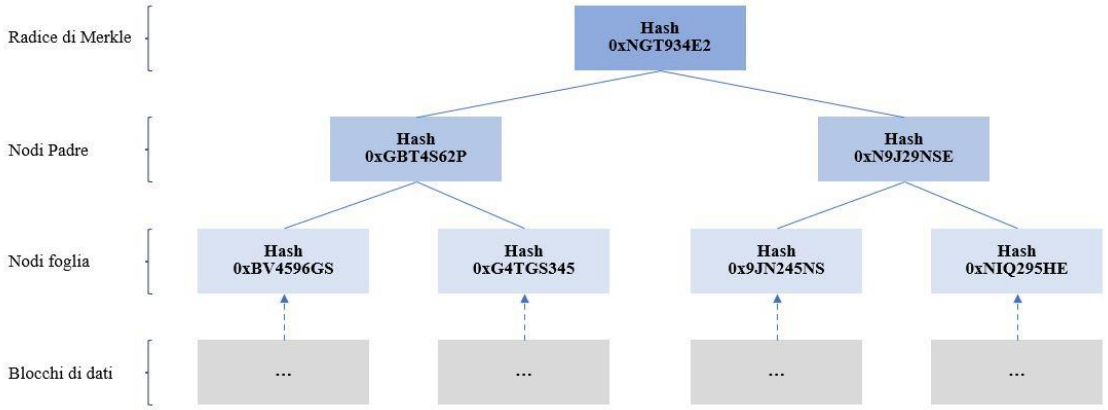

Figura 4: Esempio illustrativo di un Merkle Tree.

Il vantaggio principale del Merkle Tree è che, quando i dati all'interno di un nodo cambiano, non è necessario ricalcolare le Hash di tutti gli altri nodi, ma solo le Hash dei nodi lungo il ramo che collega il nodo foglia a quello radice.

L'ultima applicazione più rivoluzionaria che ha portato la blockchain ad essere conosciuta a tutto il mondo è stata attraverso la famosissima criptomoneta Bitcoin. Si dà a Satoshi Nakamoto il riconoscimento per aver introdotto nel 2008 la prima blockchain come la si conosce oggi. Nel 2009 viene implementata con l'obiettivo di essere un libro mastro per registrare tutte le transazioni dei Bitcoin. Scambi che avvenivano tra le persone in qualsiasi parte del mondo.

Dopo la crisi finanziaria del 2008, Satoshi Nakamoto decise di provare a decentralizzare il sistema delle transazioni, facendo in modo che ci fosse meno controllo da parte delle banche. Il codice di valuta del Bitcoin è BTC o XBT e viene utilizzato per essere riconosciuto nel mercato. Per fare in modo che funzioni al meglio la blockchain, Nakamoto ha dovuto prevedere una serie di regole per garantire e mantenerne l'integrità e la sicurezza dei dati durante le transazioni, assicurando la privacy alle persone. Il principale obiettivo della blockchain era quello di eliminare gli intermediari creando un

sistema completamente sicuro. In particolare, era di fondamentale importanza, evitare il fenomeno di **double-spending**, ovvero, il problema che potrebbe verificarsi nel momento in cui un individuo ha la possibilità di spendere più volte lo stesso valore della stessa moneta, pur non avendo quel valore, in quanto era stato precedentemente speso. Questo problema è stato superato introducendo un sistema che potesse permettere alle persone di creare un network. Attraverso questo network è consentito a chiunque di controllare le transazioni.

Che Cos'è la Blockchain?

"La **blockchain** (letteralmente "catena di blocchi") è una struttura dati condivisa ed "immutabile". È definita come un registro digitale le cui voci sono raggruppate in "blocchi" concatenati in ordine cronologico, e la cui integrità è garantita dall'uso della crittografia. Sebbene la sua dimensione sia destinata a crescere nel tempo, essa è immutabile, in quanto, il suo contenuto una volta scritto non è più né modificabile né eliminabile, a meno di non invalidare l'intera struttura." (Wikipedia. (2021) *Blockchain, Wikipedia, L'enciclopedia libera*).

La blockchain, come precedentemente scritto, non è altro che un libro mastro decentralizzato che utilizza la crittografia per far avvenire delle transazioni; la cosa più interessante è che essa permette di far scambiare alle persone non solo più delle informazioni ma anche delle proprietà. L'obiettivo di quest'ultima è stato eliminare un'autorità centrale, creando così una rete tra persone che non si conoscono e non hanno nessun motivo di fidarsi l'uno dell'altro, permettendo transazioni che siano sicure senza l'esistenza di un garante. Il libro mastro è distribuito tra più persone e condiviso da tutti i soggetti che agiscono all'interno di una determinata rete di computer che è basata su delle tecnologie; al momento, la più comune e funzionale è la blockchain che si basa sulla tecnologia peer-to-peer.

Problema dei generali Bizantini e Blockchain

Come è stato già scritto precedentemente, l'intento di Satoshi Nakamoto era di decentralizzare il sistema finanziario attraverso la tecnologia della blockchain. L'eliminazione di queste figure centrali, che permettono l'effettuazione delle transazioni in maniera sicura, richiede un livello di intervento e collaborazione tra le parti per

validare le transazioni all'interno della rete. Si può dire che Nakamoto è riuscito ad applicare al sistema blockchain l'algoritmo risolutivo di uno dei problemi più conosciuti in ambito delle comunicazioni, il **problema dei Bizantini. "**Il problema in esame considera due eserciti che sono guidati da due generali A1 e A2. Loro vogliono attaccare una città che si trova nel mezzo dei loro territori. I generali A1 e A2 possono scambiarsi informazioni solo inviandosi lettere l'uno con l'altro, ma c'è un problema; il messaggero deve passare attraverso la città, il che rende possibile la sua cattura e quindi il messaggio potrebbe non arrivare o arrivare modificato. I generali A1 e A2 devono accordarsi sull'assalto alla città in modo da agire in contemporanea, che è l'unico modo per vincere; quindi, devono ottenere un consenso sull'orario dell'attacco." (Bazzanella, D. (2021). *Introduzione alla Blockchain).*

Questo problema fa intendere che il generale A1 potrebbe comunicare al generale A2, tramite il messaggero, l'ora e il giorno dell'attacco, però il generale A1 non sa se il messaggio arriva correttamente.

In questo modo A2, una volta ricevuto il messaggio, può dare conferma ad A1 che l'informazione gli è arrivata, ma in quel momento A2 non sa se il generale A1 abbia ricevuto il messaggio e così via.

Ciò mette in risalto che, nonostante ci siano più round di conferma che si prevedono, non ci sarà mai la possibilità per entrambi i generali di sapere che il messaggio sia arrivato all'altro, non permettendo così l'assalto combinato alla città che si desidera attaccare. Dunque, il problema diviene un paradosso, in quanto ci può essere un fitto scambio di informazioni, ma non si arriva mai ad una conclusione, in quanto l'ultimo che invia il messaggio si troverà in una posizione di incertezza. Questo problema ci permette di capire che in un ambiente in cui ci sono le comunicazioni, è impossibile garantire l'accordo tra le due parti.

Successivamente questo problema è stato generalizzato. La generalizzazione del problema è stata proposta da tre informatici Leslie Lamport, Robert Shostak e Marshall Pease nel rapporto dal titolo The Byzantine Generals Problem (BGP) nel 1982. Il problema, dei generali bizantini, descrive un gruppo di generali dell'esercito bizantino che assedia una città. I generali possono scambiarsi informazioni per raggiungere un accordo sul piano da attuare per attaccare la città. Nel caso più semplice, devono solo

concordare se attaccare o ritirarsi. Alcuni potrebbero voler attaccare, ma altri potrebbero voler ritirarsi, e il problema è che se non attaccassero tutti insieme, fallirebbero.

Si supponga che i generali si possano scrivere tra di loro e che ci possano essere dei generali traditori. In questo modo diviene tutto più complicato, perché il messaggero potrebbe essere catturato e il messaggio inviato potrebbe essere falso. Proprio in questo caso si può intravedere la relazione tra il BGP e la blockchain, infatti, si ha un problema di raggiungimento di consenso tra più persone, supponendo che non ci sia onestà in una parte di loro.

In questo caso si verificherebbe che se ci fosse anche solo un traditore tra i generali o i messaggeri, potrebbe accadere che una parte dei generali non deciderà di attaccare la città, mentre una parte si. Ad esempio, si considerino cinque generali di cui: due vogliono attaccare, due non vogliono attaccare e uno è un traditore.

Nel momento in cui il messaggio del traditore arrivi ai due generali che vogliono attaccare, quei due riceveranno un messaggio che la maggioranza non vuole attaccare e quindi non attaccheranno.

Invece, i due villaggi che non volevano attaccare si trovano ad attaccare in quanto ricevono un messaggio che la maggioranza vuole attaccare.

In questo modo il problema si complica molto perché ci sono difficoltà non solo legate alla comunicazione tra le parti ma anche alla veridicità del messaggio.

Lamport, Shostak e Pease, però, sono riusciti a trovare una soluzione ideando l'algoritmo Oral message (OM), per risolvere il problema. Per far sì che l'algoritmo funzioni ci sono tre vincoli che devono essere considerati:

- Qualunque messaggio che viene inviato sarà consegnato al destinatario corretto;
- Il destinatario sarà a conoscenza di chi riceve il messaggio stesso;
- Si può essere a conoscenza di chi non invia il messaggio.

Da ciò deriva il **Teorema** dimostrato da loro, che dice: sia m il numero di traditori, l'algoritmo OM (m) può raggiungere un consenso se ci sono più di 3 m generali totali. Ergo, l'algoritmo ha senso nel momento in cui due terzi della popolazione sia leale.

Da questo teorema nasce la Byzantine Fault Tolerance (BFT) che è la proprietà che un qualsiasi sistema ha per evitare di cedere ai fallimenti derivanti dal problema dei Generali Bizantini. Successivamente, alla fine degli anni '90, è stato introdotto l'algoritmo Pratical Byzantine Fault Tolerance (PBFT) che è in grado di gestire migliaia di richieste al secondo con una latenza molto bassa. Con l'introduzione della PBFT sono stati inseriti molti altri protocolli simili, con delle migliorie rispetto al protocollo BFT, per perfezionare le comunicazioni tra sistemi comunicativi.

Come è stato precedentemente descritto il problema dei Bizantini fa sì che ci sia una relazione con la blockchain in quanto traspare la problematica inerente all'onestà della comunicazione; difatti, è proprio questo il punto più delicato e attaccabile di una blockchain pubblica, in quanto potrebbero essere inseriti dei blocchi di transazioni falsi e fraudolenti. Ciò descrive la criticità di un sistema decentralizzato.

La blockchain per questo motivo supera questa criticità attraverso un meccanismo di consenso che è stato introdotto da parte di Satoshi Nakamoto, dove ogni attore deve concordare l'autenticità di una transazione trasmessa a discapito della respinta, nel caso di contrarietà del sistema. Questa metodologia è utilizzata come soluzione al problema dei generali bizantini e prende il nome di Proof-of-Work (PoW).

La soluzione di Nakamoto nel problema dei generali Bizantini era che ogni generale potesse proporre un suo tempo di attacco. Quando ogni generale riceve una proposta di orario, si avvia quello che è un processo di PoW facendo "hash" di un testo dove è presente l'ora dell'attacco. È importante inserire qui la variabile tempo, ovvero che tutta la rete dei generali impiega al massimo 10 minuti a risolvere la PoW. Dal momento che uno dei generali conclude quest'ultima con successo, lui trasmetterà l'hash ottenuto alla rete e tutti cambiano il calcolo della propria PoW, includendo tale hash e tale orario nella PoW su cui stanno lavorando. Ogni 10 minuti si avrà che la catena sarà più lunga e, essendo tutto pubblico, ad un certo punto, tutti i generali sono consapevoli che ci sarà un orario di attacco su cui la maggioranza sarà d'accordo. Quindi potranno attaccare con sicurezza, con un orario concordato. Più avanti si vedrà nello specifico il funzionamento della PoW all'interno della blockchain.

Caratteristiche della Blockchain

Le principali caratteristiche di una blockchain, che permettono il suo corretto funzionamento, sono:

- **Nodi:** i nodi sono tutti gli utenti della rete, collegati tra di loro pear-to-pear.
- **Transazioni:** sono i singoli dati che sono inseriti nei blocchi della blockchain.
- **Blocchi:** sono l'insieme di più transazioni che vengono verificate e approvate per parte dei partecipanti alla rete.
- **Ledger o registro:** è un registro in cui sono presenti i vari dettagli delle varie transazioni. Le transazioni sono presenti sequenzialmente e sono immutabili, garantendo trasparenza. In ogni registro è presente la sequenza di blocchi concatenati tra loro mediante un codice, chiamato codice Hash.
- **Codice Hash:** è una sequenza alfanumerica, ottenuta applicando un particolare algoritmo di calcolo alla sequenza di bit che formano il testo o il file.

Distributed Ledger Technology

La blockchain è una particolare tecnologia che rientra in quelli che sono i sistemi **Distributed Ledger Technology** (DLT), in italiano database distribuito. Questa tecnologia dà la possibilità di decentralizzare il sistema facendo in modo che non ci sia necessità di un ente garante e centrale come, ad esempio, una banca nel caso di transazioni monetarie. Alcune volte si fa confusione pensando che blockchain e DLT siano la stessa cosa, invece, la blockchain è una tipologia di DLT. Ritornando al concetto del "libro mastro", il DLT permette che ogni nodo ha una copia di quest'ultimo e quindi delle transazioni, così da far avvenire la duplicazione dei dati da archiviare tra i diversi nodi della rete. Quindi è come se il "libro mastro" fosse condiviso da più parti contemporaneamente e ciò permette di evitare problemi come:

- Possibili **furti**, in quanto chiunque potrebbe rubare dei documenti cancellandoli o falsificandoli.
- **Fattore umano**, in quanto è possibile sbagliare, per esempio la scrittura del valore di una transazione.
- **Fattori fisici**, in quanto un libro mastro fisico può essere distrutto per fattori naturali o addirittura perso.

Una DLT permette di avere due caratteristiche fondamentali che sono intrinseche anche all'interno della blockchain, che sarebbero:

- **Trasparenza e immutabilità:** tutti i nodi godono di pari diritti sui dati; in questo caso tutte le decisioni vengono prese in maniera collettiva. In questo senso la DLT riesce a fornire una traccia di controllo immutabile e verificabile.
- **Resistenza agli attacchi:** questa tecnologia fa in modo che il sistema sia impenetrabile da parte di attacchi informatici rispetto ad un qualunque database centralizzato tradizionale, questo perché è distribuito. Quindi, per poter hackerare, modificando i dati e facendo in modo che quei dati modificati siano "veritieri", ci sarebbe bisogno di un dispendio di risorse troppo elevato; maggiore di quello che potenzialmente si riuscirebbe a rubare, il che rende il sistema difficilmente hackerabile.

Come è stato già detto la blockchain è un tipo specifico di DLT che si differenzia dalle altre tipologie, in quanto i dati sono salvati non in un unico file ma presenti in più blocchi che sono collegati l'uno all'altro in una catena. In genere, le azioni che possono essere fatte in una qualunque DLT sono:

- **Create:** che permette la creazione di una determinata informazione;
- **Retrive:** che permette la possibilità di recuperare una determinata informazione;
- **Update:** che permette l'aggiornamento di tale informazione;
- **Delete:** che permette l'eliminazione dell'informazione.

Nel caso specifico della blockchain, per fare in modo che ci sia integrità di dati e che i dati non siano modificabili, ci sono solo due operazioni, che sono quella di **Create** e quella di **Retrive**. La blockchain, quindi tenderà sempre ad espandersi in quanto non è presente la possibilità di eliminare dati al suo interno. Essa può essere vista come una lista di transazioni, per meglio definirla, una serie di blocchi di dati collegati tra di loro; ogni blocco è collegato al blocco precedente e questi blocchi sono in possesso di tutti gli utenti che sono collegati tra di loro in una rete **peer-to-peer**.

Concludendo con la funzionalità di DLT, si può dire che quest'ultima è un concetto architetturale di tipo peer-to-peer decentralizzata, dove ogni partecipante sarà in possesso di una copia dei dati che ha tutto il resto della rete. Proprio grazie a questa

architettura, dove ognuno ha il registro con le transazioni uguale agli altri, permette di rendere sicura la blockchain.

Utilizzando questa logica, la blockchain diviene una struttura difficilmente attaccabile poiché si avrebbe la necessità di attaccare nello stesso momento più del 50% dei nodi che hanno il registro condiviso, compromettendone i dati. Questa peculiarità, ovvero che è difficilmente attaccabile, non si potrebbe ottenere se tutti i dati fossero concentrati nelle mani di un'autorità centrale. D'altro canto, la garanzia che dà l'autorità centrale è soprattutto quella legata alla privacy, che purtroppo la DLT non la garantisce ma è risolvibile mediante l'utilizzo della crittografia.

Come funziona la Blockchain?

