



UNIVERSITÀ
POLITECNICA
DELLE MARCHE

FACOLTÀ DI INGEGNERIA
CORSO DI LAUREA IN INGEGNERIA INFORMATICA E DELL'AUTOMAZIONE

Funzionamento e Applicazioni della Tecnologia "Block-Chain"

Operation and Applications of "Block-Chain" Technology

Candidato:
Antonio Bandello

Relatore:
Prof. Simone Fiori

Anno Accademico 2021-2022

INDICE

INTRODUZIONE	3
---------------------	----------

CAPITOLO 1	
ORIGINE E FUNZIONAMENTO DELLA BLOCKCHAIN	4
1.1 Origine della Blockchain	4
1.2 Bitcoin rimedio al fenomeno del Double Spending	5
1.2.1 Brute Force Attack	
1.2.2 Majority Attack	
1.3 La cittografia a servizio della Blockchain	7
1.4 Caratteristiche della Blockchain	8
1.4.1 Decentralizzazione	
1.4.2 immutabilità	
1.4.3 Sicurezza	
1.4.4 Trasparenza	
1.4.5 Tracciabilità	
1.5 Componenti della Blockchain	12
1.5.1 Le Transazioni	
1.5.2 I Nodi	
1.5.3 Wallet	
1.5.4 Ladger	
1.5.5 i Blocchi	
1.5.6 i Codici Hash	
1.5.7 i Miners	
1.5.8 I principali meccanismi di consenso pow & PoS	
1.5.9 I Forks	
1.6 Struttura di un sistema	19
1.6.1 Centralized Ledger	
1.6.2 Decentralized Ledger	
1.6.3 Distributed Ledger	
1.7 Blockchain pubbliche o private	21
1.8 I token	23

CAPITOLO 2	
AMBITI DI APPLICAZIONE E PRINCIPALI SETTORI	25
2.1 Ambiti di applicazione	25
2.1.1 Finanziario	
2.1.2 Assicurativo	
2.1.3 Marketing e Digital Advertising	
2.1.4 Energetico	
2.1.5 Copyright	
2.2 Amministrazione pubblica	30
2.2.1 Sanitario	
2.2.2 L'e-Government	
2.2.3 L'e-Voting	
2.2.4 Sistemi di tassazione	

CONCLUSION	34
-------------------	-----------

BIBLIOGRAFIA	35
---------------------	-----------

SITOGRAFIA	38
-------------------	-----------

CAPITOLO 1

ORIGINE E FUNZIONAMENTO DELLA BLOCKCHAIN

1.1 Origine della Blockchain

La rivoluzione informatica (anche detta rivoluzione digitale) è il passaggio della tecnologia meccanica ed elettronica analogica a quella elettronica digitale che, iniziata durante i tardi anni Cinquanta, con l'adozione e diffusione di computer e memorie digitali nei paesi industrializzati del mondo, negli anni a venire avrebbe poi cambiato l'intero sistema economico e sociale. Con l'arrivo dei computer e delle seguenti tecnologie, nasce una nuova professione capace di gestire questa innovazione, ovvero programmatori ed hacker. Molti di quest'ultimi iniziarono ad intravedere come questi sistemi e servizi digitali potessero intaccare quello che è definita la privacy informatica e quindi la privacy del libero cittadino. La libertà di informazione e la privacy nel mondo digitale era tutt'altro che libera inizialmente, per questo nacquero gruppi di programmatori ed hacker ribelli interessati a creare una privacy assoluta nel mondo informatico, tra questi c'erano "The Cypherpunks".

I Cypherpunk si specializzarono nella crittografia e creazione di cypher, ovvero mailing list, in gruppi informali, con l'intento di ottenere la privacy e la sicurezza informatica degli account personali, che erano quasi impossibili da penetrare. Fra loro, annoveriamo Eric Hughes, matematico americano, programmatore di computer che attraverso il Manifesto Cypherpunk ci dice:

"La privacy è necessaria per una società aperta nell'era digitale. Non possiamo aspettarci che i governi, le aziende o altre grandi organizzazioni senza volto ci concedano la privacy. Dobbiamo difendere la nostra privacy se ci aspettiamo qualcosa. I cypherpunk scrivono il codice. Sappiamo che qualcuno deve creare i software per difendere la privacy, e ... lo stiamo facendo"

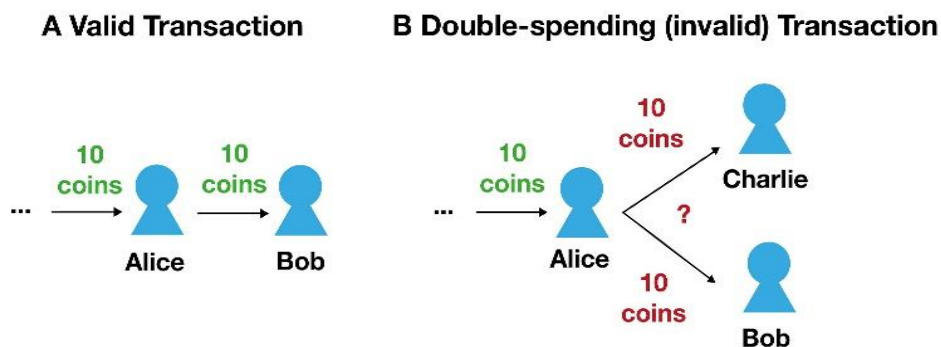
Sempre i Cypherpunk hanno sperimentato l'idea secondo la quale sulla rete si possa inviare denaro senza l'uso di un intermediario. David Chaum, un informatico e crittografo americano, ha creato DigiCash nel 1989 e ha pubblicato un documento accademico sull'argomento. Pur avendo l'idea, non sono mai riusciti a creare un tecnicismo per realizzare una vera esperienza peer-to-peer. Dopo il crollo del mercato azionario del 2008, era il momento per un passo avanti ed un'innovazione del mercato azionario. La blockchain si può dire che nasce nel novembre del 2008, grazie alla pubblicazione di un white-paper su The Cryptography Mailing list, dal titolo "Bitcoin: A Peer-to-Peer Electronic Cash System", firmato sotto il nome di Satoshi Nakamoto. Mentre l'attenzione mondiale era rivolta sulla crisi finanziaria, creata da istituzioni bancarie e colossi finanziari, Nakamoto propone un nuovo modello per effettuare transizioni totalmente decentralizzato e strutturato intorno ad un meccanismo di consensualità tra blocchi che contengono un elenco completo delle transazioni, capace di eliminare gli intermediari. L'obiettivo era quello di separare la moneta dalle istituzioni di controllo e creare una rete in cui i pagamenti potessero avvenire tra individui senza aver bisogno di un'unità centrale di controllo, eliminando inutili costi di gestione. Satoshi Nakamoto, una persona o un gruppo di persone la cui identità e tutt'ora ignota, ha inventato il Bitcoin, ma soprattutto, la tecnologia sottostante, la blockchain e per questo ha ricevuto la nomina per il premio Nobel, nonostante ancora oggi nessuno sappia chi sia realmente. Inconsapevolmente, l'autore in questione

era ignaro che la vera invenzione più che la coniazione di una moneta virtuale, fosse la tecnologia blockchain su cui si appoggiava quest'ultima. Inizialmente, la comunità di crittografi e programmatori non comprese la potenzialità del Bitcoin di Nakamoto, solo un programmatore di nome Hal Finney ne vide le capacità e accettò di lavorare gratuitamente sul progetto Bitcoin. Il 3 gennaio del 2009 fu condivisa una prima versione del software client, la prima versione del software disponibile al pubblico, ufficializzando così la nascita del Bitcoin, e con esso della prima criptovaluta. Si trattava di una rete di computer connessi peer-to-peer. La blockchain, concepita per creare criptovalute come Bitcoin, Litecoin, Bytecoin, SwiftCoin, Ripple o Ether, era ed è fondamentalmente un sistema di contabilità che registra tutte le transazioni su un libro mastro pubblico, il così detto ledger. Invece del dollaro Usa, o dell'euro Europeo, il valore viene scambiato in una valuta digitale, chiamata Bitcoin o simili. I nuovi Bitcoin vengono creati dal "mining", che è un processo che sfrutta la capacità di elaborazione dei computer per risolvere un difficile problema matematico, ed una volta risolto il cifrario, il miner viene premiato in Bitcoin. Nel caso della Blockchain ci fu un vero e proprio boom di interesse massivo alla fine del 2015 e del 2017, legato al fenomeno dei Bitcoin. Sono stati proprio questi ultimi a guidare l'attenzione verso la blockchain e, non a caso, in molti non riescono a discernere l'uno dall'altro, identificandoli come sinonimi.

1.2 Bitcoin rimedio al fenomeno del Double Spending

Oggi giorno nel mondo finanziario digitale, possiamo trovare numerose monete virtuali, come i Litecoin diretti concorrenti al Bitcoin o Ripple ed Ether sempre più popolari per le possibilità che offrono tra Smart Contracts e Blockchain private ed ognuna di esse è contraddistinta dal proprio protocollo. Il corretto funzionamento di queste piattaforme informatiche dipende, dalla crittografia e dalle politiche di consenso alla base della blockchain, il cui scopo è garantire sicurezza nelle transazioni digitali e trovar rimedio a problemi come il Double Spending.

Con il termine "Double Spending" andiamo ad indentificare il problema della doppia spesa vale a dire un potenziale difetto in un sistema di criptovaluta o in un altro schema di cassa digitale in cui lo stesso singolo sistema digitale token può essere speso più di una volta, e questo è possibile perché un token digitale consiste in un file digitale che può essere duplicato o falsificato, ovvero una transazione utilizza lo stesso input di un'altra transazione già trasmessa in rete.



Il fenomeno del double spending è estremamente dannoso per i sistemi in cui avviene, poiché la perdita di fiducia degli utenti nella valuta di riferimento, ne causa l'inflazione, rendendola di fatto priva di valore. Si tratta di un problema esclusivo delle valute digitali, data la loro facile riproducibilità da parte di hackers, a cui servono solamente conoscenze della rete di riferimento e computer dalla grande potenza di calcolo per compromettere la sicurezza dei sistemi.

Con il termine criptovaluta si intende uno strumento digitale utilizzato per effettuare acquisti e vendite in maniera del tutto sicura. La prima cosiddetta criptovaluta è il Bitcoin ovvero una moneta basata su un'architettura computerizzata decentralizzata.

Il Bitcoin e le criptovalute similari basate su blockchain si trovano in uno status di vulnerabilità a questi attacchi solo nella fase iniziale di accettazione di una transizione, poiché più il tempo passa più la transizione è sottoposta a verifiche da parte degli altri nodi della rete.

Le due azioni di hackeraggio più comuni in tali sistemi sono il Brute Force Attack ed il Majority Attack che sono azioni inusuali e molto difficili da eseguire con pochissime probabilità di successo.

1.2.1 Brute Force Attack

Come detto in precedenza, il responsabile di un Brute Force Attack avrà bisogno di un hardware dalle alte prestazioni, ovvero una capacità di calcolo della funzione hash per secondo estremamente veloce. La riuscita dell'attacco dipende dalla rapidità (frequenza di hash) di chi lo mette in pratica e dal numero di conferme previste dal negozio/servizio che sta subendo l'attacco.