Una blockchain è una catena di blocchi, ogni blocco è costituito da sette elementi:

- **Dati memorizzati**: dove al proprio interno ci sono gli oggetti che vengono memorizzati nel blocco stesso. Ovviamente, i dati sono affini a ciò che la blockchain permette di scambiare. Ad esempio, la blockchain che riguarda una determinata criptomoneta ha al suo interno dati inerenti alla transazione di quest'ultima, come: la quantità che si sta scambiando, il mittente e il destinatario.
- **Hash**: è una stringa contenente un codice alfanumerico, calcolato attraverso un algoritmo specifico, di un determinato blocco. Come detto precedentemente ha due caratteristiche, *l'unidirezionalità e l'effetto valanga,* le quali permettono ad ogni blocco di avere un codice Hash diverso e specifico in funzione dei dati dei blocchi stessi. La cosa fondamentale è che se cambiasse qualche dato all'interno del blocco, si modificherebbe anche il codice Hash del blocco stesso generando un'incongruenza con gli altri blocchi della catena.

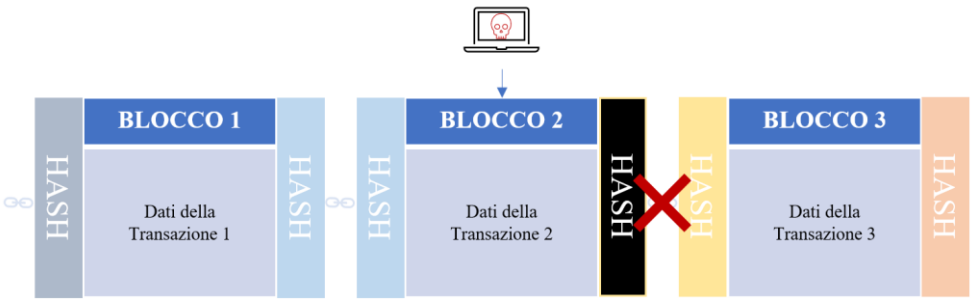

Figura 5: Rappresentazione della manomissione del blocco 2 e conseguente incompatibilità con l'hash del blocco successivo

- **Prev. Hash (Hash del blocco precedente)**: Corrisponde al codice hash del blocco precedente ed è utilizzato per fare in modo che ci sia corrispondenza tra il nuovo blocco e il blocco precedente.
- **Merkle root:** Corrisponde al digest risultante dall'Hash di tutti gli Hash delle varie transazioni presenti nel blocco.
- **Timestamp:** Corrisponde alla marcatura temporale della transazione più recente tra quelle inserite nel blocco.
- **Bits:** Valore della creazione e validazione del blocco, corrispondente alla soglia massima di accettabilità del valore del digest del blocco.
- **Nonce:** Valore che fa in modo che il digest del blocco sia minore del valore riportato nel campo Bits.

Di seguito è presente un esempio dove si possono vedere i vari blocchi, contenenti ognuno più transazioni, e ogni blocco possiede due hash.

Quello a sinistra, è il prev. Hash, riferito all'Hash del blocco precedente, mentre quello a destra è l'hash del blocco stesso generato per quell'insieme di transazioni che, a sua volta, sarà il collegamento per il blocco successivo.

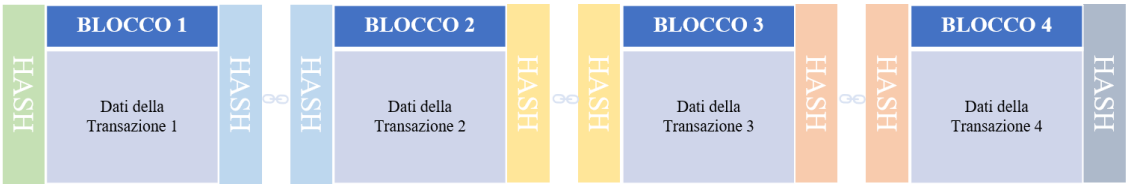

Figura 6: Esempio di una catena di blocchi, dove ognuno è collegato a quello successivo mediante codice hash.

L'interazione di questa procedura garantisce l'integrità del blocco precedente che a sua volta sarà collegato ad un altro blocco che a sua volta è collegato a quello prima fino ad arrivare al genesis block. Termine che deriva dall'anglosassone, la traduzione è blocco

genesi, ovvero il primo blocco della blockchain. Questo sistema darà la possibilità di avere un ordine cronologico dei blocchi risolvendo in parte anche il problema di double spending.

Proof of Work e Miners

Il codice Hash rende il sistema immutabile e resiliente agli attacchi, ma il punto debole è l'inserimento di nuovi blocchi. Serve un accordo di tutta la rete per poter stabilire che blocco inseriranno tutti nella loro copia della blockchain; per questo motivo serve un protocollo di consenso. Chiunque potrebbe aggiungere un nuovo blocco considerando quello precedente. Inoltre, sarebbe importante vedere come si possa bypassare completamente il problema del double spending in una rete decentralizzata.

Il double spending, si ricorda essere un problema legato agli scambi di beni digitali; infatti, il problema non sussiste se si parlasse di beni fisici. Tutti attraverso internet possiamo passare un'informazione a chiunque più volte. Il problema nasce nel momento in cui quello stesso oggetto abbia un valore che deve essere mantenuto e che deve essere scambiato per qualcos'altro. Allora, la soluzione è quella di fare in modo che ciò non possa accadere, ovvero che delle informazioni siano uniche e nel momento che si scambiano non le si possiedono più.

Già Wei Dai aveva proposto una soluzione che successivamente fu implementata da Adam Back, la quale si basava sul rendere pubblica ogni transazione effettuata e legarla ad un marchio temporale, così che tutti potessero risalire alla storia delle transazioni che erano state fatte. Tale compito era affidato al Timestamp, che inseriva data, ora e pubblicazione di un determinato blocco. Però, sapere la data e l'ora non era sufficiente. Questo perché sfruttando la latenza, i computer, in particolare quelli odierni (aventi una grande potenza di calcolo) potrebbero pubblicare centinaia e centinaia di transazioni nello stesso momento e i vari nodi della rete potrebbero riceverle in ordine differente, tutti con la stessa data. In questo modo, coloro che hanno la funzione di validare il blocco si troverebbero impossibilitati allo svolgimento della propria funzione. L'unica soluzione è quindi quella di limitare la possibilità ad ogni computer di pubblicare informazioni, inserendo nuovi blocchi di transazioni alla catena.

Questo requisito si otterrebbe mediante la **Proof-of-Work (PoW)**, un protocollo crittografico il cui significato letterale nella lingua italiana è prova di lavoro. Tale sistema è la richiesta di nuovi calcoli aggiuntivi necessari per rallentare la creazione di nuovi blocchi della catena, così da rendere più complicati eventuali attacchi hacker. Questo sistema viene fuori dalla risoluzione *del problema dei Generali Bizantini* da parte di *Satoshi Nakamoto*. C'è bisogno di un tempo t, in funzione della tipologia di blockchain, per calcolare la PoW e aggiungere successivamente un nuovo blocco alla catena. La PoW ha bisogno di essere svolta mediante calcoli. L'obiettivo è quello di avviare un test, mediante processo di ricerca casuale ed iterativo per l'intero contenuto dell'insieme delle soluzioni possibili, fino a giungere a quella soddisfacente per il sistema.

Nel caso della blockchain Bitcoin, è utilizzata la funzione Hash, che grazie alle caratteristiche di unidirezionalità ed effetto valanga che essa possiede, genera un problema difficile da risolvere e con tempi di risoluzione non immediati. Nel caso della blockchain Bitcoin la PoW consiste nel trovare un **nonce** che inserito nel blocco rende la hash dell'intero blocco minore di un certo valore fissato S^{217}. Si può concludere quindi che dato un blocco *B*, dove sono stati fissati tutti i campi ad eccezione del nonce, inserendo un valore x di dimensione pari a 32 bit, allora la PoW è risolta nel momento cui è valida la seguente disuguaglianza: $x / Hash(B(x)) \leq S$ *(dove S è un numero a 256 bit ovvero delle stesse dimensioni in bit del digest della funzione Hash).*

Il processo con cui viene svolta la PoW è quindi il seguente:

1. Si seleziona un numero casuale (nonce)
2. Si esegue la funzione Hash SHA-256 del blocco, contenente il nonce e al risultato, che sarebbe il digest, si riapplica la funzione: $Hash(B) = SHA256^2(B)$
3. Successivamente viene verificato se il valore rispetti il vincolo tale che $SHA256^2(B) \leq S$
4. Se questa disequazione fosse corretta, allora il blocco verrebbe validato; se tale disequazione non fosse soddisfatta, a quel punto ci sarebbe bisogno di cambiare il nonce fin quando non si raggiungono le condizioni desiderate (es. quella che il codice abbia un numero preciso di zeri all'inizio della stringa).

Quindi, per convalidare un nuovo blocco, il sistema calcolerà le varie soluzioni in funzione del valore Hash del blocco precedente, delle informazioni presenti all'interno del blocco stesso e del valore del nonce che sarà generato. Questo processo si ripeterà fin quando non si raggiungerà il valore desiderato. In basso è presente uno schema semplificato del processo:

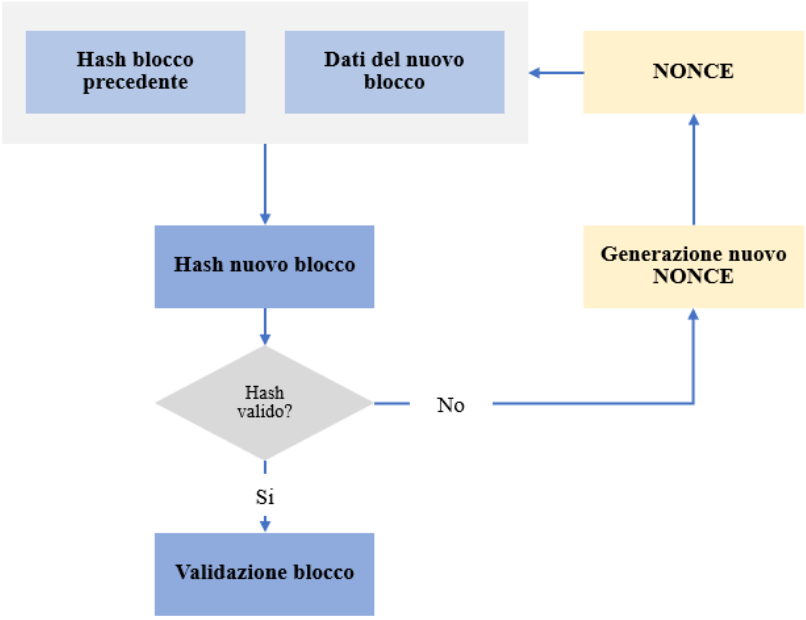

Figura 7: Schema semplificato del processo di PoW.

Nel momento in cui si raggiungerà il valore desiderato, verrà validato il blocco trasmettendolo alla rete, il quale sarà accettato come blocco successivo all'interno della blockchain.

Si può così intuire che ogni blocco è collegato l'uno con l'altro attraverso l'hash che viene calcolato. Quest'ultimo rende sicura la catena di blocchi in quanto se un malintenzionato volesse manomettere un blocco di transazioni, si modificherebbe automaticamente l'hash del blocco generandosi così l'incompatibilità con il resto della catena.

L'operazione di verifica, ovvero la PoW, è svolta da alcuni nodi della rete, che sono i cosiddetti **miners**. I calcoli computazionali, per essere svolti, hanno bisogno di processori CPU o GPU, i quali impiegano più potenza di calcolo possibile per poter validare i blocchi di transazioni in cambio di una ricompensa. Il sistema Hardware, quindi, avrà bisogno di molta energia, sia per poter tenere accese le unità di calcolo sia

perché c'è bisogno di un sistema di raffreddamento tale che possa permettere ai processori di lavorare alle giuste temperature.

Alcune volte, si potrebbe verificare che alcuni nodi validano quasi contemporaneamente un blocco con caratteristiche differenti e quindi con codice hash diverso. Se ciò si verificasse, avverrebbe una fork momentanea. Ovvero, la catena di blocchi si dirama in due parti, dove su entrambi i rami sono presenti gli ultimi due blocchi aggiunti in "contemporanea".

Successivamente, i miners sceglieranno su quale ramificazione lavorare per validare gli altri blocchi. Quindi, ognuno di loro proverà a svolgere la PoW in funzione del ramo che scelgono.

In seguito, nel momento in cui un miner validerà un nuovo blocco su una delle due ramificazioni, tutti i miners (di solito) migreranno su quel ramo, in quanto sarà quello che ha maggiori probabilità di divenire la catena definitiva.

Ciò provocherà la generazione di un blocco orfano, il quale non permetterà di generare la ricompensa per il miner che lo aveva calcolato.

Ogni persona può unirsi a questo network, diventando esso stesso un nodo del sistema, in modo da rendere il sistema decentralizzato; infatti, questa tipologia di sistema è definita **Peer to Peer**. Ogni persona, in questo modo, riceverà una copia completa del ledger e potrà verificare che effettivamente tutto sia corretto, come si vede in figura.

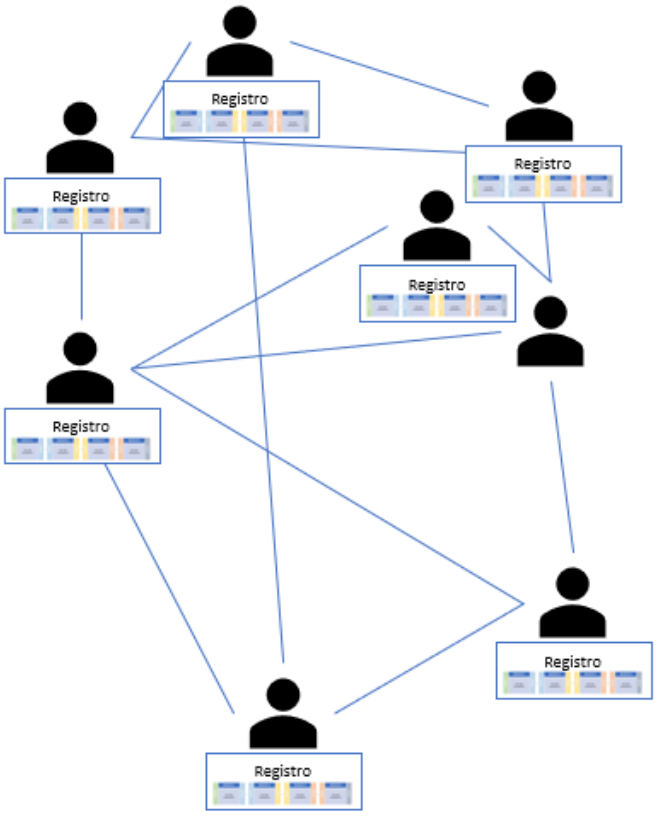

Figura 8: Esempio di rete decentralizzata Peer to Peer.

Nel momento che si ha la creazione di un nuovo blocco, i nodi sono pronti a verificare che esso sia effettivamente corretto, mediante la PoW, risolvendo l'algoritmo precedentemente descritto. Tutti loro si impegneranno in questa risoluzione, ma il primo che lo risolverà, sarà colui che lo presenterà agli altri nodi della rete. A loro volta, i nodi confermeranno che il blocco non sia stato manomesso.

In questo modo ogni nodo aggiungerà questo nuovo blocco al proprio registro. Nel caso il blocco non fosse corretto esso verrebbe respinto dal resto dei nodi.

Si può dire che è quindi di fondamentale importanza il ruolo dei miners, in quanto sono il cuore pulsante della blockchain perché sono loro che convalidano le varie transazioni.

Per questo lavoro svolto, il miner, che riesce a validare il nuovo blocco, riceverà una ricompensa dal sistema come premio. Quest'ultima si compone da una parte, che viene erogata direttamente dal sistema e un'altra che corrisponde alla transaction fee, ovvero un importo che chi scrive la transazione è disposto a pagare, per fare in modo che gli venga verificata quest'ultima. La quantità non ha un importo specifico, ma più è alta più la transazione ha priorità nell'essere verificata velocemente.

Wallet ed esempio di transazione

Per poter acquistare e rivendere una determinata moneta, all'interno di una blockchain, ogni utente avrà bisogno di un luogo dove poterle conservare. Il luogo dove possono essere custodite queste monete è il wallet, esso può essere un software o un hardware. La parola wallet sta per portafogli. Quest'ultimo ha la capacità di conservare i dati riguardo le transazioni. Esistono differenti categorie di wallet, si dividono in hot wallet e cold wallet.

Negli hot wallet rientrano:

- **Desktop wallet**, che sono dei software installabili sul pc per gestire il proprio portafogli. Quest'ultimo prevede la memorizzazione delle chiavi delle transazioni in locale o sui server del fornitore che offre il servizio.
- **Mobile wallet**, sono quelli più diffusi e sono utilizzati sugli smartphone. Il mobile wallet, come i precedenti possono memorizzare le chiavi delle transazioni in locale o sui server del fornitore.
- **Web wallet**, si può accedere tramite web e memorizzano le informazioni delle chiavi delle transazioni su un server terzo.

Tra i Cold wallet ci sono:

- **Hardware wallet**, i quali sono dispositivi che si collegano al pc e sono utilizzati per gestire un wallet.
- **Paper wallet**, che sono wallet dove le chiavi segrete, pubbliche e gli indirizzi bitcoin sono stampati per essere memorizzati a lungo termine.

La sicurezza di qualunque tipo di wallet è in funzione del suo utilizzo. Vengono utilizzate spesso autenticazioni a più fattori e un gran numero di password per poter accedere al wallet. Però questi sistemi non garantiscono la sicurezza totale del proprio wallet; soprattutto se si scrivono password semplici oppure se le si conservano scritte in luoghi fisici o ancora peggio sul proprio pc.

Definito cosa è un wallet, si può passare all'esempio di una transazione utilizzando una blockchain (DLT), con architettura di tipo peer to peer e con protocollo di validazione di tipo Proof of Work. Queste tecnologie sono utilizzate nella blockchain più famosa e

longeva al momento, che è quella Bitcoin. Si considerino due individui A e B, dove l'individuo A vuole passare una somma di monete digitali all'individuo B.

Dal punto di vista di A e B, ci sarà, nei rispettivi wallet, per A una diminuzione del valore che ha inviato a B, mentre per B un aumento del valore che riceve da A. Inoltre, essendo la transazione *pseudo anonima*, nessuno saprà mai chi siano A e B; infatti, la blockchain rende possibile le transazioni pseudo anonime. Dunque, si conosce l'effettivo scambio tra A e B, però attraverso la crittografia gli utenti appariranno anonimi con dei codici che li contraddistinguono univocamente. Infatti, ogni partecipante alla rete è contraddistinto da due chiavi:

- Una chiave privata, la quale è segreta e che vedrà solo l'utente;
- Una chiave pubblica che è accessibile a tutti per poter permettere di "comunicare" con gli altri.

Di solito nelle blockchain PoW, come la blockchain di Bitcoin, la chiave pubblica è rappresentata dall'username della persona. Come già descritto nel capitolo riguardante la crittografia, lo scambio tra due individui, avviene tramite queste due chiavi che una serve da firma e l'altra serve per mantenere il messaggio criptato al resto della rete.

Fork

Durante la vita della blockchain potrebbe accadere che in un determinato momento si abbia la necessità di dover modificare il protocollo condiviso che la regola, a causa di nuove esigenze o per renderla più efficiente. Si parla in questo caso di fork della blockchain.

Chi gestisce questi aspetti inerenti alle fork sono gli sviluppatori e lo annunciano alla propria community per vedere se effettivamente i partecipanti sono d'accordo oppure no. "Con fork si intende una modifica del codice originario il cui fine è il miglioramento di una blockchain. Ciò permette di fatto di generare una nuova versione della blockchain mantenendo però tutta la storia antecedente." (Porta M. *(2019) Cos'è un Fork di una criptovaluta e quali effetti produce*, *Cryptonomist)*.

Ci sono due tipi di fork: il soft fork e hard fork, molto diversi tra di loro.

I **soft fork** sono definiti come aggiornamenti retrocompatibili. In questa tipologia di fork si sono aggiunte delle nuove regole che non sono contrastanti con le regole precedenti. Per questo motivo, i nodi che non hanno eseguito l'aggiornamento, possono comunicare con quelli che sono aggiornati alle nuove regole di quella "nuova" blockchain.

Figura 1: Soft Fork.

Gli **hard fork** sono aggiornamenti di tipo non retrocompatibili. Questo si verifica nel momento in cui i nuovi nodi, che si aggiungono, hanno delle regole che vanno in contrasto con le regole precedenti. Dunque, si verifica che i nodi della vecchia blockchain non possono comunicare con i nodi della nuova blockchain. A questo punto si ha che la stessa blockchain si divide creando due reti separate come si può notare in figura 10, avendo così la generazione di due blockchain differenti. Entrambe le blockchain tenderanno a progredire e ad aumentare nel tempo aggiungendo ognuna dei propri blocchi contenenti le transazioni o gli scambi degli individui.

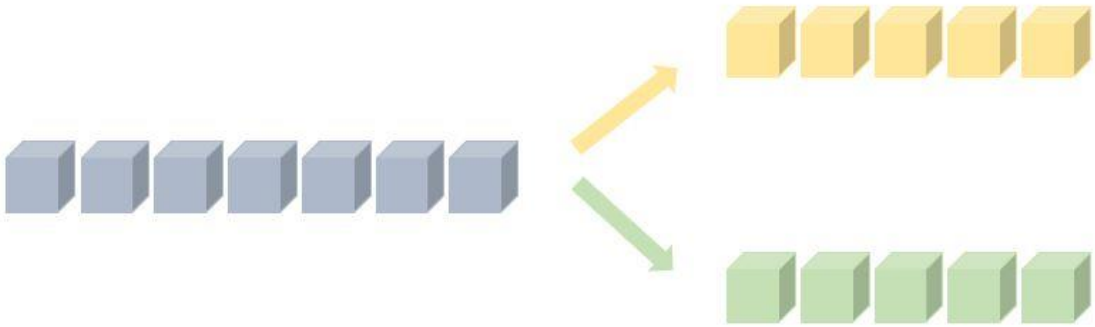

Figura 2: Hard Fork.

Di solito l'operazione di hard fork si ha quando è presente un progetto di dimensioni elevate e di rilevante incompatibilità con la blockchain da cui ci si vuole staccare. Di solito ciò accade per gestire al meglio le transazioni ed evitare l'utilizzo di grandi quantità di calcolo.

Vantaggi e Svantaggi della Blockchain

Fino ad ora si è parlato in generale della blockchain, e ci si è soffermati sugli aspetti fondamentali, considerando principalmente la blockchain più nota fino ad ora, ovvero quella di Bitcoin. Di seguito si va ad analizzare quali possono essere i vantaggi e svantaggi di questa tecnologia.

I vantaggi della blockchain sono:

- **Rete Distribuita**: la distribuzione dei dati è all'interno della rete, ciò significa che essi sono archiviati non in un luogo fisico ma all'interno di un network dove tutti possiedono una copia del registro che permette così la sicurezza che i dati non possano essere persi.
- **Difficile da manomettere:** la difficoltà di manomissione dei blocchi da parte di malintenzionati per creare delle transazioni a loro favore è impossibile in quanto l'attaccante avrebbe bisogno di una quantità di calcoli e di energia troppo elevata.
- **Velocità**: visto che essa non ha bisogno di un organo centrale, il quale approvi lo scambio di informazioni, la blockchain supera i muri burocratici rendendo le transazioni più rapide.
- **Immutabilità:** la blockchain è immutabile perché prevede solo la creazione di nuovi blocchi, infatti, non c'è la possibilità di eliminare dati ed è molto difficile poterli modificare per intenzioni fraudolenti.
- **Efficienza:** Gli scambi o le transazioni all'interno di una blockchain avvengono in maniera molto rapida, ciò garantisce agli attori di poter usufruire di tale tecnologia in tempo reale e in maniera del tutto efficiente.
- **Incontestabilità:** In funzione di qualsiasi protocollo di validazione, si raggiungerà sempre un punto di incontestabilità della validazione di una transazione. Ciò rende la blockchain incontestabile.
- **Tracciabilità dei dati da parte di chiunque:** il processo, attraverso i sistemi di registri condivisi presenta un'ottima tracciabilità dei dati, facendo in modo che tutte le transazioni possano essere visibili a tutti, garantendo allo stesso tempo anche un alto livello di trasparenza.

- **Duttilità**: La blockchain potrebbe essere utilizzata in vari ambiti, dal settore pubblico a quello privato. Potrebbe essere inserita senza problemi in qualsiasi tipo di business. Tale aspetto la rende molto adattabile in funzione di ciò che l'uomo ha bisogno.

Mentre gli **svantaggi** sono:

- **51% attack:** Questo potrebbe avvenire in particolar modo solo alle tipologie di blockchain che utilizzano la PoW come algoritmo per la validazione del blocco. In questo caso, come già detto precedentemente, è impensabile che una persona a causa del tempo e dell'ingente energia di cui ha bisogno, possa prendere il controllo del 51% della rete per raggiungere lo scopo di manomissione. Fino ad oggi non è mai successo, però teoricamente è possibile che esso si verifichi se si investissero ingenti quantità di energia per la potenza di calcolo. Questa tipologia di attacco però riuscirebbe a modificare solo le ultime transazioni in quanto è impensabile arrivare fino al blocco genesis, dato che ci vorrebbe una potenza di calcolo che ad oggi non si dispone. Quindi anche se l'attacco si verificasse cambiando un numero ristretto di blocchi, la tecnologia sarebbe abbastanza resiliente da poterlo sostenere.
- **Modifica dei dati:** all'interno della blockchain è possibile solo creare quindi risulta impossibile modificare ed eliminare dati. Quindi, è sicura però poco flessibile a nuove esigenze che nascono all'interno della rete stessa.
- **Basso livello di remunerazione:** le blockchain che utilizzano come sistema di consenso la PoW impiegano molto dispendio energetico, con un costo elevato per coloro che attuano il protocollo. Il vincitore alla fine sarà solo uno, colui che riesce a convalidare per primo il blocco. Non ci sarà mai la ricompensa distribuita a tutti i partecipanti della rete, nonostante tutti si sforzino allo stesso tempo per poter convalidare.
- **Archiviazioni:** le blockchain hanno una capienza limitata; con il tempo potranno superare la crescita in hard drive, e il network così rischia di perdere dei nodi in quanto il registro diventa troppo grande da scaricare e da poter essere conservato.

  (Binance Acaademy. (2021). *Vantaggi e Svantaggi della Blockchain)*

Protocolli di validazioni, uno sguardo alla Proof of Stake

Come è stato descritto precedentemente, il mezzo di verifica più conosciuto e anche più utilizzato dal maggior numero di blockchain è quello della **Proof of Work.** Quest'ultimo, però, non è il solo ad essere utilizzato. Si può dire che questo protocollo di validazione è uno dei primi che nasce grazie alla blockchain della criptovaluta Bitcoin per la risoluzione del Problema dei Bizantini. Però, ci sono diversi protocolli di verifica, alcuni di loro in forte tendenza, che probabilmente col tempo sostituiranno la PoW. Moltissime blockchain li stanno già testando, ce ne sono diversi, per esempio: **Proof of Stake** (PoS), **Delegated Proof of Stake** (DPoF), **Federated Byzantine Agreement** (FBA), **Proof of Elapsed Time** (PoEF). Dopo aver descritto precedentemente il funzionamento della PoW, adesso ci si soffermerà sulla Proof of Stake.

La **Proof of Stake** è una soluzione che sta prendendo sempre più spazio tra i vari protocolli di validazione delle blockchain. Infatti, il creatore di una tra le criptomonete più importanti, Ethereum, sta provando a sfruttare questo nuovo protocollo di validazione.

In questo caso non si ha più la presenza dei miners come nel caso della PoW bensì la presenza dei **validators**. Il validator sarà colui che ha il potere di convalidare il blocco. Tutte le persone della rete possono essere validatori, ma viene scelto dal sistema uno solo per ogni blocco, in maniera probabilistica, in base alla quantità di monete che possiede di una determinata criptomoneta. Presupponendo che una persona sia un gran possessore di quella determinata cripto, avrà più probabilità di essere il validatore ed è di suo completo interesse far sì che le transazioni e i blocchi non nascondano attività fraudolenti. Se infatti un validatore manomettesse un blocco, successivamente altri validatori se ne accorgerebbero, nel momento in cui andrebbero a validare anche loro altre transazioni. Questo comporterà un annullamento automatico di quel blocco manomesso dal validatore precedente, il quale si ritroverà con le proprie risorse impiegate distrutte. Quindi per qualunque validatore sarebbe positivo che tutte le parti della rete, compreso lui stesso, siano effettivamente leali, alimentando le transazioni della blockchain in maniera regolare.

Ovviamente non si terrà conto solo della quantità di monete che un validator possiede per poter validare la transazione, altrimenti sarebbe sempre la persona con più criptomonete a poter validare. Le soluzioni che sono state adottate da differenti blockchain per tener conto di decidere chi valida il blocco sono differenti:

- **Random**: sistema casuale, dove il validator sarà scelto in maniera completamente probabilistica, però questa scelta casuale sarà influenzata dalla quantità di criptomoneta che i vari attori presentano già e quindi chi ha più criptomonete ha più probabilità di poter essere eletto per validare un blocco.
- **Anzianità**: consiste nel considerare un indice che dipende dalla quantità di monete moltiplicato per il giorno che sono state possedute. Questo indice diviene zero nel momento in cui si inserisce un blocco e decade se il tempo di possedimento diventa troppo lungo.
- **Velocità**: Si considerano maggiormente gli attori che movimentano di più quel determinato bene piuttosto che tenerlo custodito

La metodologia di validazione dei blocchi è molto diversa dalla precedente, non è più sulla risoluzione di un algoritmo complesso. A primo impatto, sembrerebbe un modo ad incentivare le persone a possedere più criptomonete di una determinata blockchain così da avere più probabilità di divenire validator e ricevere la propria ricompensa.

Proof of Work e Proof of Stake a confronto

La PoS ci fa notare che potenzialmente potrebbe essere un elemento che può effettivamente sostituire la PoW e questo per i seguenti motivi:

- La PoS nasce soprattutto dall'esigenza di fare in modo che si possa risparmiare in termini di consumo energetico, in quanto la blockchain che utilizza il protocollo classico PoW ha un consumo di energia elettrica notevole perché ha bisogno di utilizzare hardware specifici, costosi e con una elevata potenza di calcolo per l'attività di mining.
- La PoS permette che la rete, la distribuzione e la possibilità di validazione sia più equilibrata in quanto tutti i partecipanti possono provare a validare un blocco. Ovviamente la probabilità di essere validator dipende in base alla quantità di assets che si possiedono.

- Inoltre, un'altra lancia spezzata a favore della PoS è che essa è molto scalabile e non ha bisogno dei lunghi tempi di calcolo per risolvere l'algoritmo di validazione del blocco.
- La PoW, comunque, si trova in vantaggio sotto alcuni aspetti. Per esempio, essa è stata già molto testata su differenti blockchain ed effettivamente si è notata la sua efficacia in tutti questi anni di funzionamento; mentre la PoS è un protocollo non molto conosciuto, che si sta cercando in questi ultimi anni di applicare alle blockchain e non si hanno ancora abbastanza analisi conclusive e dimostrative.
- La PoS, inoltre, dà maggiore possibilità alle persone più ricche di quel determinato asset di avere più probabilità di essere validator; ne consegue che le persone aventi più assets tendono a divenire sempre più ricche. Però di questa problematica si può dire che ne è affetta anche la PoW, in quanto chi ha maggiore potenza di calcolo e quindi maggiori risorse impiegate, riuscirà ad avere più probabilità di convalidare il blocco.
- Inoltre, per la PoS c'è maggiore difficoltà nella gestione di un eventuale fork, rispetto che alla PoW. Questo perché si potrebbe verificare il **Nothing at stake**. Ovvero, nel caso si volesse far avvenire una ramificazione, una persona potrebbe votare per entrambi le varianti del fork. A differenza della PoW, nella PoS non costerebbe molto lavorare su entrambe le catene generando un inganno al sistema; per esempio, la possibilità di spendere due volte in un'istanza di riorganizzazione della blockchain. Per fortuna sono già presenti delle possibili soluzioni come, per esempio: il checkpoint, limite sulla riorganizzazione dei blocchi e punire persone che lavorano su due rami nello stesso momento.

Blockchain: pubblica, privata ed ibrida

La blockchain nasce come una tecnologia pubblica, distributed, lontana da quella che potrebbe essere una tecnologia centralizzata. Nonostante parta da questo ideale, la blockchain comunque può essere di tre tipi: pubblica o permissionless, privata o permissioned e ibrida. La principale differenza tra quella pubblica e quella privata è soprattutto che nella seconda ritorna un po' l'idea di centralizzare. In una blockchain privata, per entrare a far parte di questa rete, potrebbe essere obbligatoria un'autorizzazione da parte dei gestori della rete stessa. Fino a questo momento è stata trattata principalmente la logica di funzionamento di una blockchain pubblica; ora si andranno ad analizzare le differenze tra quelle pubbliche e quelle private. Di seguito saranno analizzate le tre tipologie.

La blockchain pubblica o permissionless, come è stata descritta fino ad ora è una rete in cui nessuno prevale sull'altro, qualsiasi utente della rete può divenire potenzialmente un nodo. Tutti possono leggere e validare delle transazioni dove si è premiati in qualche modo per aver messo a disposizione i propri mezzi per la convalida di un blocco. Questa blockchain è definita decentralizzata, nessuno ha il potere di alterarne le informazioni al suo interno. La blockchain permissionless più nota è quella Bitcoin.