Per esempio:

“Se il responsabile dell'attacco possiede il 10% della potenza di calcolo della rete Bitcoin e il negozio prevede un numero di 6 conferme perché la transazione vada a buon fine, la probabilità di successo dell'attacco sarà dello 0.1%. Tuttavia, se il malintenzionato non riuscisse nell'operazione e l'attacco non andasse a buon fine, i fondi per coprire i costi della transazione verrebbero prelevati dal conto del responsabile ed inviati all'esercente, come fosse avvenuta una normale operazione all'interno della piattaforma.”

1.2.2 Majority Attack

Il Majority Attack è formalmente definito come il 51% Attack. 51% è un riferimento alla capacità elaborativa della rete blockchain, di fatto questo genere di attacchi avvengono quando uno o più malintenzionati posseggono una capacità di calcolo sufficientemente grande da poter costruire e verificare blocchi più velocemente della rete attaccata. Fintanto che l'inserimento di nuove transazioni nei blocchi della rete dipende dal lavoro svolto dai miners, si può dire che il sistema dipenda da questi ultimi. A causa di questo meccanismo,

i miners di una rete potrebbero unirsi/coalizzarsi per formare una “mining pool” (piscina mineraria), luogo dove viene concentrata la potenza di calcolo dei miners che vi partecipano.

Una volta che si detiene il 51% della potenza di calcolo di un sistema, questi possono prendere il controllo della blockchain. Essendo gli elaboratori della rete “più lenti” del mining pool nel processo di verifica e conferma delle transazioni, questa si trova soggetta ad accettare transazioni che le vengono trasmesse dall'aggressore come vere, così da permettere all'aggressore di decidere quali transazioni aggregare ai blocchi della blockchain sotto attacco. Non solo, in status di attacco, il responsabile potrebbe anche manomettere i dati registrati nella blockchain e cancellarli, oppure creare una biforcazione nella catena, “un Fork”, per avvalersi di transazioni double spending. Più i sistemi blockchain sono grandi meno sono le probabilità di successo di un 51% attack, ad oggi per esempio, sul network Bitcoin non è mai avvenuto uno di questi attacchi, nonostante è stato dimostrato che seppur estremamente difficile per altri network più piccoli sia una minaccia possibile.

1.3 La crittografia a servizio della Blockchain

La crittografia è la disciplina che studia come rendere le informazioni sicure, ossia prendendo un testo detto in chiaro e trasformandolo in testo cifrato, che risulta incomprensibile a chi non conosce i dettagli della trasformazione. Comunicazioni telefoniche, accesso a documenti online, home banking, pagamento di tasse, acquisti online, sono tutti esempi di attività che non potremmo condurre in sicurezza senza la crittografia.

Per proteggere con la crittografia una informazione bisogna trasformarla in qualcosa di equivalente ma non decifrabile e non facilmente riconducibile all'originale: è questo l'atto del cifrare. Decifrare è, invece, l'operazione inversa: da una comunicazione cifrata si ottiene nuovamente la sua forma originaria. Un procedimento ben definito per cifrare e decifrare dati è detto algoritmo crittografico e, per funzionare, può richiedere l'utilizzo di una, nessuna o più chiavi, concettualmente simili alle password che siamo abituati ad utilizzare.

Mentre la crittografia si occupa di costruire tecniche sicure per eseguire cifratura e decifratura, la crittoanalisi è la scienza che si occupa di trovare espedienti e tecniche per rompere tale sicurezza rendendo inefficaci gli schemi di cifratura. Crittografia e crittoanalisi fanno parte della più ampia scienza della crittologia. Nei protocolli Blockchain, troviamo le funzioni crittografiche di Hash, per la generazione di indirizzi ed il collegamento di blocchi nella catena, dove ogni blocco della catena possiede un numero hash composto da 256 bit.

Nei più classici sistemi centralizzati, gli utenti sono identificati con credenziali come il nome utente e password, memorizzate in banche dati centrali ed in presenza di una terza parte certificante, mentre sui sistemi blockchain, le identità sono garantite da firme digitali combinate con un sistema di chiavi private e pubbliche.

I sistemi funzionano considerando le chiavi, che possono essere private e pubbliche, gli indirizzi mentre le firme digitali così come ogni transazione devono essere convalidate da una firma, generata da una coppia di chiavi. Ogni utente può disporre di una coppia di chiavi o di diverse coppie, ed ognuna di queste coppie è composta o da una chiave privata ed una pubblica, oppure da una chiave pubblica, creata per ogni transazione, affiancata sempre dalla stessa chiave

privata per ottenere un livello maggiore di privacy. Andiamo a vedere nello specifico la chiave privata e la chiave pubblica:

- La chiavi private vengono condivise esclusivamente con gli utenti di riferimento/proprietari del wallet digitale, è utilizzata per "firmare" le transazioni, come mezzo di convalida per le operazioni.
- La chiave pubblica è fondamentale per lo scambio di criptovalute e potrebbe eventualmente essere condivisa anche con gli altri utenti appartenenti alla blockchain.

Il codice alfanumerico delle chiavi private viene generato in modalità pseudo casuale, mentre la chiave pubblica è data dalla funzione:

$$K = k \times G$$

Dove:

K sta per la chiave pubblica

k la chiave privata

La chiave pubblica è generata da una funzione matematica detta "Moltiplicazione della Curva Ellittica", dove K e G sono entrambi punti sulla curva ellittica. La moltiplicazione della curva ellittica è un genere di funzione definito dagli stessi crittografi come "Funzione Botola", questo perché una funzione di questo tipo è relativamente facile da eseguire mentre è praticamente impossibile da ricostruire. Anche se qualcuno conoscesse la chiave pubblica (K) e la funzione stessa (G), non avrebbe modo di calcolare la chiave privata.

In sostanza l'indirizzo viene determinato applicando una funzione di doppio hash alla chiave pubblica, ossia una funzione hash può convertire dati di dimensioni arbitrarie in dati di dimensioni fisse, gli indirizzi ottenuti come output saranno dei codici alfanumerici, che ideologicamente corrispondono ai codici IBAN nei normali sistemi finanziari.

Mentre le chiavi pubbliche e private conferiscono sicurezza ai sistemi blockchain ed anche ai più tradizionali sistemi informatici, è l'utilizzo della crittografia che conferisce alla suddetta tecnologia immutabilità e trasparenza nel trattamento dei dati

1.4 Caratteristiche della blockchain

Possiamo definire le blockchain come un libro mastro strutturato come una catena di blocchi, contenenti transazioni, correlate tra di loro secondo un principio cronologico e la cui integrità è assicurata da un sistema di algoritmi e regole crittografiche, e si compone di 3 elementi principali:

- Regole matematiche;
- Regole di crittografia;
- Regole di programmazione informatica



Le caratteristiche delle blockchain sono molteplici:

- decentralizzazione;
- immutabilità;
- sicurezza;
- trasparenza;
- tracciabilità;

I dati, una volta inseriti all'interno dei blocchi, non possono più essere modificati retroattivamente senza che vengano invalidati tutti i processi successivi e ciò implicherebbe il consenso della maggioranza del sistema. Ogni record viene memorizzato in modo da includere una quota di informazioni che fanno capo alle informazioni precedenti, questa connessione rende virtualmente impossibile l'alterazione senza che essa sia immediatamente visibile a tutta la rete. La blockchain permette una gestione dei dati in termini di verifica e di autorizzazione senza che sia necessaria una autorità centrale, bensì garantita dalla fiducia distribuita tra tutti i suoi utenti.

Di seguito andremo ad analizzare le caratteristiche che permettono alla tecnologia blockchain di distinguersi.

1.4.1 Decentralizzazione

Se consideriamo la blockchain come un database, dobbiamo pensare a una rete di utenti connessi tra di loro che hanno uguale accesso ai dati, senza l'intervento di un terzo che li autorizzi e che detenga il monopolio delle transazioni.

Ovviamente questo non vuol dire che all'interno delle tecnologie blockchain, che vivono di fatto in uno stato di autogoverno, sia assente un qualsiasi modello di controllo. Quando non è presente un buon modello di *governance* non è possibile realizzare una vera e propria architettura decentralizzata. Questo perché, in assenza di un'autorità centrale bisogna stabilire come prendere le decisioni, come avviene il processo di voto a maggioranza, come bisogna rapportarsi per gli scambi dei dati o come regolarsi per gli aggiornamenti del codice.

Le norme che la regolano vengono definite in fase di sviluppo, e non sono successivamente modificabili se non con l'assenso dei suoi partecipanti. Qualora l'assenso non fosse unanime, si crea un Fork, che tratteremo dettagliatamente in seguito. Queste leggi nella blockchain si identificano con l'algoritmo matematico la cui soluzione dà diritto di accesso alla catena.

1.4.2 Immutabilità

L'immutabilità è il **grande valore della blockchain**.

Per poter creare un nuovo blocco alla catena è necessario il controllo delle transazioni contenute nel blocco stesso da parte dei nodi. Questo passaggio si risolve attraverso un complesso problema matematico che richiede un cospicuo impegno computazionale in termini di potenza e di capacità elaborativa. Nel caso della blockchain è impossibile violare l'autorità centrale che la gestisce, in quanto sarebbe necessario violare tutti i partecipanti della blockchain simultaneamente. Il consenso sull'accuratezza dei dati è richiesto per tutti i membri della rete e tutte le transazioni convalidate sono **immutabili perché** vengono registrate in modo permanente. Nessuno, nemmeno un amministratore di sistema, può eliminare una transazione.

1.4.3 Sicurezza

La natura distribuita e crittografata della blockchain ne rende difficile la violazione da parte degli hacker. Questa prerogativa la rende promettente per la sicurezza aziendale e dell'Internet of Things (IoT).

La decentralizzazione e l'immutabilità dell'informazione rendono l'informazione stessa sicura. Qualora un'entità volesse bloccare l'accesso al network, la decentralizzazione

assicurerebbe l'accesso ai dati da parte degli altri nodi che possiedono la propria copia di transazioni della blockchain mentre il principio dell'immutabilità ne impedirebbe la corruzione.

Questo rende una transazione, di qualunque natura essa sia tra beni, servizi o pagamenti estremamente sicura.



1.4.4. Trasparenza

Le informazioni contenute nelle catene di blocchi sono visibili a tutti i partecipanti e non possono essere alterate. In questo modo si riducono i rischi e le frodi, instaurando al contempo fiducia.

Il decentramento va di pari passo con la trasparenza assoluta dei dati, poiché le transazioni effettuate mediante la tecnologia Blockchain sono visibili a tutti i partecipanti. Per comprendere il ruolo che assume la trasparenza in un sistema fondato su meccanismi crittografici diffusi, basterà fare riferimento all'ambito all'agroalimentare, infatti, la tracciabilità è un requisito essenziale, previsto anche per legge. Che la "storia" di un alimento, per esempio nelle industrie della trasformazione, sia anche trasparente, dal conferimento fino al confezionamento e alla commercializzazione, dipende da un percorso in cui tutti gli attori coinvolti (produttori, imprese che si occupano del packaging, operatori di logistica e trasporto ecc.) possano intervenire, ma senza modificare le informazioni condivise dagli altri. Come possiamo vedere torna il concetto di immutabilità, caratteristica della blockchain, delle transazioni proprio della Blockchain technology che, in questo caso, contiene in sé le caratteristiche della trasparenza strettamente connessa alla preservazione del dato dai potenziali rischi di manomissione o alterazione.