La blockchain privata o permissioned è una tipologia di blockchain in cui c'è una figura centrale che deve permettere l'autorizzazione agli altri membri che vorrebbero parteciparvi. All'interno di questa tipologia non è possibile modificarne il protocollo se non da parte dell'autorità centrale. Questa blockchain si avvicina molto al modello centralizzato che già si conosce, controllato da una figura centrale. Sembrerebbe che si stia facendo un passo indietro, però la blockchain privata, comunque, potrebbe essere una tecnologia che garantisce miglioramenti in termini di efficienza, velocizzando alcuni processi e garantendo un miglior scambio di dati. Questa blockchain negli ultimi anni sta riscuotendo maggior successo perché permette di poter essere applicata anche in altri contesti come società o aziende private, enti governativi e finanziari. Alcuni famosi esempi di blockchain permissioned sono Corda ed Hyperledger

L'ultima indicata è la **blockchain ibrida** che è un mix tra quella pubblica e quella privata. Una blockchain ibrida permette che non ci sia solo la presenza di un nodo che prevale sugli altri come in quella privata, bensì più nodi sono autorizzati ad avere un

potere maggiore rispetto agli altri. In questo caso rimane sempre la regola che la convalida di una determinata transazione deve avvenire almeno dalla metà delle persone che hanno il permesso di poter convalidare. Questa tipologia rientra tra le blockchain di tipo privato, però gestita da più parti di una stessa organizzazione. Nonostante quest'ultima sia un mix tra le due blockchain, permissioned e permissionless, essa si avvicina di più a quella privata.

Le blockchain di tipo ibride e private godono di una maggiore garanzia di sicurezza per le persone che ne usufruiscono, anche in termini di privacy, in quanto c'è una figura centrale che la garantisce. Inoltre, i membri convalidanti sono un numero minore e si conoscono, quindi, ogni parte assume la propria responsabilità. Ovviamente però queste ultime fanno sì che gli utenti devono affidarsi sempre ad un'entità centrale.

La Blockchain per il mondo delle criptomonete

La blockchain può essere applicata in diversi settori. La tecnologia blockchain, come già accennato in precedenza è molto conosciuta grazie al mondo delle **criptocurrency**, in italiano criptomonete. Prima di questa applicazione, infatti, il termine e il funzionamento della blockchain era quasi del tutto sconosciuto. In particolare, essa è stata resa famosa attraverso Satoshi Nakamoto per la creazione di una moneta virtuale che ha il nome di Bitcoin. L'obiettivo di Nakamoto era quello di rendere decentralizzato il sistema bancario. L'idea di decentralizzare nasce dal susseguirsi di varie crisi finanziare che si sono verificate negli ultimi anni, causate principalmente da sistemi centrali che a causa di corruzione e di clientelismo hanno creato dei buchi finanziari, i quali hanno generato forti crisi economiche. Non è una coincidenza che questa idea di decentralizzare nasca durante il periodo in cui scoppia la bolla dei mutui subprime, dove le banche di affari, pur di fare i propri interessi personali, hanno alimentato una bolla finanziaria di notevoli dimensioni, che al suo scoppio ha provocato una delle crisi più forti e distruttive in termini economici della nostra epoca. Questa crisi provocata da banche private ha trascinato dietro di sé un buco finanziario che ha piegato molti Stati facendo aumentare il debito pubblico a discapito della classe media e povera della popolazione. A causa di quest'ultima crisi fu lanciato Bitcoin.

Bitcoin, già spesso citato, non è altro che una criptomoneta che viene utilizzata per decentralizzare il sistema monetario, utilizza una blockchain di tipo permissionless, quindi pubblica, che rende il sistema totalmente efficiente su una struttura di tipo distributed ledger, utilizzando come sistema di approvazione delle transazioni la Proof of Work. Il valore di questa criptomoneta inizialmente era molto basso. Per incentivare le persone al controllo delle transazioni è stato definito un sistema PoW che generasse una quantità di bitcoin per i verificatori dei nodi. Per la convalida delle prime transazioni, la remunerazione dei bitcoin, rilasciata dal sistema per incentivare i miners a poter verificare i blocchi di transazioni, era molto alta. Successivamente con il tempo e con il numero di blocchi ormai già convalidati le ricompense sono diminuite, in quanto la quantità totale di bitcoin che viene prodotta è limitata. Ovvero si arriverà in un momento in cui i Bitcoin non saranno più generati. Questo renderà più difficile che la moneta subisca inflazione nel corso della sua vita in quanto non potrà essere generata una sovrapproduzione di essa; ciò renderà la moneta dipendente solo dalla domanda del mercato e non dall'offerta.

Il protocollo PoW ha determinato la nascita del miner, di cui abbiamo precedentemente parlato. Oggigiorno, molte sono le persone che investono sulla creazione di vere e proprie basi di mining contenenti migliaia e migliaia di CPU (central process unit) e soprattutto GPU (graphic process unit) per risolvere i calcoli complessi dovuti dalla validazione di un blocco, per poter ricevere la ricompensa da parte del sistema.

Le tecnologie hardware inizialmente impiegate erano prettamente le CPU dei computer. Successivamente si è passati alle GPU per la velocità con cui riuscivano a svolgere questi particolari calcoli. Oggigiorno, per il mining di Bitcoin, sono costruiti degli appositi circuiti hardware dedicati al solo calcolo di una determinata funzione hash, detti ASIC (application specific integrated circuit).

Il solo problema di questa tipologia di operazione è, oltre all'elettricità che necessitano i processori per poter svolgere i calcoli, quella del raffreddamento di cui si ha bisogno, generando un consumo energetico elevato; così alto, che molti imprenditori che hanno deciso di investire sul mining, hanno spostato le proprie sedi operative in paesi dove il costo dell'energia elettrica è molto basso e che si possa garantire un profitto elevato.

Il Bitcoin, avente come simbolo ₿ e codice BTC o XBT, utilizza una propria rete blockchain decentralizzata, programmata in linguaggio C++. Questa valuta con la sua relativa blockchain nasce nel 2008 ma viene lanciata effettivamente il 3 gennaio del 2009 dove il suo valore era di circa 0,01 euro per bitcoin. Con gli anni il valore di tale moneta è mutato notevolmente, rendendola una moneta molto volatile nel campo finanziario. Questo soprattutto perché non vi è garanzia da parte di un ente centrale, che la controlla, dunque, non vi è molta fiducia dalla maggior parte delle popolazioni. Per questo motivo, il valore è dipendente solo dalla compravendita della moneta e quindi è soggetta a fortissime oscillazioni da parte di speculatori. Si può dire però che oggigiorno l'andamento complessivo è sempre crescente.

In basso è presente un grafico di come è stato l'andamento storico di tale criptomoneta dall'aprile del 2013 che era il periodo in cui aveva raggiunto circa 750 euro, fino al 2021 che ha avuto un picco di circa 65.000,00 euro per avere oggi un valore di circa 53.000,00 euro (valore al 01/nov.):

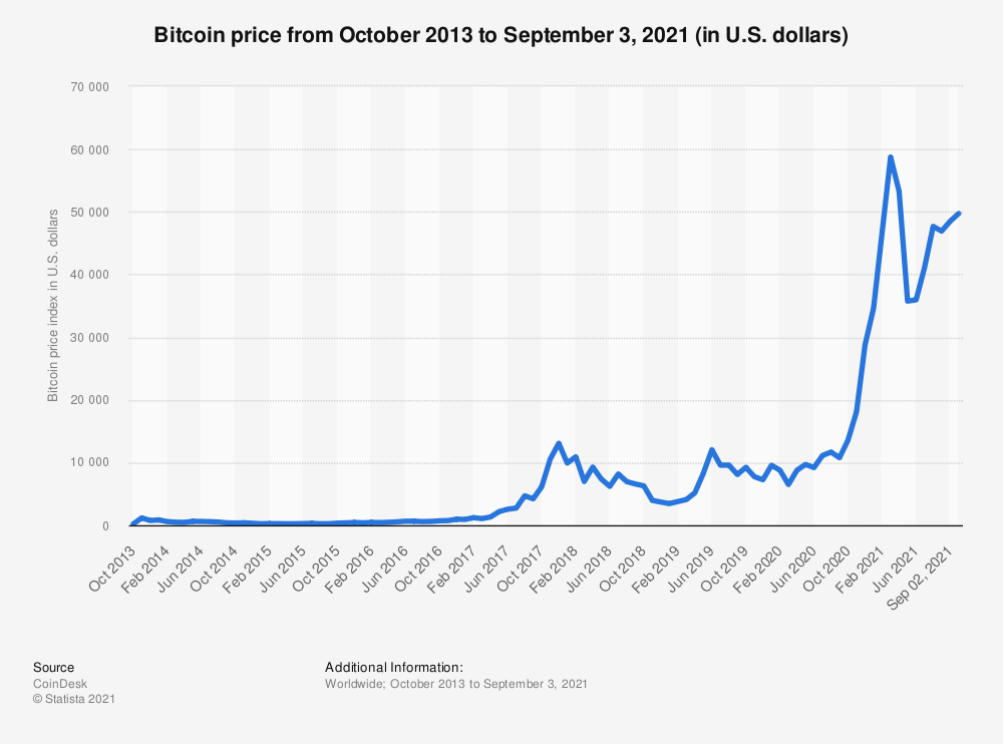

Grafico 1: Variazione del prezzo di Bitcoin da ottobre 2013 a settembre 2021. (Statista. (2021). Bitcoin price from October 2013 to September 2021).

Nell'immagine successiva è presente il market cap sempre dello stesso periodo di tempo dove nel 2020 è riuscito a raggiungere anche una capitalizzazione di 1.000 miliardi di dollari.

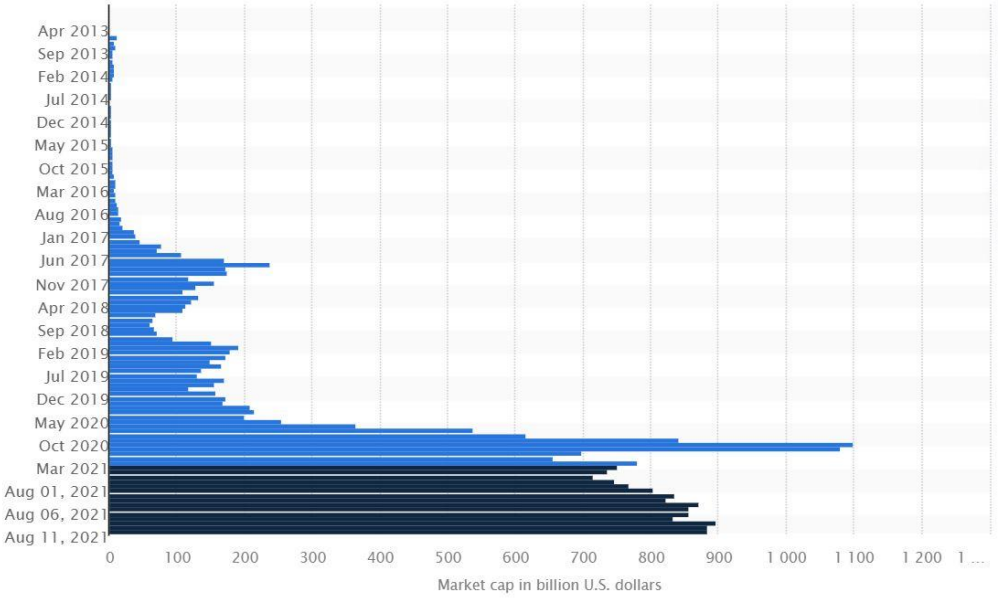

Grafico 2: Capitalizzazione del mercato dal 2013 al 2021. (Statista. (2021). Market capitalization of Bitcoin from April 2013 to September 2021).

Infine, in basso è presente il grafico che mostra la quantità di grandezza dei dati contenuti all'interno della blockchain Bitcoin. Ciò mostra un aumento della memoria che viene utilizzata di anno in anno, dove la crescita come si può notare non è lineare ma esponenziale. In quanto si verificano sempre più transazioni.

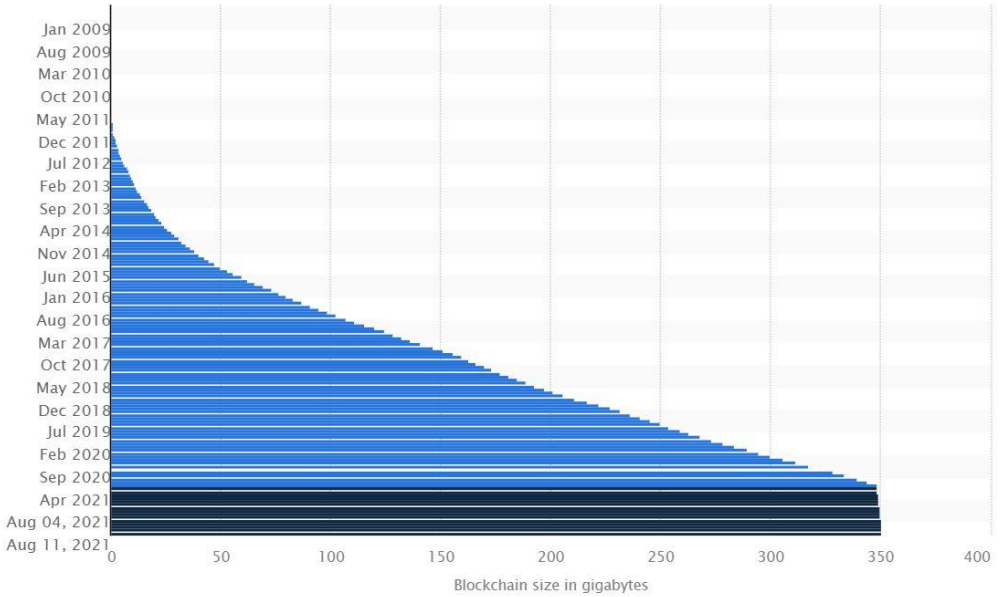

Grafico 3: Dimensione della blockchain bitcoin. (Statista. (2021). Size of the Bitcoin blockchain from January 2009 to September 2021).

Questi tre grafici permettono di capire quanto sia sempre più utilizzata questa tecnologia per una singola criptomoneta e quanto le persone effettivamente investano implicitamente su una blockchain che renda sicure le transazioni.

Oggigiorno, il Bitcoin sta rivoluzionando il mondo della finanza, cambiando anche il modus operandi di quest'ultimo. Alcuni Paesi l'hanno già accettata come seconda valuta nazionale e molti altri stanno valutando di renderla tale. Inoltre, anche valute come l'euro e il dollaro stanno cercando di seguire la scia della digitalizzazione.

Il problema legato alle transazioni attraverso criptomoneta è che gli attori che scambiano denaro per la rete sono anonimi. Per questo motivo si potrebbe verificare la compravendita di materiale illegale. Infatti, le criptomonete, soprattutto Bitcoin, sono un ottimo mezzo di scambio all'interno del deep web, dove le persone possono comprare apparentemente qualunque cosa che desiderano di illegale in maniera del tutto anonima. Però non significa che il mondo delle criptomonete deve essere visto in maniera del tutto negativo, in quanto se oggi il problema è legato alla completa anonimità delle informazioni di coloro che scambiano denaro digitale, un tempo lo era attraverso il denaro contante. Il problema non è la tipologia dello scambio ma la possibilità di far accedere degli utenti ad una rete non protetta che permetta degli acquisti contro qualsiasi principio etico e morale.

Bitcoin è solo una delle tante criptomonete che oggi si conoscono, ne esistono diverse e molte stanno acquisendo sempre più valore nel corso degli anni; un esempio è Ethereum nata dal noto russo Vitalik Buterin. Anche lui ha utilizzato una blockchain con protocollo di verifica PoW, però in questi ultimi anni Ethereum sta studiando il modo di passare ad una nuova rete, utilizzando come protocollo di approvazione delle transazioni la Proof of Stake. Il codice di Ethereum è ETH. Il valore di questa criptomoneta è anche esso molto elevato, di fatto ha raggiunto circa i 4.100,00 dollari rendendola una delle più importanti al momento. Utilizza una blockchain programmata attraverso linguaggio di programmazione Solidity e il motivo per cui è resa importante come blockchain non è solo per la transazione della propria moneta digitale bensì dello scambio e dell'approvazione degli smart contracts.

Smart Contracts

“Gli **Smart Contracts** sono protocolli informatici che facilitano, verificano, o fanno rispettare, la negoziazione o l'esecuzione di un contratto, permettendo talvolta la parziale o la totale esclusione di una clausola contrattuale. Gli smart contracts, di solito, hanno anche un'interfaccia utente e spesso simulano la logica delle clausole contrattuali”. (Smart contract. (2021). *Wikipedia, L'enciclopedia libera)*.

L’idea degli smart contracts, in italiano “contratti intelligenti”, non nasce legata alla blockchain, fu l’informatico Nick Szabo a idearli. Bisognerebbe fare un passo indietro, in quanto lo smart contract risale già alla fine del secolo scorso con un’idea di base molto simile a quella odierna. L’obiettivo era quello di poter permettere ad un utente di attivare o disattivare una determinata licenza software in base a dei vincoli. Attraverso l’utilizzo di una chiave digitale l’utente potrà usufruire del software solo se ha effettuato il pagamento; altrimenti, se il contratto non fosse più in status “pagamento” o se fosse scaduto, la licenza non avrebbe conferito il permesso al funzionamento.

La trasformazione è avvenuta nel momento in cui si è passati alla creazione di contratti eseguiti automaticamente dalle macchine. Questi contratti hanno un linguaggio di programmazione diverso da quello naturale e questo è definito *data oriented contract*.

Inoltre, si è inserito un ulteriore punto riguardo all’automatizzazione degli alert con il *computable contract*.

Infine, si arriva al momento in cui nascono gli smart contracts; essi non sono altro che dei contratti digitali che sfruttano la tecnologia blockchain. Si differenziano con i predecessori perché appartengono ad una rete decentralizzata. Se si parla di blockchain permissionless la vera differenza è che l’intera gestione dell’accordo contrattuale è completamente automatizzata senza aver bisogno di alcun intervento umano. Gli smart contracts hanno bisogno di modelli di sviluppo che danno la possibilità di rendere automatiche relazioni tra più parti evitandone possibili errori.

Uno smart contract deve far sì che alla base ci sia un linguaggio di capacità interpretativa molto ampio. Infatti, per poter permettere che si verifichi la stesura di un contratto, avente azioni diverse a seconda del verificarsi di una determinata clausola, è

necessario che il linguaggio macchina possa comprenderne il significato effettivo del linguaggio umano, entrando nei panni di una persona.

Lo smart contract come lo si intende oggi ha bisogno necessariamente della blockchain per poter funzionare. Uno smart contract per esistere ha bisogno di un codice di scrittura e una piattaforma generica e deve soprattutto garantire tre punti fondamentali:

- Il **codice** con cui esso viene scritto deve avere la caratteristica di non poter essere modificato.
- Le **fonti dei dati** che ne determinano le condizioni di applicazione devono essere certificate e avere un'alta qualità.
- Le **modalità di lettura** e controllo delle fonti devono essere anche esse certificate.

Gli smart contracts come tutti gli strumenti che usufruiscono della blockchain godono di quella che è la decentralizzazione del sistema. Se si considerano i tradizionali contratti, essi hanno bisogno di una terza figura che in questo caso faccia da garante per gli attori che intendono stipulare un contratto (es: avvocato o un notaio); mentre con gli smart contracts la terza parte viene rimpiazzata dai nodi decentralizzanti che convalidano l'autenticità di un determinato contratto.

Le caratteristiche di uno smart contract sono:

- **Account**: sarebbe la combinazione delle chiavi pubbliche e private delle due parti che richiedono di stipulare un contratto.
- **La quota della memoria del registro che esso occupa**
- **Codice di esecuzione**

Le due parti, in questo caso, è importante che si conoscano, in quanto devono stipulare un vero e proprio contratto. Inoltre, dovranno decidere i termini, i contenuti e le clausole del contratto stesso. Le varie clausole del contratto dopo che sono state stipulate, da parte degli attori, sono inserite attraverso chiavi private in un blocco, che automaticamente seguono il processo di cifratura. Il blocco viene immesso all'interno del network e validato dai miners che, attraverso le chiavi pubbliche, potranno accedere al contenuto dell'informazione e validarlo, aggiungendo questo blocco al resto della catena. Il contratto passerà in una procedura nominata if/then; se il sistema riuscirà a

riconoscere la clausola, il contratto potrà essere registrato, altrimenti c'è bisogno che le parti interessate trovino un'altra soluzione. Esistono due tipi di smart contracts, **deterministici e non deterministici**. Si differenziano perché quelli deterministici non richiedono l'intervento da parte di enti esterni alla blockchain, mentre i secondi hanno bisogno di una terza parte che viene chiamata oracolo**,** in anglosassone **oracle.**

"Un oracolo blockchain è un servizio offerto da terze parti ed è responsabile della fornitura di informazioni esterne (al di fuori della blockchain) agli smart contracts, in modo che possano eseguire decisioni… Quindi, l'oracolo è incaricato di fornire i dati esterni alla blockchain in modo che il contratto intelligente possa conformarsi alle condizioni precedentemente stipulate nel contratto." (Perez R. (2020). *Cos'è un Oracle Blockchain, Bitnovo*). Essi si classificano in due categorie principali:

- **Oracle software** che sono collegati a delle fonti di informazioni online;
- **Oracle hardware** che sono collegati a informazioni legate al mondo hardware, per esempio uno scanner, e traducono gli eventi del mondo reale in valori digitali per poter essere compresi dagli smart contracts.

Quindi la funzione dell'oracle è quella di convalidare il contratto nel momento in cui combacia con un'informazione registrata dall'esterno della blockchain. Essi sono definiti come il ponte tra le blockchain e il mondo esterno. Le caratteristiche che un oracle deve possedere sono:

- **Attendibilità:** in quanto non deve fornire dei dati manomessi;
- **Affidabilità:** utilizzare svariate fonti per ridurre probabili errori;
- **Trasparenza:** tutti devono avere la possibilità di verificare la correttezza delle informazioni fornite.

Il limite che affligge gli oracle è che purtroppo essendo dei dati che arrivano dall'esterno, possono presentare dei rischi legati alla manomissione, che potrebbero impattare negativamente sugli smart contracts.

Gli smart contracts necessitano di una blockchain. Ovviamente hanno caratteristiche differenti in base ai linguaggi con cui sono programmate. In funzione del linguaggio di programmazione e come è programmata la blockchain, ci possono essere delle capacità

computazionali limitate che rendono impossibile l'utilizzo di tale tecnologia per gli smart contracts.

Questo strumento è diventato sempre più rilevante grazie all'aiuto della blockchain Ethereum. Tale blockchain ideata dall'ormai conosciuto russo Vitalik Buterin, ha reso possibile lo scambio degli smart contracts in maniera semplice e veloce. Ethereum è programmata tramite linguaggio Solidity, quindi gli smart contracts sono codificabili utilizzando questo linguaggio di programmazione che consente istruzioni di codice complesso, utilizzando anche la logica del loop. In questo modo è possibile avere una maggiore personalizzazione del proprio contratto; ed è questo il motivo principale per cui questa blockchain è tra le più utilizzate. Un'altra blockchain anche più efficiente in ambito di smart contracts, però meno conosciuta, è **NEM** che rispetto alla precedente è anche più scalabile e consente di poter gestire anche centinaia di transazioni al secondo fornendo anche molta sicurezza. Quest'ultima è scritta in Java.

Oggigiorno, gli smart contracts purtroppo hanno dei propri limiti in quanto presentano numerose criticità che non li rendono vantaggiosi e le operazioni contrattuali poco efficienti. Le principali cause di questi ultimi sono la difficoltà nella gestione della complessità di alcuni contratti e la difficoltà nel gestire la naturale ingerenza/ influenza di altre categorie giuridiche nel momento in cui un contratto viene eseguito.

Per quanto riguarda gli smart contracts in Italia, il Ministero dello Sviluppo Economico ha dato l'incarico ad esperti per stabilire una definizione di quest'ultimo. Secondo il testo normativo, uno smart contract, deve avere le seguenti caratteristiche:

- Essere un programma per elaboratore;
- Operante su tecnologie basate su registri distribuiti;
- La cui esecuzione vincola automaticamente due o più parti;
- Sulla base di effetti predefiniti dalle stesse;
- Deve soddisfare il requisito della forma scritta nel caso di previa identificazione informatica delle parti interessati tramite un processo fissato dall'AgID (agenda digitale italiana).

Vantaggi degli Smart Contracts

Gli smart contracts trovano sempre più spazio nelle applicazioni in diversi settori in quanto garantiscono diversi benefici:

- Non si ha più la necessità obbligatoria di una terza parte per la convalida di un contratto, i quali possono essere eseguiti in maniera del tutto autonoma su una rete controllata, sicura e decentralizzata.
- Trasparenza delle clausole presenti all'interno del contratto per tutte le parti coinvolte nella stipula del contratto stesso.
- Immutabilità delle transazioni registrate rendendo impossibile modificare o annullare allo stesso tempo il contratto.
- Completa automatizzazione del processo contrattuale così da non avere tempi lunghi per la convalida da parte di figure terze. In questo modo oltre alle tempistiche più veloci, diminuiscono anche i costi dovuti alla burocrazia e rallentamenti dovuti ad attori terzi.

Token

Con la nascita delle criptomonete dopo pochissimo tempo sono emersi dei nuovi strumenti, i **tokens**. La parola token deriva dall'anglosassone e si può tradurre come gettone. Un token può essere definito come "un insieme di informazioni digitali all'interno di una blockchain che conferiscono un diritto a un determinato soggetto; la tokenizzazione è la conversione dei diritti di un bene in un token digitale registrato su una blockchain". (Jovacchini L. e Nardella P. (2020*). Token: cos'è e come viene utilizzato nelle criptovalute Blockchain 4innovation Netwok Digital 360).*

La parola token è molto comune e assume anche un significato molto vasto, per questo motivo essi sono differenziati in tre categorie:

- **Utility Token**: danno diritto all'utilizzatore di alcune features su una piattaforma, fornendo benefici o servizi aggiuntivi.
- **Security Token**: conferiscono il diritto di partecipazione al profitto della piattaforma che ha deciso di emetterli.

- **Payment Token**: sono delle criptomonete e molte volte questi token sono chiamati anche coin.

I tokens sono legati alle criptomonete e attraverso quest'ultime sono permessi gli scambi all'interno della blockchain. Inizialmente, per poter acquistare i tokens, c'era bisogno di comprare prima la criptomoneta di riferimento e successivamente attraverso quest'ultima acquistare il token.

Oggigiorno si sono trovate soluzioni più smart e veloci per avvantaggiare gli utenti a scambiare e permettere di fare transazioni di tokens. Questa evoluzione avviene tramite l'utilizzo di smart contracts. In questo modo c'è sempre bisogno di una blockchain di riferimento per poter acquistare un token, ma l'acquisto non bisogna necessariamente farlo attraverso la criptomoneta di quella determinata blockchain. Quindi gli utenti potrebbero comprare direttamente i tokens utilizzando anche le valute tradizionali come per esempio euro o dollaro. Rispetto ad una moneta digitale, il token può essere creato più facilmente in quanto sarebbe semplicemente la scrittura di uno smart contract. Mentre nel caso di una valuta ci sarebbe bisogno della creazione anche di un protocollo di consenso. Attraverso l'acquisto di un token, un determinato individuo possiede un determinato pacchetto dati che conferiscono un diritto a quella persona.

I token, di solito, fanno riferimento a qualcosa che effettivamente è esistente nel mondo reale. Infatti, un oggetto, un prodotto o un servizio che viene digitalizzato ha una propria associazione ad un pacchetto di dati che compone "l'oggetto digitale"; questo processo è definito **tokenizzazione**. Esso permette di creare un legame tra mondo reale e mondo digitale. Potenzialmente tutto può subire un processo di tokenizzazione, la quale potrebbe essere utilizzata in qualsiasi tipo di business.

Principalmente i tokens sono utilizzati dalle aziende. Infatti, Molte aziende potrebbero utilizzare questi ultimi come abilitatori di un servizio. Per esempio, si pensi alle aziende di trasporto pubblico urbano. Queste ultime, invece di vendere dei biglietti fisici per poter essere obliterati all'interno del mezzo pubblico, potrebbero vendere dei tokens (corrispondenti univocamente ad un biglietto). Il biglietto è nominativo e quindi univoco di quella persona e quest'ultima potrebbe timbrarlo nel momento in cui sale sul mezzo pubblico. Questo processo garantisce maggiore comodità al cliente, minori

sprechi ambientali per la produzione di un biglietto fisico e vantaggi economici all'azienda di trasporto.

Inoltre, i tokens possono essere anche un modo per finanziare dei progetti. Infatti, molte startups, attraverso l'emissione di questi ultimi, possono trarre vantaggi in ambito finanziario.

Tradizionalmente le startups per finanziare il proprio progetto cercano degli investitori che possano fornire loro liquidità. Il problema che si è riscontrato è che gli investitori sono generalmente pochi (di solito sono Business Angels o Venture Capitalists). Queste entità però non investono in qualsiasi tipo di azienda, bensì in quelle più ricercate, con idee che reputano possano essere più redditizie.

Le Startups, per attrarre investitori di qualsiasi dimensione di capitale, mettono in vendita i tokens riguardo il proprio progetto. In questo modo, anche i piccoli investitori che credono nel progetto, potrebbero acquistare dei tokens, così da conferire liquidità all'azienda. Il token acquistato darà la possibilità a colui che lo ha comprato di ricevere benefici nel momento in cui verranno lanciati i prodotti o i servizi sviluppati. In questo modo colui che comprerà un token potrà figurare come un "partecipante" di quel progetto e successivamente potrà usufruire dei servizi offerti dalla startup che gli ha venduto quei tokens. Nel momento che una persona acquista un token direttamente dall'azienda lo metterà all'interno del proprio wallet e potrà scambiarlo con altre persone per una quantità di denaro o di altre criptomonete all'interno della blockchain di riferimento, creandosi così un mercato parallelo.

Gli investitori prima di compiere l'investimento avranno la premura di informarsi riguardo il progetto in sé attraverso il cosiddetto whitepaper, ovvero un documento che spiega precisamente quali sono le caratteristiche e gli obiettivi del progetto stesso, scritto dal team che sta implementando quest'ultimo.

La vendita di tokens per denaro avviene già da molti anni attraverso siti delle aziende oppure attraverso delle piattaforme di exchange che permettono lo scambio di tokens con denaro.

La prima tipologia di vendita di questo tipo fu chiamata ICO, ovvero **Initial coin offering**. Permetteva alle persone che avevano preso nota del whitepaper di poter

comprare i tokens in maniera facile e veloce dal sito ufficiale dell'azienda, senza troppe regole e senza la presenza di un organo centrale, che facesse in modo di garantire che l'azienda fosse vera e che effettivamente esistesse. Naturalmente questo ha causato diverse truffe agli investitori da parte di alcune aziende che non sono state rintracciate, suscitando così scandalo all'interno del mondo della blockchain, più nello specifico dei tokens.

A causa di questa problematica subito si è passati a soluzioni prestanti che potessero mettere al sicuro gli investitori, infatti, da ICO si è passati ben presto agli IEO, **Initial exchange offering**. In questo caso, le aziende dopo la presentazione del proprio whitepaper devono far valutare il proprio progetto a delle piattaforme exchange così da permettere acquisti di token sicuri per i cittadini. Questo ha comportato una maggiore sicurezza negli scambi, in quanto c'è la presenza di un "garante".

Con gli anni, parallelamente agli IEO sono stati introdotti anche gli STO, **Security Token Offering**. Questi tokens sono molto sicuri in quanto regolamentati, infatti, essi assumono una figura prettamente finanziaria che li rende soggetti alle normative dei mercati finanziari. Essi danno il diritto di partecipare al profitto dell'azienda che li emette. Ciò fa sì che nel momento in cui un token è identificato come STO, il livello di sicurezza corrispondente è molto elevato, ma essendo soggetto a molti controlli le tempistiche di rilascio di questi tokens a volte potrebbero essere molto lunghe.

Not Fungible Tokens

Con gli anni attraverso la blockchain, sono stati ideati nuovi strumenti cha stanno rivoluzionando vari settori: da quello produttivo fino al mondo dell'arte. Questi strumenti sono gli **NFT**, **Not Fungible Tokens**; sono una tecnologia con un funzionamento molto simile ai tokens. Un NFT, in italiano token non fungibile sarebbe: "un tipo speciale di token crittografico che rappresenta qualcosa di unico; i gettoni non fungibili non sono quindi reciprocamente intercambiabili. Ciò è in contrasto con le criptomonete, come bitcoin e molti token di rete o di utilità, che sono per loro stessa natura fungibili." (Wikipedia. (2021). *Non-fungible token. Wikipedia, L'enciclopedia libera*).

Oggigiorno, sono una delle tendenze crittografiche con maggiore rilevanza, però l'invenzione degli NFT risale già alla fine del 2012 quando nacque il concetto di Bitcoin Colored Coins. Queste monete altro non erano che delle piccolissime frazioni di Bitocin con delle informazioni che le contraddistinguevano; ciò ha dato inizio alla creazione degli NFT che si conoscono oggi.

Come i tokens, anche gli NFT necessitano di una blockchain che possa permettere lo scambio di questi ultimi, mantenendone l'autenticità. Oggigiorno la blockchain più utilizzata per gli NFT è quella di Ethereum, ma sono diverse quelle che offrono un ottimo servizio per lo scambio di queste informazioni.

Per trasformare un oggetto, un'immagine in NFT non c'è bisogno di passaggi molto complessi, effettivamente tutti potenzialmente potrebbero creare un NFT in maniera rapida e venderlo. Per esempio, se immaginassimo di utilizzare come piattaforma quella di Ethereum si avrà bisogno di un wallet di tipo ERC-721 che supporti gli NFTs, una quantità di valuta di Ethereum così da poter permettere di caricare il file scelto e renderlo un NFT e successivamente di poterlo mettere sul marketplace per venderlo.