1.4.5 Tracciabilità

Il fatto che i dati della blockchain siano inalterabili ne fa un sistema ideale, per esempio, per il tracciamento e il monitoraggio di articoli e provenienze lungo supply chain anche complesse.

Come abbiamo visto un utilizzo importante della tracciabilità della blockchain lo troviamo nella tracciabilità alimentare.

La tecnologia blockchain permette **di** tracciare l'intera filiera dalla materia prima al prodotto a scaffale, con tutte le informazioni relative a produzione, trasporto e alle relative condizioni

1.5 Componenti della Blockchain

Ora andremo ad analizzare meglio alcuni tecnicismi per comprendere meglio il funzionamento di una blockchain. Quest'ultima si compone di:

- Transazioni;
- Nodi;
- Wallet;
- Blocchi;
- Ledger;

- Codici Hash;
- Miners;
- Meccanismo di consenso;
- Forks;

1.5.1 Le Transazioni

La transazione è quel bene, servizio o informazione digitale che viene scambiato tra due o più soggetti o nodi su una piattaforma informatica e che necessita di essere dapprima approvato, verificato ed in fine archiviato.

Le transazioni per esistere necessitano di un mandante, un ricevitore ed infine delle informazioni relative all'oggetto o servizio che si vuole trasferire.

“Per esempio, volessimo considerare il passaggio di proprietà di un'automobile, le informazioni saranno il prezzo, l'attuale proprietario del veicolo, le caratteristiche del mezzo, i dati storici, e via dicendo.”



1.5.2 I Nodi

Per nodo si intende un qualsiasi dispositivo hardware, capace di comunicare con gli altri dispositivi appartenenti alla stessa rete.

I vari nodi sono collegati tra di loro ed ognuno di essi funge anche da server per la gestione delle transazioni interne alla rete.

1.5.3 I Wallet

Un Wallet, tradotto in italiano come “portafoglio”, è uno strumento necessario per l'utilizzo di criptovalute ed appunto funge da portafoglio digitale per gli utenti, strumento attraverso cui è possibile eseguire transazioni su blockchain come archiviare e gestire le proprie criptovalute.

Nella pratica, un wallet è un software o hardware disponibile per l'installazione su computer, smartphone o simili che permette di gestire in autonomia il proprio numero di conto registrato su blockchain. Come è già stato discusso in precedenza un wallet digitale si compone di una chiave pubblica ed una privata.

La chiave privata è semplicemente un numero casuale che funge come una firma consentendo all'utente di esser ricollegato al proprio conto e di confermare transazioni.

La chiave pubblica è utilizzata per ricevere fondi, identificare l'account degli utenti nel network e può essere tranquillamente condivisa con altri utenti.

1.5.4 Ledger

Il ledger è un “Libro Mastro”, definibile come una delle basi della nostra civiltà, attraverso cui vengono gestite ed interpretate le relazioni o transazioni tra persone o tra organizzazioni.

Il ledger ha valore nel momento e nella misura in cui può essere consultato e permette di stabilire una memoria storica di transazioni e scambi effettuati tra utenti, ovvero come fosse un registro della contabilità all'interno di un sistema, che sia sociale o digitale.

Il ledger, di per sé, è una tecnologia che consente lo scambio di ogni forma di transazione e collaborazione all'interno di un network informatico, ed in questo caso appoggiata e gestita attraverso un sistema blockchain.

1.5.5 I Blocchi

I blocchi, sono il raggruppamento di una serie di transazioni, e solitamente possono contenere fino ad un massimo di 1 Megabyte ciascuno. Ogni blocco si compone di una transactions list e di un header.

Le transactions list o anche detto body, sono semplicemente l'elenco completo di tutte le transazioni che il blocco contiene. Mentre l'header del blocco si suddivide in:

- Version: definibile come il protocollo che un blocco deve seguire perché venga considerato valido;
- Previous Block Hash: in italiano, l'hash del blocco precedente, indispensabile per creare il concatenamento dei due blocchi;
- Markle Rooth Hash: senza entrare in tecnicismi, è come fosse l'albero genealogico degli hash utilizzati per il concatenamento dei blocchi. L'hash finale porta con sé caratteristiche di tutti gli hash che l'hanno preceduto;
- Timestamp: indica la data e l'ora di creazione del blocco di riferimento;
- Nonce: è quel numero che il miner dovrà calcolare per ottenere un blocco valido per la concatenazione.
- Height: detto anche numero del blocco, indica la posizione di un blocco all'interno della catena.
- Target difficulty: è un valore a 256 bit che si modifica in virtù del tempo necessario a validare 2016 blocchi e misura quanto sia difficile trovare un hash per un certo target. Rappresenta l'indice di difficoltà per la convalidazione di un hash.



1.5.6 I Codici Hash

Il codice Hash di un blocco rappresenta il suo codice di autenticazione. La si può considerare come la firma digitale che ne determina l'unicità e assicura l'inviolabilità dell'intero blocco. L'hash del blocco di riferimento registra tutte le informazioni relative al suddetto, mentre l'hash con le informazioni relative al blocco precedente permette di creare la catena e di legare un blocco all'altro.

Nella pratica si parte da una stringa di dati dalla lunghezza variabile (input) che vengono poi processati dalla funzione hash, trasformando la stringa ad una lunghezza predefinita. Questa procedura rilascia un output, detto digest, un codice alfanumerico irreversibile che non consente in alcun modo di risalire ai dati dell'input.

Per questa caratteristica, le funzioni crittografiche di hash svolgono numerose funzioni negli ambiti di sicurezza informatica., tra cui:

- Firme digitali;
- Identificazione di dati;
- Verifica password;
- Protezione dagli errori.

1.5.7 I Miners

Il miner è colui che mette a disposizione l'elevata potenza di calcolo del proprio computer per trovare un algoritmo di risoluzione al problema, per validare le transazioni e registrarle sul ledger della catena blockchain. Il processo di certificazione effettuato dai miner è definito mining. La chiave per la validazione di un blocco si ottiene attraverso la ricerca da parte del miner di un valore numerico detto nonce, ed un valore alfanumerico hash, per la chiusura del blocco.

Il blocco validato verrà poi aggiunto alla catena. Questa operazione si basa sulla "crittoeconomia", la combinazione di incentivi economici e meccanismi di verifica che utilizza la crittografia. In breve, una volta trovata la soluzione, il miner che ha trovato la soluzione al problema, valida il blocco ed otterrà una ricompensa in criptovaluta, come premio al suo contributo per il funzionamento dell'intero sistema. I nodi disonesti o inefficienti vengono espulsi rapidamente dal network della blockchain, mentre i miner onesti ed efficienti hanno il potenziale di ricevere sostanziose ricompense per il loro lavoro.

Nella risoluzione dei blocchi è possibile che due miner riescano a trovare una soluzione per lo stesso blocco a distanza di pochi secondi. In questo caso si genererà una

biforcazione con l'inserimento di due blocchi non perfettamente identici ma che rispettano entrambi la verifica matematica del blocco precedente. Il blocco che formerà la catena più lunga sarà ritenuto valido mentre l'altro, il blocco orfano, verrà eliminato.

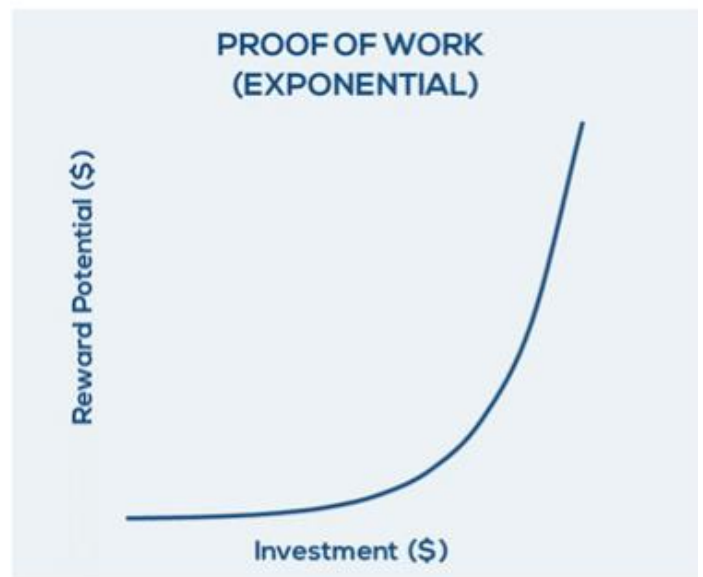
1.5.8 I principali meccanismi di consenso PoW & PoS

I protocolli di consenso sono fondamentali poiché permettono il corretto funzionamento di un qualsiasi sistema blockchain. Nella pratica si tratta degli algoritmi che regolano il meccanismo di validazione delle transazioni e stabiliscono le regole attraverso cui tali transazioni vengono trascritte su quest'ultima a formazione dei blocchi.

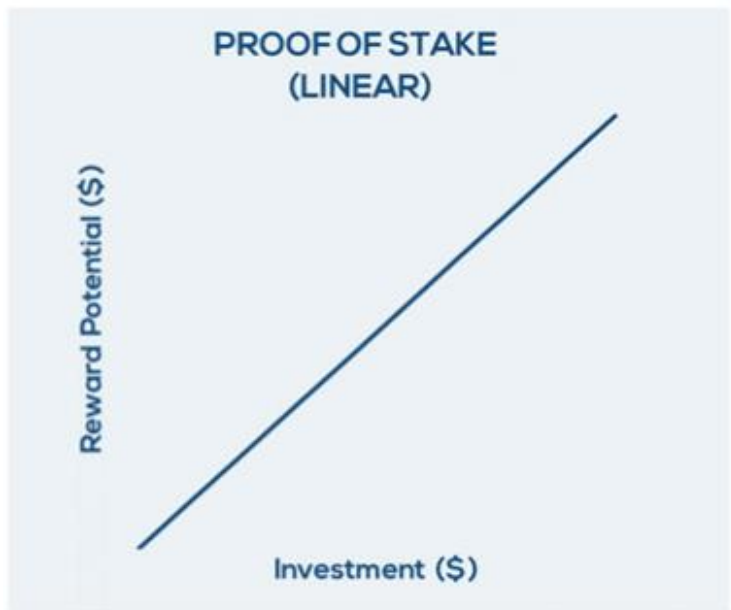
Sono proprio questi meccanismi di consenso che rompono il paradigma del più classico consenso centralizzato favorito dalle istituzioni di tutto il mondo. I meccanismi di consenso garantiscono che le informazioni aggregate ai blocchi siano vere ed affidabili, due fra i più utilizzati meccanismi sono la Proof of Work (PoW) e la Proof of Stake (PoS).