Gli NFT sono una tecnologia molto interessante, essi sono definiti anche come certificati di autenticità, grazie alla loro capacità di essere distinguibili l'uno dall'altro. Essi si possono collegare parallelamente ad un oggetto reale e renderlo unico e ineguagliabile digitalmente. Oggigiorno, Gli NFTs vengono utilizzati molto in campo artistico. Una persona crea un'immagine, la trasforma in un NFT sulla blockchain e di solito la vende. Questo permette all'acquirente di poter acquistare una sola copia di quella determinata opera d'arte, rendendo quest'ultima inimitabile, in quanto è presente un codice crittografico che la identifica come la sola opera d'arte digitale esistente. In questo modo, colui che possiede l'immagine sarà il proprietario effettivo di quell'opera. L'acquirente essendo possessore di un'opera d'arte anche lui potrà successivamente rivenderla. Molti sono gli utilizzi degli NFTs relativi al campo artistico e del collezionismo, ma essi trovano anche un ampio spazio nel settore industriale.

Blockchain, una tecnologia dirompente

Come si è potuto vedere, la blockchain è una tecnologia che ha riscosso molto successo nel corso degli ultimi anni. Essa è stata definita disruptive technology, ovvero una tecnologia innovativa che sostituisce completamente le altre già esistenti. In questo modo interrompe un mercato esistente e una rete di valori, sostituendosi ad esse.

In generale, una tecnologia dirompente influenza e modifica profondamente le abitudini di coloro che la utilizzano. Alcune volte cambiano persino gli usi e i costumi anche di popolazioni. Esempi di tecnologie dirompenti sono state: l'automobile, la quale ha stravolto completamente il trasporto fisico delle persone, il telefono, il quale ha permesso la comunicazione tra persone e la macchina fotografica digitale, che ha completamente sostituito l'uso del rullino.

Quindi, si può definire innovazione dirompente, qualunque nuova tecnologia che riesca a provocare nel breve periodo forti cambiamenti, che sia in grado di cancellare un mercato già esistente e crearne completamente uno nuovo. Oggigiorno, la blockchain appare essere tale, ovvero, una tecnologia dirompente.

Negli ultimi secoli, la tecnologia, è stato un fattore chiave nel mondo lavorativo e nel creare comodità alla società. Attraverso lo sviluppo di nuove tecnologie, si è assistito a dei cambiamenti radicali in tutti i settori lavorativi. Infatti, in tre secoli il modo di fare impresa è cambiato.

Con la prima rivoluzione industriale, si è riusciti a sostituire il lavoro manuale con quello affidato alle macchine. Questo attraverso l'aiuto delle prime macchine a vapore.

Con la seconda rivoluzione industriale, attraverso l'utilizzo di energia elettrica si sono create le prime linee di lavoro a catena di montaggio, per rendere più efficiente i tempi di lavorazione.

Con la terza rivoluzione industriale si è cercato di migliorare e perfezionare ancora di più la linea produttiva, aggiungendo al lavoro umano anche quello di robot e computer, per sostituire l'uomo in lavori monotoni e rischiosi per la propria salute.

Oggigiorno, si sta assistendo alla quarta rivoluzione industriale. L'obiettivo è una maggiore digitalizzazione, utilizzando tecnologie innovative sempre più sofisticate.

Queste ultime, in particolare sono: l'intelligenza artificiale, l'IoT, i Big Data e anche la blockchain, che insieme a quelle elencate precedentemente potrebbe apportare dei benefici significativi nei vari settori industriali.

Blockchain, una medicina per tutto?

A valle di ciò che si è detto è importante considerare che comunque la blockchain ha anche dei limiti. Non le si può attribuire a lei il rimedio a tutti i problemi che si vogliono risolvere.

Con gli anni la sua evoluzione e gli studi in campo informatico hanno effettivamente consentito di migliorare questa tecnologia e di permettere a quest'ultima di avere più sbocchi in differenti settori.

In basso sono presenti due grafici, il primo che mostra in percentuale l'applicazione della blockchain per ciascun settore, mentre il secondo racconta in che percentuale è applicata per ogni processo:

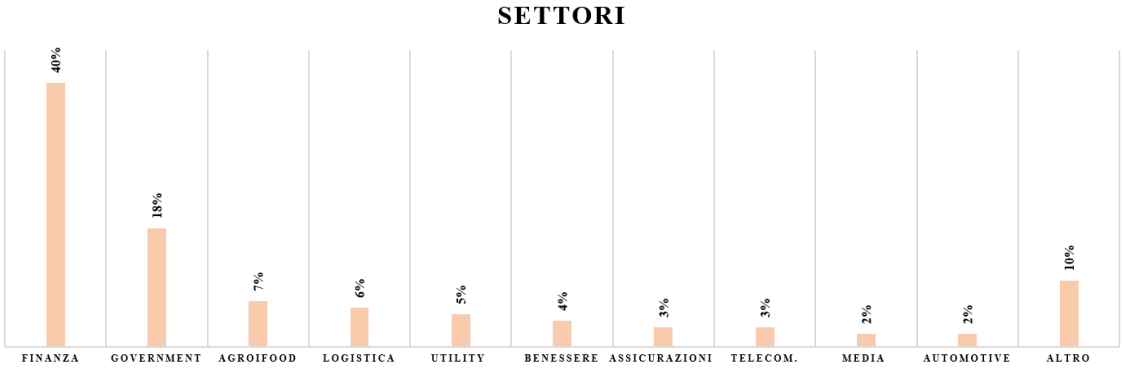

Grafico 4: Implementazione della blockchain (in percentuale) nei diversi settori. (Osservatori.net digital innovation. (2020). BLOCKCHAIN: THE HYPE IS OVER, GET READY FOR ECOSYSTEMS, Politecnico di Milano)

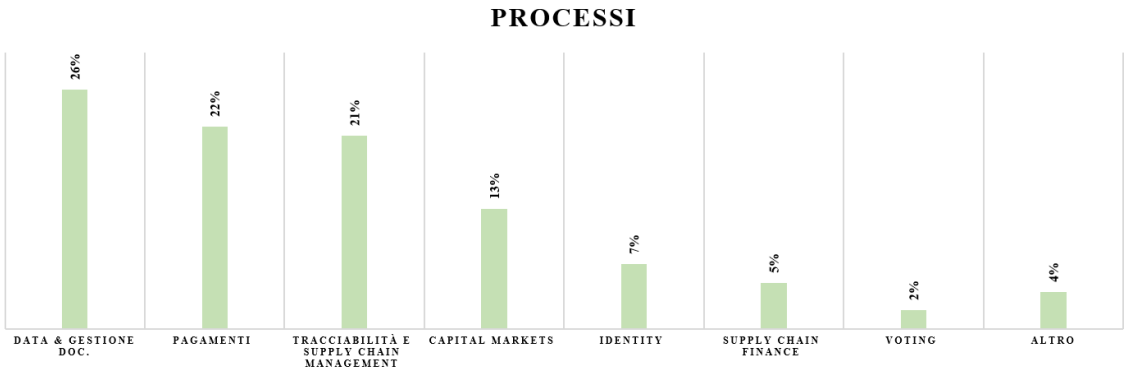

Grafico 5: Implementazione della blockchain (in percentuale) nei diversi processi (Osservatori.net digital innovation. (2020). BLOCKCHAIN: THE HYPE IS OVER, GET READY FOR ECOSYSTEMS, Politecnico di Milano.)

La blockchain di solito nell'applicazione ad altri settori non è unica, ha bisogno di essere accompagnata ad altre tecnologie (es. IoT e AI). Inoltre, essa tende a far cooperare le aree più disparate di una azienda, per esempio, il dipartimento legal e quello sviluppo e ricerca.

La blockchain per sua natura (essendo una tecnologia disruptive), il più delle volte tende a cambiare o a mutare profondamente l'organizzazione o la struttura aziendale. Infatti, è raro trovare applicazioni di blockchain che lasciano immutata una determinata area; per questo motivo non sempre questa tecnologia può essere applicata o utilizzata in alcune realtà. In alcuni casi essa può essere utile e avere un ruolo fondamentale, ma solo in specifiche situazioni. È importante quindi prendere in considerazione l'utilizzo di una soluzione basata su blockchain, se l'azienda ha in generale alcune di queste caratteristiche:

- **Ecosistema economico:** è quindi capace di gestire transazioni/relazioni tra un alto numero di imprese e organizzazioni;
- **Eterogeneità:** imprese e organizzazioni che hanno attività molto varie;
- **Disponibilità a far parte di una community**: che sia un distretto industriale, una filiera, una supply chain, si devono condividere obiettivi comuni;
- **Disponibilità a condividere i dati**: accordo sulla necessita di condividere dati e informazioni in modo strutturale;
- **Alto livello di digitalizzazione**: tutti gli attori coinvolti devono avere un alto livello di digitalizzazione (es. IoT, AI, Big Data...);

- **Trasparenza e immutabilità**: all'ecosistema in questione deve essere necessaria, o almeno utile, l'immutabilità dei dati e la loro trasparenza;
- **Governance**: serve la disponibilità a condividere regole, comportamenti, valori e processi.

Viceversa, la blockchain non risulta utile se l'azienda presenta le seguenti caratteristiche:

- **Singola azienda**;
- **Scarsa disponibilità alla condivisione e trasparenza**: aziende o attività che non vogliono condividere i propri dati;
- **Basso livello di digitalizzazione**;
- **Autonomia nella governance**: realtà che preferiscono non cambiare la propria gestione organizzativa e dei processi.

L'applicazione della blockchain all'interno delle funzioni aziendali avviene attraverso una rete di tipo privata, gestita da una governance centrale.

La Blockchain e le altre tecnologie

Sarebbe difficile che si verifichi una rivoluzione tecnologica in un determinato settore, se si facesse leva solo su una tecnologia. Infatti, molto spesso, alcune tecnologie hanno bisogno di camminare parallelamente e convergere in alcuni punti con altre, per poter fare in modo che insieme possano apportare dei benefici. Adesso, verranno analizzate alcune tecnologie che insieme alla blockchain possono essere definite abilitatori di nuovi servizi.

Internet of Things e Blockchain

Si introduce una delle prime tecnologie, che insieme alla blockchain possono divenire un binomio perfetto. La tecnologia che si introduce è l'Internet of Things (IoT), in italiano internet delle cose. Questa tecnologia nelle comunicazioni si riferisce all'estensione di Internet al mondo degli oggetti e dei luoghi concreti. (Wikipedia. (2021). *Internet delle cose, Wikipedia, L'enciclopedia libera*). Essa rappresenta l'evoluzione dell'uso della rete internet che oggi conosciamo. Invece, per quanto riguarda la blockchain, come già si è visto, è un sistema di archiviazione crittografato, utilizzato per creare dei registri sicuri e distribuiti.

Con l'unione di queste due tecnologie è possibile fare in modo che si ottengano i seguenti vantaggi:

- Supervisione: se le transazioni di dati avvengono attraverso organizzazioni diverse, un registro immutabile nel tempo è una garanzia dell'effettivo monitoraggio dei dati. Quindi, c'è la possibilità che i dati o i beni fisici possono essere tracciati lungo tutta la supply chain. In caso di perdita dati o di attacchi informatici, sarà facile capire il problema e trovare una soluzione.
  I dati che sono presenti all'interno di dispostivi IoT, sono dei dati sensibili ed è importante evitare che si verifichino attacchi informatici, per la sicurezza della privacy delle persone. Per questo motivo, nel momento in cui la blockchain è collegata al mondo IoT, è come se si aggiungessero dei livelli di sicurezza maggiori, in quanto la blockchain rende i dati immodificabili e sicuri.
- Fiducia: attraverso l'utilizzo della blockchain non ci sarebbe bisogno della presenza umana per supervisionare le transazioni. Inoltre, dal momento che non

si possiedono le chiavi private degli utenti, nessuno può sovrascrivere o modificare a proprio piacimento i registri nella blockchain.

- Accelerazione nella reperibilità dei dati: La blockchain, in questo campo, potrebbe permettere anche di ridurre le problematiche legate allo storage dei dati. Infatti, può sostituire gli attuali data center centralizzati con una propria rete. Essa stessa è duplicata tra più individui della rete. In questo modo, si genererebbe un'infrastruttura ridondante, la quale garantisce che i dati siano sempre a portata di mano, riducendo tempi di latenza lunghi ed evitando rischi come dei guasti o inaccessibilità ai server, compromettendone la rete stessa.
- Automazione: attraverso gli smart contracts è possibile rendere esecutivi degli accordi, confermati da apparati IoT, nel momento in cui delle condizioni accadano.

Artificial Intelligence e Blockchain

Un'altra tecnologia che potrebbe abbinarsi molto bene alla bockchain è quella dell'**artificial intelligence** (AI), in italiano intelligenza artificiale. Con quest'ultima si intendono tutte quelle tecnologie che riescono da sole a svolgere delle azioni, aventi bisogno di capacità di elaborazione. Questo avviene attraverso l'implementazione di machine learning. Il funzionamento di questa tecnologia dipende da *algoritmi* e dai *dati* che saranno elaborati.

Per quanto concerne la parte riferita all'immagazzinamento dei dati, potrebbe venire in aiuto la blockchain, in quanto per l'AI è di fondamentale importanza che i dati siano corretti ed immutabili (che è una caratteristica tipica del lavoro svolto dalla blockchain). Come si è detto, attraverso la blockchain, si possono gestire grandi quantità di dati ed evitare manomissioni. Infatti, questa tecnologia può permettere di conservare i dati cifrati e questo significa che solo le chiavi di cifratura hanno bisogno di essere mantenute al sicuro, evitando di allocare molta memoria come si fa per un classico database.

La tecnologia AI utilizza delle reti neurali per l'identificazione di trend e pattern con risultato finale una black-box. Essa genera una decisione in output in funzione delle tante micro-decisioni che ha preso attraverso la rete neurale, elaborando i dati. Al momento, con le classiche tecnologie, è difficile risalire alle micro-decisioni prese.

Attraverso la blockchain tutte le attività di auditing verrebbero semplificate, se tutte le micro-decisioni fossero registrate in una logica punto a punto, per poter verificare la correttezza dei vari algoritmi, aumentando così la fiducia del sistema.

In modo differente, anche l'intelligenza artificiale potrebbe conferire benefici alla blockchain. Infatti, si potrebbe pensare di applicare l'AI per analizzare i dati registrati in una blockchain. I dati nella blockchain, seppur anonimi e cifrati, sono registrati in modo pubblico. Attraverso l'AI si potrebbero riconoscere dei pattern che permettono di arrivare ad una parziale deanonimizzazione.

Le due, sono tecnologie molto diverse: l'AI presenta dati centralizzati e algoritmi complessi che non sono trasparenti, mentre la blockchain è contraddistinta da dati decentralizzati e immutabili, dalla sicurezza e infine dalla trasparenza. Unire queste due tecnologie potrebbe portare dei veri e propri vantaggi, in quanto si completano per alcuni aspetti l'una con l'altra.

Big Data e Blockchain

I Big Data, all'interno delle attività aziendali, stanno riscuotendo maggiore rilevanza. La blockchain potrebbe rivoluzionare completamente il modo di collezionare i dati.

Oggigiorno, poche aziende sono effettivamente in grado di avere a disposizione ingenti quantità di dati; mediante questi ultimi e attraverso sistemi di machine learning e intelligenza artificiale, le aziende riescono a migliorare i loro prodotti, offrendo servizi che possono essere sempre più su misura dei clienti.

Grazie alla blockchain, si potrebbe abbattere questo oligopolio di aziende grandi e potenti, le quali possono permettersi di possedere e gestire grandi quantità di dati, attraverso tecnologie hardware e software all'avanguardia. La blockchain, infatti, potrebbe fare in modo che gli utenti abbiano maggior controllo dei propri dati, in maniera sicura ed immutabile. L'utilizzo della blockchain applicata ai Big Data permette di dare la possibilità alle persone di vendere i propri dati (mediante smart contracts) a ricercatori o ad aziende che necessitano di informazioni per fare delle analisi. In questo modo, si potrebbe avere un mercato di dati aperto a chiunque, anche ad aziende di piccole dimensioni.

I dati che sono presenti all'interno di una blockchain sono anonimi e potranno essere certificati dagli utenti stessi. Inoltre, saranno immodificabili e le aziende che ne hanno bisogno possono comprarli dagli utenti che decidono di venderli, rinunciando così ad una parte della propria privacy. Ciò apporterebbe vantaggi a qualsiasi settore che oggi si basa sui dati.

La blockchain è adattabile anche a lavoro di Cloud computing. I Cloud computing consistono nell'erogazione di servizi di calcolo e di storage attraverso la rete internet. Ciò avviene in via configurabile, in funzione delle esigenze del cliente. Il termine Cloud computing è molto vago, infatti, viene utilizzato in vari contesti apportando valore aggiunto in maniera differente:

- **SaaS** (software as a service): programmi installati su un server remoto in collegamento via internet, in genere attraverso un server web;
- **PaaS** (platform as a service): a differenza del SaaS è eseguita l'intera piattaforma, piuttosto che i singoli programmi;
- **IaaS** (Infrastructure as a Service): oltre alle risorse software, sono messe a disposizione in remoto anche hardware come server o sistemi di memoria;
- **DaaS** (data as a service): Sono condivisi via web solamente i dati ai quali gli utenti possono accedere tramite qualsiasi applicazione come se fossero su un disco locale (Cloud Storage).

  (Bazzanella, D. (2021). *Applicazioni, Slide del corso Blockchain e criptoeconomia, Politecnico di Torino*).

Di solito il cloud computing viene fatto da remoto da un singolo server, però, si può verificare anche un distributed computing. Esso permette di suddividere il calcolo in più parti ed essere eseguito da una rete di server attraverso internet. Una evoluzione di quest'ultimo è mediante il Secure multi-party computation, che vincola tutti i computer che eseguono i calcoli a non essere in grado di risalire agli input e output dell'elaborazione.

L'applicazione della blockchain in questa tecnologia permetterebbe di gestire un calcolo distribuito in modo sicuro su una rete di computer, garantendo maggiore sicurezza, resilienza ed immutabilità dei dati. La blockchain, quindi, permetterebbe di migliorare

di gran lunga il cloud computing; infatti, molte aziende stanno cercando di migliorare queste ultime.

La Blockchain e le sue applicazioni nei principali settori

Come è stato già detto, la blockchain, non è una tecnologia che è valida per tutti i settori o tutte le imprese, bisogna valutare se essa possa avere una reale applicazione nel settore dove la si vuole applicare, se apporta effettivamente dei vantaggi e quale sia il costo dell'implementazione di quest'ultima. I principali settori che verranno analizzati saranno i seguenti:

- **Finanziario**
- **Assicurativo**
- **Farmaceutico**
- **Energetico**

Infine, si darà uno sguardo alla **Supply chain**, in quanto è un macro-processo che è presente in qualsiasi tipo di realtà produttiva.

Blockchain per il settore finanziario

Uno dei settori, dove la blockchain assume una funzione maggiormente dirompente e che quindi può provocare il punto di non ritorno a quello che è il sistema tradizionale, è quello del mondo bancario. Infatti, la Decentralized Finance (DeFi), sta assumendo e acquisendo spazi di dimensioni notevoli. La Decentralized Finance è l'insieme di nuovi strumenti finanziari basati su reti già decentralizzate che ne sfruttano le opportunità (es. smart contracts, token e NFT) per poter ricreare i servizi finanziari già conosciuti, però con la caratteristica di non avere bisogno di una terza parte (es. intermediario). Questo grazie alla blockchain, la quale permette di creare un sistema sicuro senza la presenza di un operatore finanziario.

Il funzionamento del mondo finanziario (in maniera semplicista) è quello che chi possiede un capitale lo fornisce alla banca in cambio di interessi. Invece, la banca presta il denaro a coloro che lo richiedono, per i propri bisogni, a fronte della restituzione della somma ricevuta con l'aggiunta degli interessi. Questo ragionamento, seppur molto

semplificato, potrebbe essere ripreso anche all'interno di una struttura blockchain, saltando gli intermediari.

Colui che necessita di capitale si accorda con colui che lo offre momentaneamente, in cambio di interessi. La certezza di tale operazione è che tutto è garantito attraverso lo smart contract, il quale verrà stipulato tra le due parti. Nel caso, una parte non possa restituire la somma di denaro alla scadenza, lo smart contract attiverà automaticamente delle clausole che costringono colui che ha richiesto il prestito ad impiegare altre risorse per poter saldare il debito.

Al momento, questo sistema, non può sostituire completamente quello bancario, però negli ultimi anni le piattaforme DeFi stanno registrando valori molto alti di denaro scambiato e di utenza, come si può vedere dal grafico in basso.

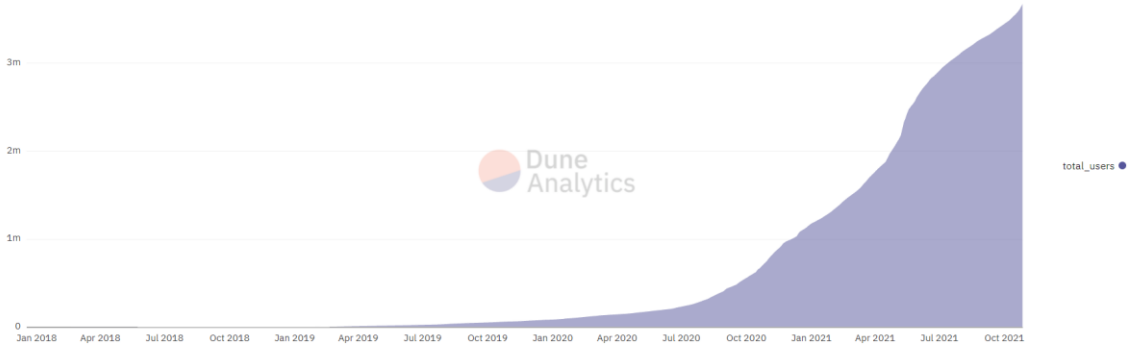

Grafico 6: Numero totale di users che utilizzano piattaforme DeFi. Dune Analytics. (2021).

Nonostante la blockchain sia sicura, è comunque di fondamentale importanza che ci siano dei controlli. Essa non permette nessuna certezza sulla correttezza dei dati. Infatti, se si aggiungessero dei dati falsi all'interno della blockchain, questi ultimi, rimarrebbero tali. Quindi affidare parte dei risparmi ad una piattaforma DeFi, pensando che la blockchain sia sicura in termini di inattaccabilità, non è una buona decisione. Per il momento è importante che gli utenti sappiano che possano verificarsi degli scam e quindi è fondamentale che le persone si informino bene.

La principale necessità è cercare una soluzione che permetta di evitare che queste truffe si verifichino (azioni che non dipendono dalla logica DeFi o dalla blockchain, bensì dalla mal intenzione degli esseri umani).

Blockchain per le Assicurazioni

Anche il mondo delle assicurazioni potrebbe subire una totale mutazione attraverso l'utilizzo della blockchain. Essa potrebbe apportare anche in questo campo maggiore trasparenza ed efficienza nelle operazioni. In questi ultimi anni, le transazioni digitali hanno posto le agenzie di assicurazione davanti al problema di come proteggere la sensibilità dei dati dei propri utenti e rendere più efficace il sistema.

La blockchain, nel campo assicurativo, potrebbe favorire questi aspetti garantendo maggiore sicurezza con un registro pubblico, condividere la mole di dati che sono presenti, garantire l'aumento delle transazioni e migliorare la flessibilità dei contratti attraverso l'uso degli smart contracts.

Per migliorare il sistema delle assicurazioni sono già diffusi dei sistemi di Insurance Telematics che sarebbero delle assicurazioni con tecnologia IoT che rilevano i dati dei clienti e permettono loro di personalizzare il proprio servizio.

Nel caso si considerassero le assicurazioni sulle autovetture, potrebbero esistere dei sistemi molto flessibili, in funzione delle necessità del cliente. Per esempio, potrebbero esserci dei sistemi come:

Pay-per-use: che sono contratti assicurativi in funzione dei chilometri che un utente assicurato compie e non in funzione solo del tempo. Utile per persone che comunque fanno poco utilizzo della macchina.

Pay-as-you-drive: Servizio assicurativo che pone una polizza in funzione del modo di guida del conducente, inducendo anche i clienti ad avere uno stile di guida più pulito e sicuro così da permettere un sistema win-win.

Il funzionamento per tali tipi di polizze assicurative funziona attraverso gli smart contracts. L'utente e l'assicuratore attivano insieme uno smart contract e nel caso del pay-per-use, i km vengono trasmessi in tempo reale attraverso tecnologia IoT alla rete e il cliente è coperto dall'assicurazione fino allo scadere di questi ultimi. Al raggiungimento dei km, si possono attivare delle clausole automatiche per acquistare km aggiuntivi oppure si verifica l'obbligo di rinnovo della polizza.

Le assicurazioni potrebbero avere moltissimi campi applicativi dal momento che loro hanno una capacità maggiore di customizzazione. Per esempio, potrebbero essere fatte delle assicurazioni nel settore turistico mediante gli smart contracts. In questo caso, un utente, pagando una polizza meteo, avrebbe un rimborso nel momento in cui le condizioni meteo siano avverse, in quanto non permettono di usufruire del proprio soggiorno.

La blockchain potrebbe trovare spazio per il campo delle assicurazioni anche sui ritardi dei trasporti di passeggeri. Per esempio, nel momento di acquisto del biglietto aereo, si attiva uno smart contract, dove l'oracolo fornirà i dati delle partenze/arrivi dei voli, e in caso si presentassero dei ritardi, verranno generati dei rimborsi automatici.

La blockchain in questo contesto potrebbe insediarsi molto bene. Infatti, potrebbe generare i seguenti benefici:

- **Immodificabilità dei dati**;
- **Sicurezza delle informazioni:** Dati che a valle della validazione non possono essere alterati all'interno della blockchain;
- **Trasparenza e Tracciabilità:** condivisione di dati tra tutti gli attori coinvolti e verifica dei dati per generare le polizze personalizzate;
- **Automatizzazione:** procedure di richiesta di risarcimento o rimborsi automatizzati attraverso gli smart contracts, riducendo i numeri di intermediari;

EY e aziende di consulenza di spiccata rilevanza hanno più volte denunciato che il mondo assicurativo per migliorare il proprio servizio in termini di costi, tempi e customer satisfaction dovrà usufruire della tecnologia blockchain. (PCA. (2019). *Le soluzioni della Blockchain per le assicurazioni*)

Blockchain per il Voto elettronico

Questa tipologia di voto permette alla popolazione di esprimere la propria idea politica in modalità remoto, attraverso un sistema informatico. Al momento, questo processo è molto difficile che avvenga in maniera efficace, in quanto, sfruttando solo dei database, il sistema di votazione non è affidabile.

In questo caso si andrebbe incontro a problemi come l'affidabilità del sistema, la trasparenza e per ultimo la duplicazione del voto tramite attacchi hackers. La blockchain invece potrebbe permettere di superare queste difficoltà rendendo questa modalità di votazione un ottimo strumento per il popolo. Alcuni paesi come Svizzera, Estonia e Canada hanno già provato ad utilizzarlo con degli ottimi risultati.

Attraverso l'utilizzo della tecnologia blockchain per questa logica sono presenti molti benefici quali:

- Maggiore comodità;
- Risparmio delle risorse in termini di tempo e costi;
- Possibilità di far votare anche persone che si trovano in luoghi diversi (sul territorio nazionale o all'estero) da quello dove si può votare.

Ciò migliorerebbe di gran lunga la qualità del voto e i cittadini sarebbero maggiormente coinvolti a prendere parte al voto.

Per il voto elettronico, il miglior protocollo da utilizzare è il **Proof of Authority** (PoA), che presenta un numero di gestori affidabili della blockchain. Ogni votante invia il proprio voto a più gestori e successivamente si applica il protocollo di consenso accettando quel determinato voto. L'accettazione avviene solo se la maggioranza dei nodi che consentono la validità del voto siano d'accordo.

La blockchain, nonostante possa garantire sicurezza per le transazioni che avvengono, ha dei punti deboli. Infatti, quest'ultima non può garantire che il voto non subisca influenza esterna durante il processo di votazione. Infatti, nell'atto di espressione del voto si potrebbero verificare problemi come:

- Attacchi hacker sul terminale da cui si sta votando, compromettendo il voto;
- Intimidazioni o manipolazioni nei confronti di persone che stanno per votare; infatti, nessuno potrebbe sapere cosa accade dall'altra parte del computer mentre una persona sta votando.

Inoltre, si potrebbe verificare anche un problema dal lato governance. Il gestore del server raccogliendo i dati ha la possibilità di barare compromettendo i dati stessi,

oppure potrebbe subire anche lui un attacco informatico, non garantendo la sicurezza di questi ultimi.

Nel caso si parlasse di elezioni politiche, molti sono i soggetti interessati ad investire per governare una nazione e nessun sistema informatico rende sicura la votazione elettronica dai rischi precedentemente citati.

La comunità informatica italiana, unendosi alle preoccupazioni degli USA, ha annunciato i rischi del voto elettronico nelle elezioni politiche sottolineando che nessuna tecnologia al momento, persino la blockchain, possa garantire la sicurezza del voto elettorale.

Nonostante ciò, comunque la blockchain potrà trovare con il tempo, attraverso ricerche e l'aiuto di altre tecnologie, più spazio anche in questo ambito, grazie alle sue qualità e al suo potenziale.

Blockchain per il Settore energetico

Al momento, il settore energetico, è un settore molto frammentato; infatti, si trovano sia grandi produttori energetici che piccoli, i quali utilizzano soluzioni innovative e alternative. La blockchain, essendo una tecnologia decentralizzata e gestendo transazioni, appare ideale per questo settore.

Fino a qualche anno fa, il settore energetico, era molto centralizzato ed erano presenti solo grandi produttori e grandi distributori.

Con gli anni sono nate anche piccole realtà che hanno reso questo sistema simile ad un network. Quest'ultimo però appare sempre centralizzato, in quanto tutti i piccoli produttori, che possiedono poco potere contrattuale, fanno capo alle grandi aziende del settore per poter vendere. Oggi, i piccoli produttori si sentono costretti a vendere l'energia ad un prezzo più basso ai grandi produttori che a loro volta la vendono ai consumatori finali.

Quindi il network è distribuito in una complessa rete di attori, dai produttori ai consumatori, con capacità rispettivamente di produzione e di consumo molto diverse tra di loro.

Il mercato con il tempo ha mutato profondamente, infatti si è passati da una modalità di business di tipo B2C ad una di tipo B2B2C e in un secondo momento anche una parte della rete C2B2C.

Grazie alla Blockchain si potrebbe fare in modo che al modello di business B2B2C si unisca anche il modello C2C, con possibilità di estendersi anche al C2B.

Infatti, molto spesso, i consumatori stessi sono anche dei produttori di energia, questa categoria è definita prosumer, crasi anglosassone tra producer e consumer.

Dato che con il tempo, il numero di prosumer sono aumentati a dismisura, il modello centralizzato si sta rivelando sempre meno vantaggioso per questi ultimi, in quanto loro, come i piccoli produttori, sono costretti a vendere a dei big dell'energia con dei prezzi ovviamente minori e meno vantaggiosi.

Attraverso la blockchain, si sta andando verso un modello decentralizzato, dove i prosumer o i piccoli produttori possono attuare forme transazionali a livello locale. In questo modo si può applicare il P2P energetico con la blockchain che gestisce le transazioni, identità, monitoraggio dei consumi e i pagamenti. In questo caso, attraverso la blockchain, si potrebbero collegare anche i prosumer e i produttori direttamente ai consumatori finali, senza passare per i grandi produttori e distributori di energia.

Un'altra soluzione, più ambiziosa, sarebbe quella che, attraverso l'organizzazione e il coordinamento di un ecosistema di prosumer, l'energia prodotta in eccesso contribuisca a rispondere al fabbisogno energetico di aree geografiche che ne hanno maggiormente bisogno. Si parla così di smart grid, ovvero rete intelligente.

In questo caso la rete è riorganizzata e coordinata in base alla quantità di energia immagazzinata dai vari attori. Questo progetto farebbe in modo di non allocare energia inutile in alcune aree che sono già sufficientemente fornite, così da evitare che l'energia in eccesso si perda. Infatti, questa energia potrebbe essere distribuita in parti dove ce ne è più carenza, evitando di utilizzare metodi più dannosi per l'estrazione. Quindi, l'energia in eccesso che andrebbe persa, attraverso un marketplace blockchain verrebbe velocemente allocata in punti dove si ha bisogno.

Attraverso la blockchain, si potrebbe creare un mercato dell'energia distribuito. Quest'ultima grazie anche alla tecnologia IoT, potrebbe gestire in modo automatico,

trasparente ed economico tutta la rete. Infatti, queste ultime permetterebbero una comunicazione tra le varie parti e/o tecnologie interessate, portando ad un grande risparmio di energie ed evitando il problema di perdita energetica.

In questo caso, la blockchain non rivoluzionerebbe semplicemente questo settore ma creerebbe un nuovo mercato aperto a tutti. Anche i prosumer potrebbero vendere direttamente ai clienti finali o ad altre aziende. In questo modo, l'energia in eccesso, che non rientra nel fabbisogno del piccolo produttore, può essere trasferita direttamente ad un cliente che ne necessita, distribuendo l'energia in maniera efficiente.

Blockchain per il settore Farmaceutico

Un ultimo campo che si analizza, prima di passare a quello della supply chain, è quello del settore Farmaceutico. In questo ambito sono molto sentite le problematiche legate alla contraffazione dei farmaci e agli usi impropri; per questi motivi il settore è fortemente regolato da leggi severe.