Tuttavia, esistono decine di differenti protocolli, con le proprie regole e specifiche per approssimare i problemi, ognuno con lo scopo di gestire la validazione delle transazioni e permettere di trasferire valore in un network in cui altrimenti mancherebbero sicurezza e fiducia reciproca.

In questo momento il protocollo di consenso più conosciuto ed utilizzato è la Proof of Work, il quale prevede di mettere i miners della rete in competizione, offrendo dei compensi in criptovaluta per la risoluzione di una serie di problemi computazionali molto complessi con il fine di validare ed aggiungere un blocco di transazioni all'interno di una catena. Questo approccio è caratterizzato al contempo da una sicurezza pressoché perfetta, a discapito di quelli che sono percepiti come i principali limiti della proof of work, ovvero lentezza ed alto dispendio energetico. Per questo motivo PoW non è considerata una soluzione efficiente nell'ambito imprenditoriale.



Il sistema di Proof of Stake (PoS) invece, funziona in modo simile ad una società per azioni, dove ogni azionista detiene una quota della società. Non si basa sulla potenza computazionale espressa dai nodi della rete, bensì da blocchi più semplici da risolvere, questi sono più vantaggiosi in termini di scalabilità, necessitano di una potenza di calcolo inferiore e di meno energia. La Proof of Stake è un sistema non competitivo dove ciò che più conta è l'efficienza del sistema; infatti, in questi sistemi i miners devono dimostrare di avere un ammontare di criptovalute del sistema, che potrebbe perdere in caso di comportamenti malevoli nei confronti del sistema. La risorsa che viene confrontata è la quantità di criptovalute che un miner detiene. In breve, la PoS è un meccanismo di consenso in cui i blocchi vengono convalidati in base alla posta in gioco dei partecipanti e ad un fattore di randomizzazione; quindi, il miner di ogni blocco viene selezionato secondo un processo pseudocasuale. Per i miners vi è il rischio legato alla quota investita per la partecipazione ad una operazione di consenso nella rete, che li rende i soggetti con il maggiore interesse nel garantire la stabilità della rete. I nodi che fanno maggiormente girare l'economia del sistema sono anche quelli con più possibilità di minare il sistema, questa sua propensione a creare una sorta di oligarchia si può anche definire il limite di questo metodo.



3iQ Research Group

Proof of Work VS Proof of Stake

Mining capacity depends on computational power

Validating capacity depends on the stake in the network

Miners receive block rewards to solve a cryptographic puzzle

Validators do not receive a block reward, instead, they collect transaction fees as reward

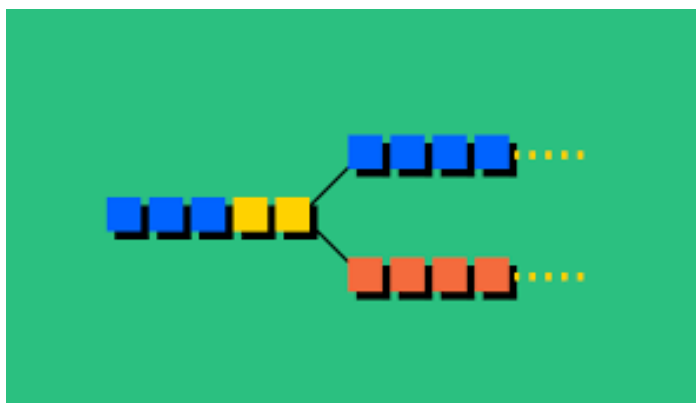
Hackers would need to have a computer powerful than 51% of the network to add a malicious block, leading to 51% attack

Hacker would need to own 51% of all the cryptocurrency on the network, which is practically impossible and therefore, making 51% attacks impossible.

Tuttavia, vale la pena di notare che questi non sono gli unici algoritmi di consenso utilizzati. Per certi aspetti la tecnologia blockchain è ancora in fase di sviluppo, alcuni sviluppatori vivono in un costante processo di creazione di nuovi algoritmi, utilizzando un mix di caratteristiche dei protocolli classici per ottenere soluzioni più efficienti, che propongono nuove funzioni che si adattino alle numerose applicazioni della blockchain.

1.5.9 I Forks

Con il termine “Fork” si intende una modifica al codice originario della blockchain. Il network, comprendente miner e sviluppatori, non sempre è d'accordo sulle modifiche e gli adattamenti dei protocolli della blockchain. Quando un gruppo è irremovibile su un particolare cambiamento del codice, ma una restante parte del gruppo non è d'accordo, avviene una separazione all'interno della blockchain, avviene un fork. La catena si duplica e si divide, mantenendo tutte le caratteristiche della blockchain precedente, fatta eccezione per l'implementazione di nuove soluzioni progettuali e cambiamenti al protocollo di base. Questo significa che i nodi non aggiornati sono ancora in grado di elaborare transazioni e aggiungere nuovi blocchi alla blockchain, a condizione che non vadano in contrasto con le regole del nuovo protocollo.



Spesso si generano a seguito della creazione di nuovi token. Creare token da zero è il metodo più comune e prevede un copia e incolla del codice esistente che poi viene modificato e lanciato come nuovo token. Un metodo alternativo è invece quello di biforcare. In questo caso le modifiche vengono applicate alla blockchain esistente che si divide.

Esistono due tipologie, l'hard fork ed il soft fork.

I Forks che sono incompatibili con le vecchie versioni del software sono chiamate "Hard Forks". Questi di solito cambiano le regole di consenso, ad esempio la dimensione del blocco, l'algoritmo minerario ed il protocollo di consenso in un modo che rende incompatibili le versioni precedenti del software con le nuove implementazioni. Dal momento che ogni nodo avrebbe regole di consenso diverse, sarebbero essenzialmente in esecuzione blockchain separate.

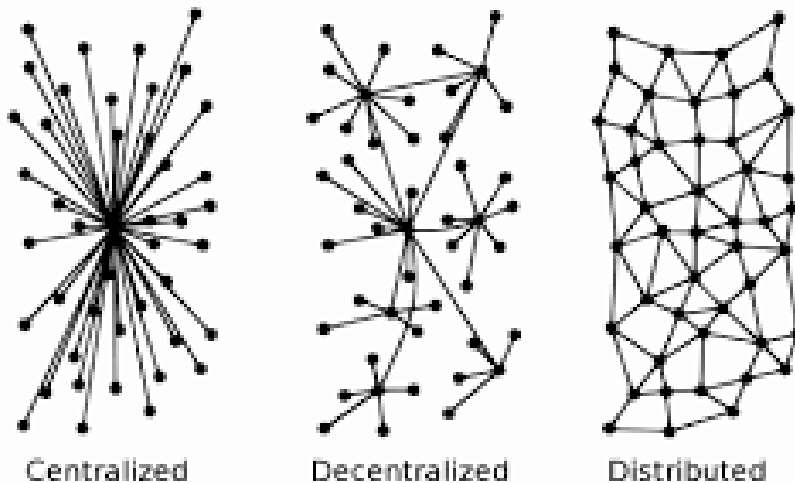
Tuttavia, ci sono alcuni fork che sono compatibili con le vecchie versioni del software, i così detti "Soft Fork", i quali sono aggiornamenti del software, che funzionano ancora con le versioni precedenti. Finché almeno il 51% della potenza di hashing passa al soft fork degli aggiornamenti, le vecchie versioni del software funzioneranno ancora.

1.6 Struttura di un sistema

Quando parliamo della struttura di un sistema tecnicamente ci stiamo riferendo alla disposizione dei suoi singoli elementi come insieme, i quali connessi tra loro formano un elemento più complesso, appunto definito come sistema.

Di questi, tre sono le tipologie di strutture più comunemente utilizzate:

- Centralizzato;
- Decentralizzato;
- Distribuito;



1.6.1 Centralized Ledger

I Centralized Ledger sono i più intuitivi e facili da capire e definire. Sono sistemi che utilizzano un'architettura client/server in cui uno o più nodi client sono collegati direttamente ad un server centrale. Questo è il tipo di sistema più comunemente usato in molte organizzazioni dove il cliente invia una richiesta ad un server aziendale da cui poi riceverà risposta.

Il sistema si definisce centralizzato a riferimento della sua architettura, dove abbiamo un nodo centrale detto nodo server che appunto serve e coordina tutti gli altri nodi del sistema detti nodi client. La questione più rilevante di avere un sistema centralizzato è ammettere un unico punto di guasto nel sistema, che lascia le catene di fornitura vulnerabili al fallimento in caso di hackeraggio o corruzione per esempio.

In passato alcuni scandali hanno dimostrato che nonostante costosi sistemi di sicurezza questi non sono in grado di garantire la completa sicurezza dei dati, lasciando le organizzazioni nella rete esposti a un potenziale rischio. Questo è anche uno dei grossi limiti di questa tecnologia, in quanto l'eccessiva dipendenza dei nodi client nei confronti del nodo centrale ne influenza

negativamente l'affidabilità, perché chiaramente qualora si verificassero problemi nel coordinamento generale ed il sistema fallisse il guasto/hackeraggio nel nodo centrale influenzerebbe l'intero network.

1.6.2 Decentralized Ledger

I Decentralized Ledger possono essere descritti come sistemi con più nodi dedicati all'elaborazione e gestione del traffico delle informazioni. Una parte centrale non è responsabile della gestione dell'intero sistema. È molto più difficile tracciare le informazioni in un sistema di questo tipo, in quanto le informazioni passano attraverso una varietà di nodi e non solo attraverso una singola entità.

Pertanto, rispetto a una rete centralizzata, un sistema decentralizzato consente una maggiore riservatezza dei dati, nonostante in questo sistema i vari nodi siano dotati di una certa autonomia, questi dovranno sempre e comunque fare riferimento ad una struttura centrale.

1.6.3 Distributed Ledger

La vera evoluzione a queste tecnologie si ha con la nascita dei Distributed Ledger, la peculiarità di questo sistema è che ogni nodo funge da nodo server, sfruttando un'interazione peer-to-peer tra i vari utenti che compongono la rete, ossia ogni nodo equivale a tutti gli altri.

Di conseguenza, ogni nodo gode di eguale responsabilità e assicura il corretto funzionamento del network stesso, il che differisce molto dal modello classico client/server: in un sistema P2P ogni nodo è in grado di ricoprire sia il ruolo di client che di server.

La base per la creazione di sistemi distribuiti sono, appunto, network peer-to-peer. Nella loro configurazione più semplice, un network peer-to-peer è costituito da due o più computer che interagiscono tra di loro attraverso un cavo USB, come mezzo di comunicazione per lo scambio di file.

Ciò che caratterizza un sistema distribuito sta nell'assenza di un server dedicato alla gestione del traffico di informazioni, bensì nel caso un nodo fallisca, gli altri nodi appartenenti alla rete semplicemente prendono il suo posto ed assicurano che il meccanismo di trasmissione proceda regolarmente. A discapito di una maggiore difficoltà di coordinamento ed una complessità di programmazione decisamente superiore, la distributed ledger ha saputo distinguersi nell'architettura dei sistemi informatici presentando una potenza di calcolo maggiore, unita a costi di gestione inferiori e ad una maggiore affidabilità, oltre alla possibilità di crescita naturale che deriva dall'aggiunta progressiva di nuovi partecipanti al network.