Attraverso l'utilizzo di registri, si possono tracciare tutti i segmenti della supply chain sia per lotti che per singolo parcel, combattendo così la contraffazione dei medicinali. La blockchain può essere adattata a qualsiasi tipo di industria farmaceutica, trovando vantaggio anche per industrie di piccole dimensioni. In questo campo, attraverso la blockchain è immediata anche la riconciliazione tra la consegna del farmaco e i pagamenti da parte dei servizi sanitari. Questo potrebbe verificarsi attraverso l'utilizzo degli smart contracts.

Oltre che nella supply chain, la blockchain per il pharma può apportare migliorie anche in altri modi. Una delle applicazioni più interessanti riguarda quella dei test clinici e sperimentali in ambito farmacologico. Essi garantiscono confidenzialità e integralità dei dati ai pazienti che partecipano. La tecnologia potrebbe dare la possibilità di memorizzare l'identità dei partecipanti e rende possibile alle aziende del pharma l'accesso e la condivisione di tali informazioni aggiornate, in base ai progressi della sperimentazione. Tale modello, garantirebbe allo stesso tempo anche anonimato e nuovi modelli collaborativi. Infatti, i pazienti potrebbero venire a conoscenza di come e in quale misura i propri dati abbiano potuto essere utili nel settore farmaceutico aumentando la fiducia dei partecipanti nei confronti delle aziende farmaceutiche.

Blockchain per la supply chain

Fino ad ora si è dato uno sguardo alle applicazioni della tecnologia blockchain in alcuni settori specifici e come quest'ultima possa apportare i propri vantaggi. Ora, si andrà a descrivere come questa tecnologia avvantaggi la supply chain, area molto vasta che è appartenente un po' a tutte le tipologie di aziende produttrici.

Anche in questo caso, la blockchain figurerebbe come una tecnologia dirompente, mutando profondamente quelli che sono i modi di lavorare di un'organizzazione e sostituendosi o integrandosi ad alcuni sistemi informativi già utilizzati in azienda. Gli strumenti che in questo caso sono utilizzati maggiormente sono gli smart contracts e gli NFTs.

Riguardo gli NFTs si potrebbe pensare di crearli in modo che ognuno di loro sia collegato ad un prodotto o materiale reale, presentando le caratteristiche di questi ultimi all'interno della blockchain. In questo modo ogni NFT corrisponde ad un determinato prodotto e ognuno di esso racconta la storia del prodotto all'interno di tutta la filiera della supply chain (es. il tipo di lavorazione, il tipo di trasporto, la conservazione in magazzino e al di fuori di esso…). Inoltre, attraverso gli NFTs è più semplice gestire anche i prodotti a magazzino e utilizzare politiche di movimentazione e di picking più accurate.

L'analisi del settore della supply chain avverrà dividendo quest'ultima in tre processi:

- Pianificazione degli approvvigionamenti e della domanda;
- Gestione dei flussi logistici;
- Produzione.

Per la supply chain è importante che la blockchain sia condivisa tra i vari attori, con le relative informazioni. È fondamentale che avvenga la comunicazione tra esse e quindi che i partner esterni siano in possesso anche loro di una propria blockchain.

Blockchain per la pianificazione degli approvvigionamenti e della domanda

In questo processo della supply chain, la blockchain, si propone principalmente di migliorare l'accuratezza della domanda e di fare in modo che si attivino alcuni processi in maniera del tutto automatico. In questa fase, di particolare rilievo sono gli mart

contracts. I tre attori che riguardano la fase di pianificazione della domanda e degli approvvigionamenti sono:

Supplier: i fornitori della materia prima;

Retailer: coloro che richiedono la merce;

Distributor: gli attori che hanno la responsabilità di trasporto della materia.

I vantaggi della blockchain per questi tre attori, si hanno nel momento in cui avviene la comunicazione tra le proprie blockchain. Se ognuno condividesse una parte della propria blockchain, ogni attore, saprebbe cosa fare in anticipo. Infatti, il retailer potrebbe stipulare uno smart contract con il supplier, che nel momento in cui si trovi sottoscorta, lui verrà automaticamente rifornito. Se fosse incluso anche il distributor all'interno dello smart contract, anche quest'ultimo potrebbe pianificare in anticipo la spedizione. In questo caso ogni attore dovrà possedere delle proprie chiavi per avere accesso alle transazioni scritte sul registro della blockchain, così da permettere di poter rispondere al proprio ruolo.

Oltre alla velocità con cui possono essere fatte alcune azioni in termini di approvvigionamento o di vendita, è possibile permettere un accuratissimo livello di pianificazione. Questo perché, se le varie blockchain sono condivise tra di loro, ogni attore riuscirebbe a pianificare in funzione degli ordini del proprio cliente.

Per esempio, un supplier potrebbe essere a conoscenza degli ordini del retailer e del client di quest'ultimo e così potrebbe pianificare la propria produzione in funzione della domanda a valle della supply chain.

A sua volta, anche il retailer, sapendo quanto materiale serve al cliente in funzione delle sue vendite e dei suoi ordini, potrebbe pianificare al meglio le attività di approvvigionamento e di produzione nel medio/breve periodo.

Un po' come il sistema informativo VMI, attraverso la blockchain, si potrebbe cercare di "gestire" il magazzino del proprio cliente, così da rifornirlo sempre in tempo e fare in modo che la propria attività non abbia problematiche di pianificazioni.

Inoltre, questo sistema creerebbe delle vere e proprie partnership tra i diversi attori, dove uno dei requisiti fondamentali per questi ultimi è quello di avere una blockchain condivisibile così da poter permettere a tutti di lavorare con la massima efficienza.

Gestione dei flussi logistici

Sia per quanto concerne la fase di distribuzione, sia per la gestione dei flussi interni ai magazzini, la blockchain può essere uno strumento molto utile. In precedenza, si è visto, che per un distributore la condivisione della blockchain gli permette di pianificare i propri viaggi/trasporti con largo anticipo. In questo modo, il distributore è sempre in linea con le tempistiche scritte sugli smart contracts, stabiliti tra i propri clienti.

È importante che durante la fase di trasporto, durante l'attività logistica e durante la fase di movimentazione merci sia tutto monitorato, ovvero che su ogni tipo di materia prima e su ogni prodotto finito, si possa avere la possibilità di tracciare il prodotto.

Nel campo della movimentazione, attraverso gli NFTs, che sono collegati con un codice univoco segnato sul prodotto stesso, si potrebbe percorrere tutta la movimentazione dello stesso. Oltre a tracciare la storia del prodotto, attraverso le tecnologie IoT c'è la possibilità di monitoraggio della merce in tempo reale. In questo modo si può avere maggiore tracciabilità dei singoli prodotti e avere più cura di essi aumentandone la qualità.

Attraverso la blockchain, sarebbe così tutto tracciato, si delinea in maniera più precisa la responsabilità delle varie parti e le informazioni sono al sicuro in quanto gli NFTs non possono essere distrutti, eliminati o copiati senza autorizzazione.

Gestione della produzione

L'intervento della blockchain in questo processo è più complicato da applicare. Nell'area produzione, l'attività che può svolgere la blockchain dipende molto dal layout produttivo.

Per esempio, se si prendesse in considerazione la **produzione per progetto**, essa non è standardizzabile, in quanto il lavoro è in funzione di ogni singolo ordine e quindi è più complicato utilizzare la blockchain. L'utilizzo degli smart contracts è inutile in quanto la trascrizione del progetto è sicuramente molto difficile, essendo specifica di un

determinato progetto. Inoltre, in questo caso, i miglioramenti in termini di tempistiche sono difficili da poter percepire.

Un impiego interessante è l'applicazione della blockchain in ambienti dove i volumi di produzione sono medio-alti e la produzione deve essere abbastanza flessibile. Un esempio che calza a pennello è la produzione per lotti, dove ogni lotto ha una parte della produzione che si differenzia da quella di altri lotti.

In quest'ultimo caso è possibile standardizzare più facilmente i processi nonostante la tipologia di produzione sia molto flessibile. Se in questo caso venisse accompagnata alla blockchain anche la tecnologia IoT sarebbe perfetto, in quanto tutto il reparto produttivo potrebbe comunicare.

Attraverso la tecnologia IoT e gli smart contracts si verifica che le lavorazioni avvengono in maniera autonoma anche per ordini differenti. La tecnologia IoT permette di far comunicare le varie parti del reparto produttivo, mentre gli smart contracts, nel momento che si compiono delle determinate clausole, permettono di avviare delle nuove fasi di produzione o movimentazione merci.

Per esempio, se si considerassero dei robot che hanno finito la lavorazione di un lotto e questi ultimi devono passare ad un lotto successivo (con un differente tipo di lavorazione) allora verrà attivata una clausola dello smart contract, la quale permetterà a tutti i robot di prepararsi per questa nuova attività lavorativa. Infatti, se il sistema riconoscesse il lotto da lavorare tramite un codice univoco che identifica quel lotto, la macchina farebbe avvenire direttamente il setup, impostando i propri parametri per la lavorazione di quel determinato lotto. Così, sia le fasi di cambio lavorazione che quelle di setup potrebbero essere più veloci e presentare meno sprechi di tempo.

Benefici della Blockchain nella supply chain

Essendo la supply chain un'area molto vasta che è associabile a qualsiasi tipo di impresa di produzione, si può concludere che la blockchain potenzialmente, in maniera differente, si può applicare a tutti i settori che hanno una filiera produttiva. Sicuramente in alcuni campi può trovare una migliore applicazione che in altri. I vantaggi che essa apporta sono notevoli in alcune aree della supply chain:

- Garantisce maggiore tracciabilità e monitoraggio dei singoli prodotti lungo tutta la filiera;
- Consente una migliore pianificazione della domanda e anche delle attività di approvvigionamento, con conseguente miglioramento anche nella schedulazione della produzione e distribuzione;
- Riduzione di sprechi e costi legati alle attività di produzione e di movimentazione della merce;
- I prodotti possono essere anche certificati più velocemente attraverso la blockchain.

  Un prodotto potrebbe essere sottoposto a controlli dove, nel caso di superamento di questi ultimi, si attiverebbero delle clausole di uno smart contract, generando la certificazione per il prodotto. Questa attività si potrebbe espandere anche a livello di processi.
- Processi più standard e monitorati;
- Maggiore sicurezza informatica, in quanto la blockchain di per sé è immutabile;
- Consente di mostrare l'originalità del prodotto. Infatti, un cliente attraverso la blockchain, potrebbe vedere se un prodotto sia effettivamente originale, in quanto può risalire a tutta la sua filiera di produzione, partendo dalle materie prime.

Conclusioni

Le conclusioni che possono essere tratte, attraverso le analisi fatte, è che effettivamente la blockchain non ferma i suoi spazi applicativi solo al mondo delle criptomonete e dei servizi finanziari. Bensì essa trova applicazioni in svariati settori in maniera trasversale e in molti casi si insedia in maniera dirompente rispetto ai modelli già presenti.

Al momento c'è ancora bisogno di attività di ricerca per poter raggiungere l'obiettivo di utilizzarla in qualsiasi tipo di settore. Nonostante i costi abbastanza elevati e influenti nell'attività di business, quest'ultima è effettivamente la soluzione a molti problemi che al momento sono ancora presenti.

Si conclude così che questa giovane tecnologia possa essere il punto di inizio per aumentare i valori che un'azienda vuole trasmettere attraverso il proprio prodotto e i servizi per la società. Con la blockchain, si rendono più semplici dei processi che non possono essere migliorati se non con l'utilizzo di essa stessa.

Bibliografia

Wikipedia. (2021). *Crittografia, Wikipedia, L'enciclopedia libera*. //it.wikipedia.org/w/index.php?title=Crittografia&oldid=122445846

Bazzanella, D. (2021). *Gergo Basilare, Slide del corso Crittografia, Politecnico di Torino*.

Bazzanella, D. (2021). *Slide del corso Crittografia, Politecnico di Torino.*

Wikipedia. (2020). *Libro mastro, Wikipedia, L'enciclopedia libera.* //it.wikipedia.org/w/index.php?title=Libro_mastro&oldid=116488069.

Wikipedia, (2021). *Bitcoin, Wikipedia, L'enciclopedia libera.* //it.wikipedia.org/w/index.php?title=Bitcoin&oldid=123712952.

Cavicchioli, M (2018). Cos'è e come funziona il Double-Spending. https://medium.com/@marcocavicchioli/cos%C3%A8-e-come-funziona-il-double-spending-390b737fb255

Blockchain. (2021). *Wikipedia, L'enciclopedia libera.* //it.wikipedia.org/w/index.php?title=Blockchain&oldid=123726728.

Frankenfield J. (2021). Proof of Work (PoW) https://www.investopedia.com/terms/p/proof-work.asp

Bazzanella, D. (2021). *Strumenti, Slide del corso Blockchain e criptoeconomia, Politecnico di Torino.*

Bazzanella, D. (2021). *Bitcoin, Slide del corso Blockchain e criptoeconomia, Politecnico di Torino.*

Ittai A. (2020). *The first Blockchain or how to Time-Stamp a Digital Document https://decentralizedthoughts.github.io/2020-07-05-the-first-blockchain-or-how-to-time-stamp-a-digital-document/*

Bit2me Academy (2021). Cos'è un albero di Merkle? https://academy.bit2me.com/it/cos%27%C3%A8-un-albero-di-merkle/

Bazzanella, D. (2021). *Introduzione alla Blockchain, Slide del corso Blockchain e criptoeconomia, Politecnico di Torino.*

Ledger Academy. (2019) *What is Proof-of-Work* https://www.ledger.com/academy/blockchain/what-is-proof-of-work

Porta M. (2019) *Cos'è un Fork di una criptovaluta e quali effetti produce, Cryptonomist* https://cryptonomist.ch/2019/07/27/fork-criptovaluta-spiegazione/

Binance Academy. (2021). *Vantaggi e Svantaggi della Blockchain* https://academy.binance.com/it/articles/positives-and-negatives-of-blockchain

Bazzanella, D. (2021). *Protocolli di consenso, Slide del corso Blockchain e criptoeconomia, Politecnico di Torino.*

Statista. (2021). *Bitcoin price from October 2013 to September 2021* https://www.statista.com/statistics/326707/bitcoin-price-index/

Statista. (2021). *Market capitalization of Bitcoin from April 2013 to September 2021* https://www.statista.com/statistics/377382/bitcoin-market-capitalization/

Statista. (2021). *Size of the Bitcoin blockchain from January 2009 to September 2021* https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

Smart contract. (2021). *Wikipedia, L'enciclopedia libera* //it.wikipedia.org/w/index.php?title=Smart_contract&oldid=123585482.

Perez R. (2020) Cos'è un Oracle Blockchain, Bitnovo https://blog.bitnovo.com/it/che-cosa-e-un-oracolo-blockchain/

Poma B. (2021). *Cosa sono gli Smart Contract: Applicazioni, vantaggi e limiti*, *finaria* https://www.finaria.it/criptovalute/smart-contract/

Guida G. (2020). *Blockchain e smart contract: benefici e limiti Altalex* https://www.altalex.com/documents/news/2020/10/21/blockchain-smart-contract-benefici-limiti

Jovacchini L. e Nardella P. (2020). *Token: cos'è e come viene utilizzato nelle criptovalute Blockchain 4innovation Netwok Digital 360* https://www.blockchain4innovation.it/criptovalute/token-cose-come-viene-utilizzato/

Wikipedia. (2021). *Non-fungible token, Wikipedia, L'enciclopedia libera* //it.wikipedia.org/w/index.php?title=Non-fungible_token&oldid=123713326.

Caccioppoli V. (2021). *DeFi: cresono ancora i volumi sulle piattaforme di finanza decentralizzata,* The Cryptonomist https://cryptonomist.ch/2021/09/20/defi-crescono-i-volumi-sulle-piattaforme/

Dune Analytics. (2021). https://dune.xyz/rchen8/defi-users-over-time

PCA. (2019). *Le soluzioni della Blockchain per le assicurazioni*, https://www.pcabroker.com/le-soluzioni-della-blockchain-per-le-assicurazioni/

Bellini M. (2020). *La Blockchain per le imprese, Come prepararsi alla nuova "Internet of Value".*

Portale V. (2018). *Osservatori.net digital innovation* https://blog.osservatori.net/it_it/dapp-blockchain-cosa-sono

Bazzanella, D. (2021). *Applicazioni, Slide del corso Blockchain e criptoeconomia, Politecnico di Torino.*

Wikipedia. (2021). *Internet delle cose, Wikipedia, L'enciclopedia libera*. //it.wikipedia.org/w/index.php?title=Internet_delle_cose&oldid=123669632.

M. Zimmerman (2020). *AAAS, Letter to Governors and Secretaries of State on the insecurity of online voting.* https://www.aaas.org/programs/epi-center/internet-voting-letter

Ministero dell'interno. (2021). https://www.interno.gov.it/sites/default/files/2021-07/linee_guida_voto_elettronico_decreto_9.7.2021.pdf

Osservatori.net digital innovation. (2020). BLOCKCHAIN: THE HYPE IS OVER, GET READY FOR ECOSYSTEMS, Politecnico di Milano. https://www.osservatori.net/it/ricerche/infografiche/blockchain-hype-is-over-get-ready-ecosystems-infografica