1.7 Blockchain pubbliche o private

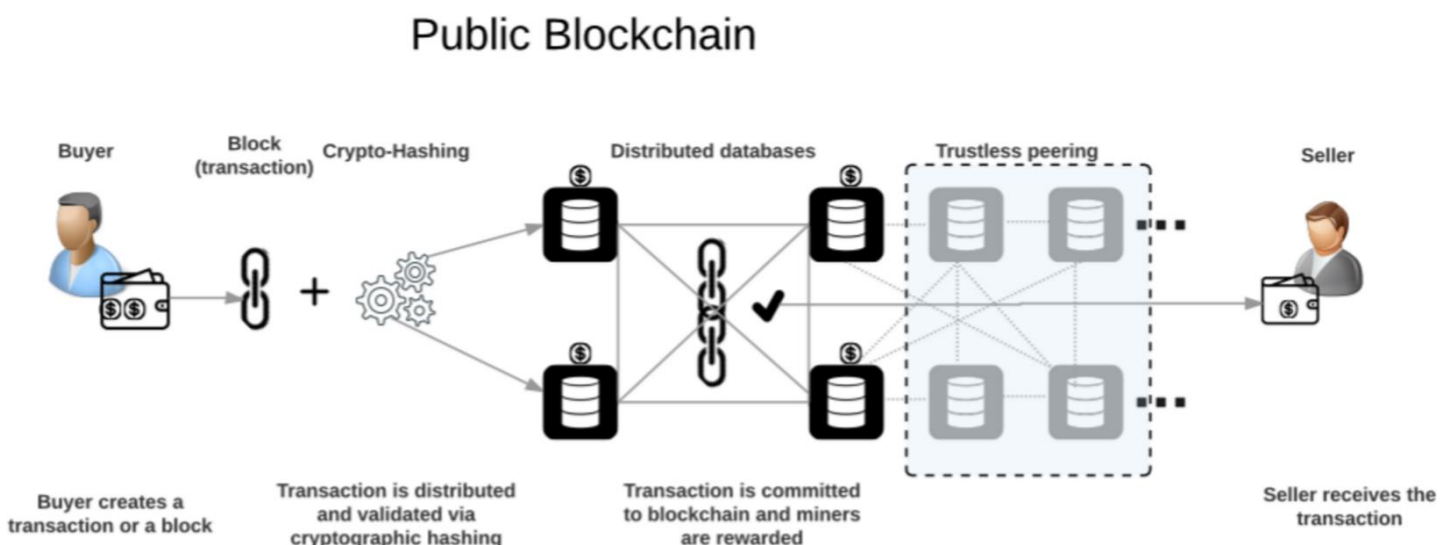
Al momento sono due le tipologie di Blockchain prese in considerazione, la pubblica (Unpermissioned Ledger) e la privata (Permissioned Ledger). La blockchain pubblica è una rete aperta, dove chiunque può scaricare il protocollo e leggere, scrivere o partecipare alla rete, mentre la privata è accessibile esclusivamente alle persone che hanno avuto accesso alla rete tramite invito.

Nonostante abbiano due scopi differenti, entrambe mantengono delle somiglianze per quanto riguarda le caratteristiche di base, che sono:

- Entrambe godono di reti decentralizzate peer-to-peer, dove ogni nodo della rete possiede una copia del libro mastro di ogni transazione;
- Entrambe mantengono sincronizzate le suddette copie attraverso un protocollo di sincronizzazione basato sul consenso;
- Entrambe garantiscono l'immutabilità delle informazioni contenute nella blockchain e quindi sicure da frodi e malintenzionati;

Una blockchain è definita pubblica quando un qualsiasi ente può deliberatamente averne accesso, non solo alla rete ed ai servizi che offre, ma anche a tutte le informazioni condivise all'interno del suo sistema. Inoltre, ogni suo partecipante ha diritto di far parte del processo di consenso.

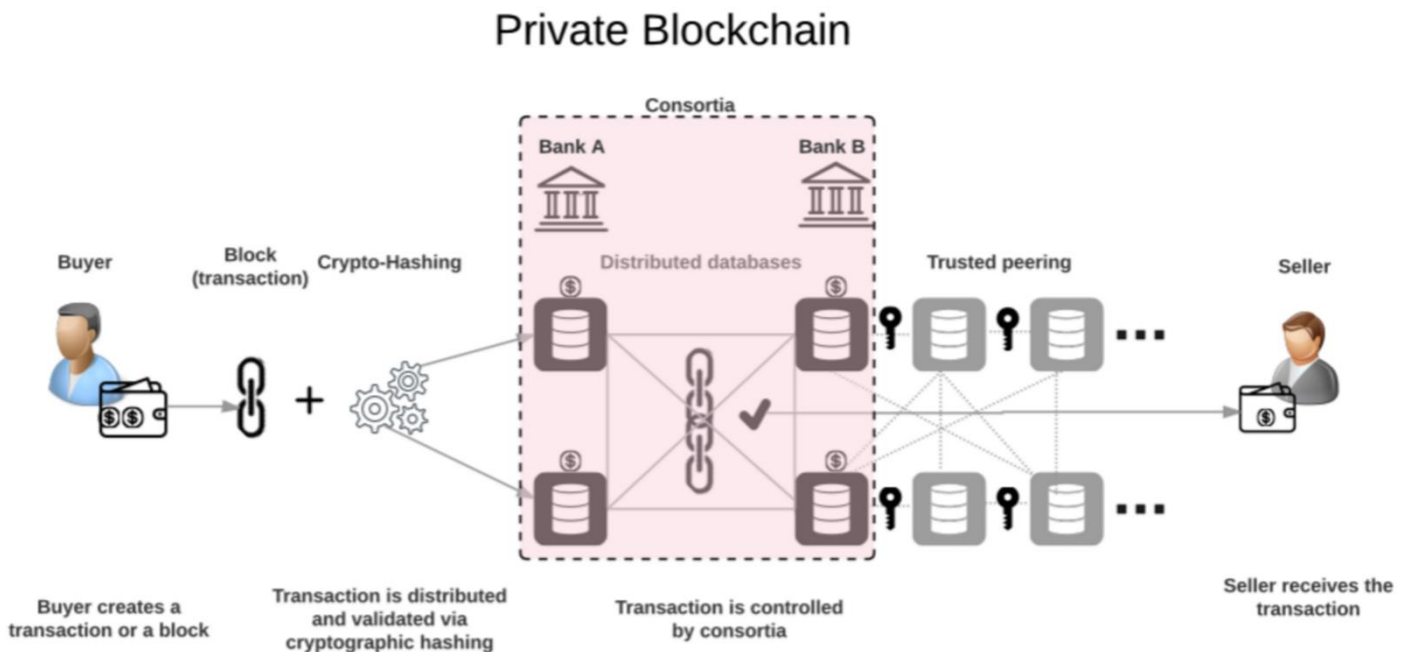
La governance di questi canali pubblici, derivato del movimento open source e dai cypherpunk, è semplice: "Il codice è Legge". In questo sistema, i nodi della rete convalidano le scelte discusse e avviate dagli sviluppatori decidendo se integrare le modifiche proposte. Basato su un approccio comunitario ed alternativo all'economia, questo sistema ha dimostrato la sua forza e la sua resilienza. Qualsiasi blockchain pubblica per funzionare necessita una sua moneta o generica criptovaluta. Due esempi di criptovalute che si affidano a blockchain pubbliche, sono anche le più popolari ad oggi, Bitcoin ed Ethereum.



Se la blockchain pubblica si basa sull'emergere di una nuova forma di fiducia digitale distribuita, la filosofia della blockchain privata è totalmente diversa. Il loro approccio si basa su un controllo centralizzato, questo significa che non condividono la caratteristica più distintiva delle blockchain: il decentramento.

Ma in realtà sono molte le distinzioni tra le due simil-tecnologie, d'altronde, un sistema blockchain viene definito come privato quando:

- il processo di consenso può essere raggiunto solo da un numero limitato e predefinito di partecipanti;
- l'accesso, in scrittura di codici e progettazione, è affidato ad una organizzazione centrale;
- i permessi di lettura possono essere aperti al pubblico o limitati. In questo caso, il processo di consenso è controllato da un insieme di nodi preselezionati;
- il sistema non necessita di miners; nessuna proof-of-work o conseguente remunerazione. Questo è ciò che differenzia maggiormente i due tipi di magazzini e tecnologie di trasmissione;
- ci possono essere diversi livelli di accesso e le informazioni possono essere criptate per proteggere la riservatezza commerciale. I partecipanti alla rete richiedono l'autorizzazione a leggere, scrivere o controllare informazione all'interno della catena;
- consentono alle organizzazioni di utilizzare la distributed ledger technology senza rendere pubblici i dati;



In molti sostengono che le blockchain private non si possono relazionare alla tecnologia di base da cui nascono, sono solamente database centralizzati che utilizzano la tecnologia dei distributed ledger per la sincronizzazione e protezione dei dati. Questo perché le blockchain pubbliche richiedono molto se non troppo tempo ed energia per convalidare le sue transazioni (genericamente si stimano 10 minuti per ognuna), mentre nei sistemi privati viene sacrificata parte della decentralizzazione e quindi parte della sicurezza ed immutabilità in cambio di spazio di archiviazione, velocità di esecuzione e riduzione dei costi di gestione.

In sintesi, le transazioni della rete privata vengono verificate esclusivamente da alcuni nodi, che godono di una potenza di elaborazione molto elevata e di fiducia garantita dalla affidabilità del brand a cui fanno riferimento. La conoscenza dell'identità dei miner implica che il loro lavoro non debba essere controllato o verificato dagli altri nodi della rete ed in caso di bug di sistema, questi possono essere risolti rapidamente con un intervento manuale, consentendo l'utilizzo di algoritmi di consenso che offrono finalità con tempi di validazione dei blocchi molto più brevi. Questo non solo comporta un maggiore livello di privacy per le imprese ma anche significativa riduzione nelle tempistiche ed economicità delle transazioni.

È presumibile che società private e istituzioni finanziarie avranno bisogno di scalabilità, di ridurre i propri costi operativi a favore di una maggiore redditività, di un elevato controllo degli accessi e di algoritmi di consenso praticabili per adattarsi alle esigenze del proprio business.

1.8 I token

Inizialmente va definito che con il termine token, in ambito informatico, si può far riferimento a due significati distinti. Comunemente viene affiancato il primo significato di token a quello delle criptovalute basate su blockchain, dove i token sono semplicemente frazioni di una criptovaluta.

La particolarità è che per ogni criptovaluta esiste un distinto registro di archiviazione dati pertinente alle transazioni eseguite con quest'ultima. Per quanto riguarda il secondo significato di token, la distinzione si incontra proprio nell'assenza di questo registro. Infatti, i token non necessitano di un registro proprio per esistere, ma trovano appoggio su piattaforme come Ethereum mediante gli smart contracts.

Il token ha quindi le stesse caratteristiche della criptomoneta (sicurezza e trasferibilità non censurabile) ma non è "nativo" e soprattutto "interno" alla blockchain sulla quale vengono memorizzate le transazioni che lo riguardano ma rappresenta il gemello digitale di un bene reale, un diritto "reale", ma che esiste al di fuori del sistema blockchain.

Quindi, un token è definibile come un asset digitale che gli utenti appartenenti ad una rete blockchain possono scambiare per effettuare transazioni. Il token di per sé è la rappresentazione del valore digitale di un qualsiasi bene, servizio, diritto o proprietà attraverso una piattaforma digitale, di solito una blockchain, se si considera che ad oggi l'85% dei token esistenti vengono generati sui sistemi di Ethereum.

Questi si caratterizzano per:

- trasformazione in criptovaluta;
- frazionabilità del valore di un bene in unità molto piccole;

- possibilità di eseguire compravendite tra utenti di una rete;
- immutabilità delle informazioni digitali.

Andando invece ad analizzare le tipologie di token esistenti è difficile farne una vera e propria classificazione, anche gli enti regolatori stanno cercando di districarsi in questo nuovo mondo, ma tutt'ora non esiste un chiaro quadro legale che ne garantisca la regolamentazione, per questo motivo propongono una breve introduzione alle 4 tipologie ad oggi più comuni:

1. Asset Token: rappresentano il diritto di proprietà di un determinato asset materiale o immateriale che sia. Gli asset possono essere quote societarie, flussi di reddito, un diritto a dividendi o al pagamento di interessi. In termini di funzione economica, i token sono analoghi ad azioni, obbligazioni o derivati;

2. Payment Token: questi token possono sviluppare solo le funzionalità necessarie per essere accettati come mezzo di pagamento, parliamo precisamente di Token Coin;

3. Utility Token: conferiscono il diritto di accesso digitale ad un servizio o applicazione digitale ed al suo utilizzo, come fosse l'accesso a dei contenuti;

4. Equity Token: è un tipo di token di sicurezza che funziona come un'azione tradizionale, esattamente come per le azioni societarie più comuni, i detentori possiedono letteralmente la loro percentuale del totale di un'impresa. Possono anche avere diritto a una parte degli utili dell'impresa e ad un diritto di voto sul suo futuro dato che il valore del token è determinato dal successo o dal fallimento dell'azienda di competenza.

CAPITOLO 2

AMBITI DI APPLICAZIONE E PRINCIPALI SETTORI

2.1 Ambiti di applicazione

La tecnologia Blockchain ottenne il suo riconoscimento a livello mondiale grazie all'applicazione Bitcoin. Tuttavia, lo sviluppo delle blockchain, per la sua applicazione in ambito aziendale e pubblico, è ancora molto lontano dall'esprimere piene potenzialità. Grazie al suo approccio decentralizzato nella gestione del valore ed alle sue caratteristiche di affidabilità e sicurezza, la tecnologia blockchain, ha iniziato a suscitare un gran interesse, e con tutta probabilità, avrà la possibilità di essere introdotta in numerosissimi campi e settori dell'economia.

Il codice open source della blockchain è stato modificato e riadattato per creare sistemi che possono scambiare e mettere al sicuro vari tipi di informazioni. Recentemente, ingegneri e aziende hanno indagato come questa tecnologia possa tornare utile anche in settori al di fuori di quello finanziario.

Tra questi, alcuni hanno già avviato azioni di incorporamento di questa tecnologia, mentre per altri sono già state teorizzate alcune possibili future metodologie di utilizzo. Nella presente sezione andremo ad esaminare i seguenti settori:

- **Finanziario**: riduzione delle commissioni dovuti all'assenza di intermediari nelle transazioni e nei pagamenti digitali;

- **Assicurativo**: prevenire frodi e riduzione dei costi delle piattaforme di gestione velocizzandone i processi;

- **Pubblicitario**: prevenire frodi informatiche e garantire la privacy degli utenti;

- **Energetico**: trasformare l'intero settore e le sue metodologie di distribuzione a favore di una riduzione negli sprechi;

- **Diritti d'autore**: transazione di acquisto su piattaforme di servizi più sicure e regolamentate grazie agli smart contracts a protezione dei copyrights.

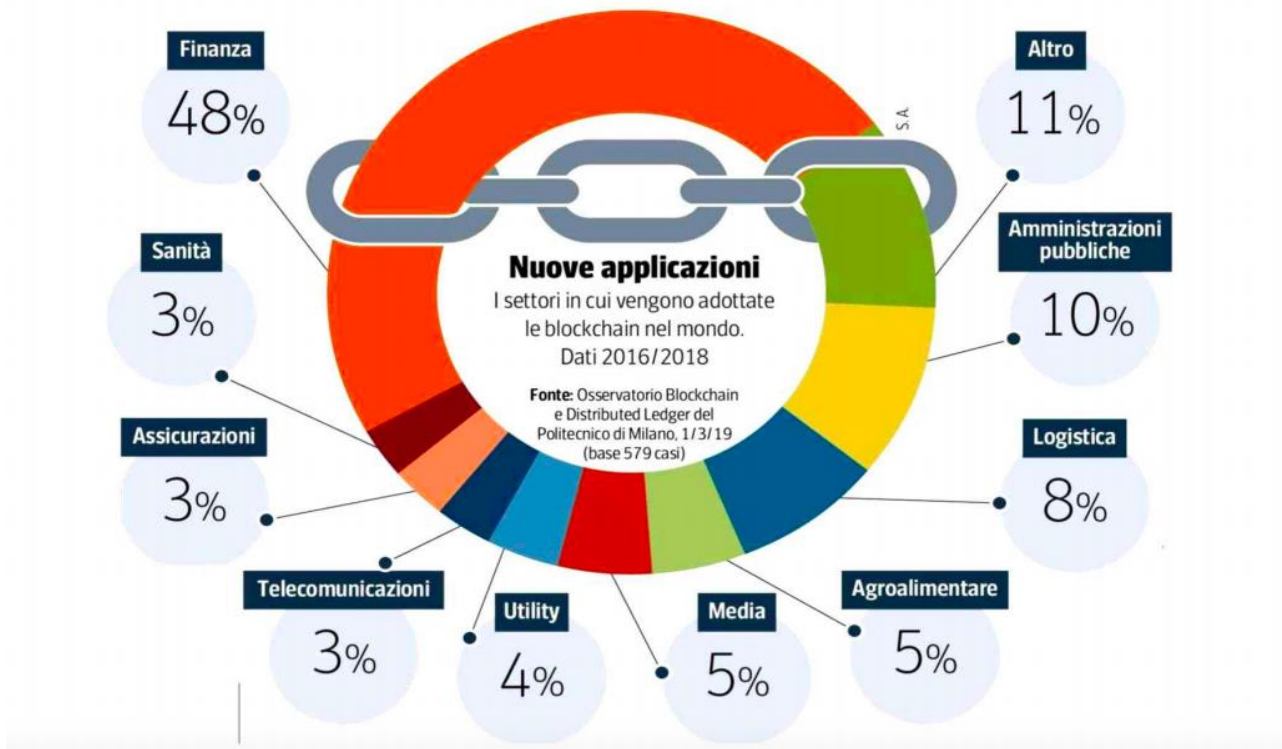
- **Amministrazione pubblica**: immediato accesso ai dati con il conseguente abbattimento dei tempi burocratici;

- **Sanitario**: creazione di uno storico sul paziente, facilitando la consultazione di informazioni per il personale sanitario;

- **e-Governance**: alta riservatezza dei dati condivisi dei cittadini e alleggerimento burocratico per quest'ultimi;

- **Voto elettronico**: a protezione dell'opinione pubblica e prevenzione di frodi per garantire il corretto svolgimento delle elezioni;

- **Tassazione**: evitare frodi fiscali e ricreare un sistema di tassazione più equo ed efficiente;



2.1.1 Finanziario

La nascita del Bitcoin, può essere definito un evento scatenante, se andiamo a vedere l'ingente numero di criptovalute nate da allora, ed ognuna distinta da funzionalità proprie. Basti pensare che nel 2009 il Bitcoin entrava nel mercato digitale con un valore iniziale di 0,00076 dollaro per criptovaluta, e ad oggi il suo valore si aggira intorno ai 13.000 dollari per unità

La Blockchain è una delle tecnologie più chiacchierate del mondo finanziario. Le banche e i player del settore hanno ormai compreso l'importanza di Blockchain e Distributed Ledger e sono sempre più numerosi i servizi basati su queste tecnologie promossi da istituti finanziari e assicurativi nel mondo.

Anche gli istituti finanziari e le compagnie assicurative italiane stanno iniziando a investire nelle tecnologie Blockchain e Distributed Ledger, sia partecipando a soluzioni di sistema internazionali o italiane, sia con progettualità individuali.

Sono nate anche **iniziative di sistema tutte italiane**. Un primo esempio è il progetto Spunta Interbancaria, sviluppato da 14 istituti finanziari in collaborazione con ABILab, NTT Data e SIA. Il progetto, che ha concluso la prima fase di test a inizio autunno 2018, ha l'obiettivo di applicare le tecnologie Distributed Ledger ai processi interbancari per migliorare la trasparenza e la visibilità delle informazioni scambiate tra gli istituti e aumentare la velocità delle operazioni utilizzando la piattaforma Corda.

Alcuni istituti stanno poi sviluppando progetti internamente. **Intesa Sanpaolo**, ad aprile 2017, ha sviluppato una sperimentazione in collaborazione con la startup Eternity Wall per notarizzare dati relativi a transazioni finanziarie sulla Blockchain di Bitcoin. Banca Popolare di Sondrio ad agosto 2018 ha lanciato un servizio per registrare sulla Blockchain di Bitcoin il consenso al rinnovo della polizza RC Auto espresso dal cliente. Borsa Italiana in collaborazione con IBM ha invece testato la tecnologia Blockchain in un progetto volto a sostituire i certificati di trading cartacei emessi dalle PMI.

Negli istituti assistiamo ad approcci alle tecnologie Blockchain e Distributed Ledger molto differenti: c'è chi si sta adoperando per trasformare in progetti operativi le sperimentazioni e chi si dichiara non ancora convinto della portata innovativa della tecnologia. Tuttavia, nonostante il meccanismo di fiducia distribuita della blockchain potrebbe essere una soluzione ottimale per lo scambio di denaro su scala globale, la mancanza di un sistema di regolamentazione chiaro e condiviso in scala globale di tale tecnologia, alimenta gli scetticismi e ne rallenta l'implementazione su larga scala. È probabile che queste criticità troveranno soluzione nel breve periodo.

2.1.2 Assicurativo

Ad oggi, molte polizze assicurative sono ancora trattate su carta stampata, e quindi soggette ad un trattamento manuale su tutto il processo assicurativo, ciò nonostante, con l'avvento dell'IoT, il sistema di relazionarsi con gli utenti ed i modelli di business del mondo assicurativo hanno avuto, e stanno tutt'ora subendo un notevole cambiamento.

A tal proposito sono nate collaborazioni come B3i Services AG, nata nel 2018, un consorzio che comprende 19 delle principali compagnie del mercato assicurativo, tra cui Allianz, Zurich, China Pacific Insurance Company, Aegon, Generali e Mapfre, con l'obiettivo di creare sistemi assicurativi autonomi, che sfruttano una base di dati estremamente ampia, dedicata a far previsioni, valutare rischi e sviluppare algoritmi, che sappiano calcolare il giusto prezzo per ogni assicurazione ed il corrispettivo premio, utilizzando come riferimento tutte le informazioni possibili dell'utente interessato.

Inoltre, l'automatizzazione della gestione dei contratti ha portato a stimare una possibile riduzione dei costi gestionali del 60% per le compagnie assicurative. La combinazione di blockchain e smart contract potrebbe veramente rivoluzionare i metodi gestionali di un settore vecchio di decenni, migliorando non solo i processi per chi lavora nel settore assicurativo, ma anche per i suoi clienti.

2.1.3 Marketing e Digital Advertising

Una recente pubblicazione dell'AdAge Marketing Fact Pack 2020 ha rivelato che il digital advertising nel 2020 raggiungerà più della metà (il 53%) della spesa pubblicitaria nel mondo. La crescita complessiva della spesa pubblicitaria nel 2020 potrebbe essere il doppio rispetto al 2019, per un totale di 656 miliardi, di cui 336 miliardi corrispondono ad investimenti online.

In questo mercato la blockchain vive ancora in uno stato di incognita, ma la sua tecnologia di base, seppur agli inizi, è quella con il maggior potenziale per innescare una vera e propria rivoluzione nel settore. I sistemi blockchain mirano a mettere in contatto tutte le parti coinvolte tra editori, pubblicitari, fornitori di tecnologia e agenzie così da incentivare anche il crearsi di fiducia tra loro. Inoltre, apportando soluzioni nei punti di criticità dell'industria pubblicitaria tra frodi online e importanti problemi di privacy, usare una miglior tracciatura dei contenuti attraverso la blockchain potrebbe rivelarsi una grossa opportunità per ridistribuire i budget pubblicitari in modo corretto, ed instaurare tra gli utenti che ci lavorano un ecosistema più stabile e giusto.

I marketer potranno costruire profili dei propri clienti più affidabili. L'interazione peer-to-peer sappiamo che elimina intermediari, mettendo a diretto contatto, in questo caso, i brand con i loro clienti.

Questo permette ai dipartimenti di marketing di interagire direttamente con gli utenti della rete ed estrapolare le informazioni di cui hanno bisogno da loro, in modo più semplice e diretto, attraverso un sistema più sicuro e trasparente per la condivisione dei dati sensibili.

2.1.4 Energetico

Il settore energetico ormai da tempo ha iniziato un percorso di trasformazione data da una crescente attenzione al tema ambientalistico da parte dei consumatori. Per lungo tempo l'attenzione era riposta nello sviluppo di fonti nuove di energia con un'impronta sempre più green, a discapito di processi produttivi di origine nucleare o per mezzo di combustione.

Ad oggi, gli attori impegnati in questa evoluzione si incontrano tutt'ora nella ricerca e nello sviluppo di fonti energetiche alternative, dando però particolare attenzione a nuove tecniche di gestione e razionalizzazione dei consumi. La blockchain e le tecnologie annesse sembrano particolarmente adatte per aprire a nuove forme di scambio e commercializzazione dell'energia e presto, con l'ascesa dell'IoT, il mercato energetico si ritroverà a dover affrontare una vera rivoluzione tecnologica e socioeconomica, l'intero settore potrebbe subire una vasta trasformazione.

L'utilizzo di numerosi dispositivi elettronici collegati tra loro porta con sé la necessità di creare una vasta rete di informazioni, in cui diversi dispositivi abbiano la possibilità di ricevere e condividere dati in tempo reale e senza bisogno di intermediari. Uno degli usi più ovvi per una tecnologia a distributed ledger come blockchain è quello di fornire una piattaforma efficiente nella registrazione ed esecuzione di tali transazioni.

Una delle più interessanti prospettive nel campo energetico è l'introduzione di scambi peer-to-peer, ovvero lo scambio di energia tra consumatori finali. A fronte di uno sviluppo di strumenti e mezzi sempre più efficienti nell'ottimizzare la produzione privata di energia va man mano definendosi la figura del "Prosumer", ovvero microproduttori e consumatori di energia.

Lo sviluppo tecnologico lascia presumere un aumento nella produzione privata di energia nei prossimi anni, portando nei singoli casi un eccesso di produzione che se non redistribuito nel mercato creerebbe esclusivamente degli sprechi. In altre parole, serve l'introduzione di un sistema di gestione intelligente dell'energia a favore di una gestione migliore della produzione e dei consumi. A questo scopo un sistema peer-to peer energetico permetterebbe di attuare transazioni tra pubblici cittadini, per la compravendita del surplus energetico tra diversi soggetti, andando a gestire nella miglior forma possibile gli esuberanti e limitare gli sprechi. In parole semplici, significherebbe dare la possibilità ai prosumer di vendere ai propri vicini di casa l'energia prodotta in eccesso.

I vantaggi connessi ad un corretto bilanciamento della rete sono evidenti, considerando che la produzione energetica dei privati si basa per lo più nell'utilizzo di pannelli fotovoltaici e quindi con un'impronta ambientale decisamente inferiore rispetto all'energia venduta dalle aziende private che al più si affidano a fonti di combustione inquinanti.

Quindi, una rete elettrica Smart mette in comunicazione produttori e consumatori, integrando nella rete di distribuzione le funzionalità di una rete di informazioni; quest'ultima preleva informazioni, in tempo reale, dai contatori, dai veicoli e da tutti i prodotti e gli strumenti connessi agli utenti, per poi razionalizzare e distribuire l'energia in maniera efficiente, evitando i sovraccarichi e le variazioni di tensione. È dotata di strumenti di monitoraggio che consentono di tenere traccia di tutto il flusso elettrico del sistema.

2.1.5 Copyright

Indipendentemente dal settore, il Copyright è uno dei temi che con l'avvento di Internet e quindi della società dell'informazione, ha subito una gestione sempre più difficile. La creazione e diffusione di materiale creativo risulta oggi alla portata di tutti, l'offerta di un'ampia quantità di contenuti e l'incredibile crescita nella richiesta di tale materiale creativo trova un limite nella loro facile reperibilità. Questo ha innescato una serie di problematiche proprio in merito ai diritti d'autore, in particolar modo riguardanti le norme giuridiche che dovrebbero regolamentarne l'utilizzo e punire l'inappropriato utilizzo o distribuzione.

La protezione e l'applicazione del copyright erano già molto complesse prima che il mondo si digitalizzasse, la rapida introduzione di servizi di condivisione peer-to-peer di file digitali, non ha permesso ai sistemi giuridici dei paesi di integrare ed applicare normative legislative volte ad una regolamentazione adeguata dei diritti d'autore, questo perché il diritto non ha lo stesso passo evolutivo della tecnologia.

Qui è dove la blockchain, insieme agli smart contracts, potrebbe venire in soccorso ai detentori di copyright. Per fotografi, designer e creatori di contenuti multimediali stanno nascendo piattaforme che permettono agli utenti di caricare i proprio contenuti su una blockchain, che non solo fornirebbe l'autenticazione di proprietà del contenuto ma permetterebbe anche di avere controllo e visibilità sull'utilizzo del contenuto da parte di terzi. Un NFT è un contenuto digitale che rappresenta oggetti del mondo reale come opere d'arte, musica, giochi e collezioni di qualsiasi tipo.

L'NFT è l'acronimo di non fungibile token che in italiano significa gettone non copiabile ossia qualcosa di unico che non può essere sostituito da altro. Chi acquista un'opera legata a un non-fungibile token non acquista l'opera in sé, ma semplicemente la possibilità di dimostrare un diritto sull'opera, garantito tramite uno smart contract. Tutto comincia con una versione digitale dell'opera d'arte. Tipicamente, si usa una foto digitale o una sua documentazione filmata e salvata in formato digitale. Questa versione digitale non è altro che una lunga sequenza di numeri, 0 e 1 nel linguaggio informatico. Tale sequenza viene quindi "compressa" in una sequenza, chiamata hash, derivata da essa ma molto più corta, con un processo non invertibile conosciuto come hashing. Il passo successivo è la memorizzazione di questo hash su una blockchain, con una marca temporale associata.

L'uso di questi token ha aperto la strada a un mercato automatizzato di hash, in cui il creatore dell'hash può usare il token per aggiungere al suo interno il proprio hash e successivamente venderlo in cambio di un pagamento in criptovaluta, come per esempio la moneta ETH usata in Ethereum. L'NFT tiene al suo interno traccia delle vendite dell'hash, in modo che risulta possibile tracciare i passaggi di mano dell'hash, fino al suo creatore, quindi dimostrandone il possesso. Questo meccanismo fornisce quindi una prova di autenticità e, al contempo, di proprietà dell'opera.

Il possessore dell'hash, secondo quanto riportato nell'NFT può dimostrare i suoi diritti senza necessità di rivolgersi a intermediari e senza limiti di tempo (finché la blockchain su cui è ospitato il suo token continuerà ad essere attiva).

Per l'industria musicale invece la comparsa Internet e di piattaforme streaming negli ultimi 15-20 anni ha portato all'affermazione del sistema Pay per Play, ossia una forma di pagamento per singolo ascolto a scopo commerciale. La tecnologia Blockchain può aiutare a rendere trasparente il processo di pagamento delle royalty mantenendo un database decentralizzato accurato e completo per l'archiviazione delle informazioni sulla proprietà dei diritti musicali.

2.2 Amministrazione pubblica

La Blockchain trova ambiti di applicazione e potenzialità enormi anche nel settore pubblico, se si pensi solo all'incredibili opportunità, favorevoli e sfavorevoli, che porterebbe avere un registro pubblico di tutte le identità digitali dei cittadini, condiviso ed indelebile.

Tramite lo sviluppo di registri distribuiti, la pubblica amministrazione potrebbe mantenere sotto controllo alcune specifiche situazioni di norma difficilmente gestibili. Andando ad analizzare i vantaggi, alcuni esempi possono essere per l'evasione fiscale, questa verrebbe realmente sradicata dalla lista dei problemi dei principali paesi, o nel combattere la criminalità un registro dei cittadini di una nazione sicuramente darebbe grande supporto, oppure nei sistemi di welfare grazie alla semplificazione delle procedure burocratiche.

Tuttavia, lo sviluppo di tale tecnologia nei settori governativi è ancora argomento di discussione. La blockchain garantisce metodi innovativi ed efficienti per fornire e gestire i servizi pubblici, ma ad oggi non sono ancora stati stabiliti degli standard da rispettare perché venga garantita la sicurezza e la privacy a lungo termine delle informazioni immagazzinate in queste piattaforme.

A livello pubblico sono numerosissimi i settori che gioverebbero di un sistema blockchain nella gestione delle informazioni, di questi meritano particolare attenzione:

- Il settore sanitario;
- L'e-Governance;
- L'e-Voting;
- I sistemi di tassazione

2.2.1 Sanitario

La rapida ascesa della digitalizzazione ha portato a grandi progressi anche nel campo sanitario, e la blockchain al momento è al centro di numerosi sviluppi a favore di tale settore.

Sicurezza dei dati, archiviazione, accesso, ed integrazione sono immensamente preziosi per qualsiasi organizzazione che necessita manipolare una grande quantità di dati, e quindi per il settore sanitario. Senza efficaci mezzi di tutela dei dati, i pazienti non permetteranno mai la condivisione delle informazioni personali. Per ottimizzare questo servizio è in fase di sperimentazione già da anni il FSE (Fascicolo Sanitario Elettronico).

Il progresso digitale in questo settore, non porta con sé esclusivamente all'introduzione di nuove tecnologie di supporto alla medicina, ma anche alla inevitabile modifica delle politiche a gestione dei dati elettronici e della privacy dei pazienti, l'integrazione della blockchain richiederebbe cambiamenti di vasta portata al sistema giuridico, obbligando a riformare le leggi su banche dati e proprietà intellettuale.

Le applicazioni della blockchain per la sanità può ridefinire ed essere di supporto a sei operatori del settore:

1. Per ospedali apporterebbe migliorie nella gestione dei dati sensibili dei pazienti, riducendo gli errori, migliorando l'interazione tra sistemi differenti e garantendo l'integrità delle informazioni.

2. Per i pazienti tale tecnologia potrebbe garantire la reperibilità dei dati sanitari personali di ogni utente in forma completa ed affidabile, sui quali, tra l'altro sono in corso esperimenti di monetizzazione. Inoltre, permetterebbe un miglior controllo su tali dati per l'utente, che potrebbero scegliere in autonomia con chi condividere tali informazioni ed a quali condizioni.

3. Per i medici diventerebbe uno strumento estremamente efficace per l'ottimizzazione del lavoro e quindi del rapporto con i pazienti. Nonché un perfetto sistema di gestione dell'identità professionale, con certificazioni annesse.

4. Per aziende farmaceutiche la blockchain potrebbe divenire un importante mezzo per la gestione della supply chain, sia per contrastare i fenomeni di contraffazione dei medicinali che per avere un migliore monitoraggio del trattamento clinico a cui è sottoposto ogni paziente.

5. Per le aziende biomediche uno storage dei dati in un sistema chiuso e sicuro permetterebbe una migliore distribuzione di quest'ultimi, considerando sistemi di archiviazione sul cloud, che permetterebbe la condivisione di dati scientifici su scala globale, e sarebbe di incredibile supporto a tutti i reparti di ricerca e sviluppo distribuiti nel pianeta.

6. Per le imprese assicuratrici offrirebbe importanti strumenti di controllo dei dati più affidabili e complete, per analisi più veritiere prima dell'autorizzazione di una copertura di spese mediche, riducendo le frodi e permettendo la creazione di polizze più dinamiche e personalizzate per i suoi clienti.

La tecnologia blockchain apre a nuovi scenari per tutte gli attori coinvolti, ponendosi l'obiettivo di risolvere numerose problematiche di auditing fornendo nuove opportunità per la gestione dei dati sia per il personale sanitario che per i pazienti.

2.2.2 L'e-Government

Una delle funzioni fondamentali di un governo è quella di fornire servizi pubblici adeguati ed efficienti ai suoi cittadini. La blockchain è considerata la tecnologia chiave nello sviluppo dell'e-Government grazie ai suoi innegabili vantaggi e potenzialità.

Da un punto di vista tecnico, la tecnologia blockchain aumenta l'efficienza, fornisce protezione dei dati e trasparenza. Tuttavia, molte nazioni devono ancora affrontare alcuni ostacoli nell'applicazione di tali sistemi a servizio dell'e-Government.

Quando si tratta dei vantaggi della tecnologia blockchain, la trasparenza e la sicurezza delle informazioni sono i primi che vengono in mente. Tuttavia, considerando entrambe queste caratteristiche nello sviluppo dell'e-Government, si creeranno alcuni conflitti. L'obiettivo primario nella sicurezza delle informazioni personali digitali è la riservatezza, ovvero limitare l'accesso ai dati solo a determinati entità è l'unica via perché questa non vadano nelle mani di malintenzionati.

Al contrario, la trasparenza mira alla parità di accesso alle informazioni per tutte le persone, garantendo chiarezza, coerenza ed affidabilità. Per applicare un sistema blockchain a sostegno di un e-government bisogna identificare l'obiettivo principale della protezione dei dati e comprendere come inserirlo nel contesto politico in cui si trova il paese di riferimento. Garantire trasparenza e riservatezza in un sistema blockchain comporta numerose difficoltà computazionali dovendo ricreare protocolli di sicurezza estremamente complessi.

Le caratteristiche di trasparenza e di immutabilità che offrono permettono di rilevare la manipolazione dei dati e le informazioni memorizzate al suo interno risultano quasi impossibili da rubare, modificare o cancellare, il che garantisce l'integrità dei dati dei cittadini e delle pubbliche amministrazioni.

2.2.3 L'e-Voting

Un'altra delle applicazioni più suggestive nel settore pubblico è sicuramente collegato all'utilizzo della blockchain a sicurezza del voto elettorale elettronico, che ormai da tempo trova difficoltà di implementazione a causa delle complessità nel poterne garantire la totale sicurezza.

La sicurezza del metodo di voto richiede sicurezza dell'intero processo, a prevenzione di possibili attacchi esterni si identificano le vulnerabilità dei processi elettorali elettronici su quattro punti:

1. Manipolazione dell'opinione pubblica pre-elezioni. I media ed i servizi volti all'informazione pubblica hanno un profondo effetto sui risultati elettorali. Prima di un'elezione, le opinioni politiche degli elettori possono essere plasmate dai media a cui siamo costantemente esposti. Campagne di disinformazione mirate possono causare difficoltà per gli elettori nel distinguere le fonti veritiere da quelle che non lo sono e quindi dare una logica al proprio voto seguendo resoconti derivati da informazioni accurate e non casuali;

2. Violazioni dei database di registrazione degli elettori. La rimozione di un utente dai database di registrazione minaccia fortemente le capacità di voto delle persone. Uno di questi attacchi eseguito su larga scala potrebbe ritardare o addirittura impedire il corretto svolgimento di una elezione.

3. Intrusione nei sistemi hardware di voto o di tabulazione dei dati. Gli esperti di sicurezza informatica concordano sulla vulnerabilità dei dispositivi elettronici e dei sistemi di rete informatica connessi ad internet. Un hackeraggio potrebbe compromettere la tabulazione dei dati oppure permettere la manomissione di questi, e minare la credibilità del sistema elettorale.

4. Falsificazione delle verifiche post-elezioni. Sistemi di reporting manipolati potrebbero annunciare risultati di votazione imprecisi o falsati, il che permetterebbe la diffusione di notizie non vere al pubblico.

Apparentemente la blockchain necessita ancora di strumenti di supporto e riadattamenti tecnici per raggiungere il suo potenziale e fronteggiare tutte le problematiche di sicurezza legate al e-voting, questa tecnologia pone delle buone basi per un cambio radicale nel modello elettorale di molti paesi.

2.2.4 Sistemi di tassazione

Le autorità fiscali di tutto il mondo stanno iniziando a intravedere i possibili vantaggi derivanti dall'utilizzo di sistemi blockchain in aree come il welfare pubblico ed il pagamento delle tasse per i cittadini, che potrebbe portare ad una grossa riduzione nell'evasione fiscale, specialmente in paesi come l'Italia.

È importante che un governo garantisca efficienza del suo sistema di riscossione delle imposte e che la riscossione avvenga tramite una metodologia volta a rispettare costi minimi a fronte del massimo risultato, dato che è proprio grazie ai proventi della riscossione che tali servizi ed operazioni statali vengono elargiti.

Fornire informazioni trasparenti, controllabili, sicure e in tempo reale è fondamentale per offrire un sistema di riscossione delle imposte efficace. In molti paesi l'evoluzione tecnologica ha portato il settore pubblico a dover individuare nuove modalità di riscossione delle imposte dai suoi cittadini.

Troviamo già degli esempi negli Emirati Arabi o nel Regno Unito: entrambi pianificano di implementare un sistema fiscale digitalizzato in pochi anni.

Ogni informazione verrebbe registrata in forma permanente su blockchain, creando così una fonte affidabile, indiscutibile e dal facile accesso su cui le autorità possono fare affidamento. Dall'altra parte i cittadini grazie alla crittografia legata ad ogni transazione avrebbero la possibilità di vedere dove andranno ridistribuiti ed usati i soldi delle proprie tasse, massimizzando così la trasparenza dell'intero sistema statale.

CONCLUSIONI

Fatta un po' di chiarezza, in merito al concetto di blockchain, sono state descritte le componenti principali, la struttura, il funzionamento di base e sono state anche presentate, nonché ipotizzate, alcune delle possibili applicazioni di questo nuovo sistema.

L'analisi svolta in questa tesi permette di affermare che i sistemi basati su tecnologia Blockchain sono estremamente versatili, ed il fatto che vengano sfruttati per lo più come base a favore dello sviluppo di criptovalute riduce fortemente l'impatto che potrebbero avere sulla società.

L'applicazione di sistemi Blockchain a supporto del management può realmente agire come fonte di un vantaggio competitivo non solo per le imprese, ma anche per le nazioni ed i governi degli stessi, nonché per ogni organizzazione coinvolta.

Nonostante gli enormi progressi fatti negli ultimi cinque anni, la tecnologia blockchain si può considerare in uno stato di sviluppo, volendo però essere ottimisti, la costante evoluzione tecnologica potrebbe, nel breve termine, portare sul mercato gli strumenti necessari per permettere la corretta implementazione dei sistemi blockchain in qualsiasi ambito economico e sociale.

In conclusione, la Blockchain potrebbe rivelarsi il mezzo perfetto, la conclusiva e definitiva pagina del completamento della rivoluzione industriale 4.0, portando, un po' di certezza ed ordine in tutti i settori economico-sociali conosciuti.

BIBLIOGRAFIA

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

<https://bitcoin.org/bitcoin.pdf>

[2] G.B. Martelli, BLOCKCHAIN a cura di Studio Martelli & Partners S.p.A., editoriale e grafico Studio Martelli & Partners S.P.A., Settembre 2014.

https://www.studiomartelli.it/wp-content/uploads/2014/10/STUDIO-MARTELLI_blockchain.pdf

[3] Iuon-Chang Lin and Tzu-Chun Liao, A Survey of Blockchain Security Issues and Challenges, International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017.

<https://arxiv.org/ftp/arxiv/papers/1911/1911.02013.pdf>

[4] Dominique Guegan, Public Blockchain versus Private blockchain, Documents de Travail du Centre d'Economie de la Sorbonne , May 2017.

[Public Blockchain versus Private blockchain \(archives-ouvertes.fr\)](Public Blockchain versus Private blockchain (archives-ouvertes.fr))

[5] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, Muhammad Imran, An Overview on Smart Contracts: Challenges, Advances and Platforms, the Deanship of Scientific Research at King Saud University, Dic 2019.

<https://arxiv.org/pdf/1912.10370.pdf>

[6] Maher Alharby and Aad van Moorsel, Blockchain-based smart contracts: A systematic mapping study, School of Computing Science, Newcastle University, 2017.

<https://arxiv.org/ftp/arxiv/papers/1710/1710.06372.pdf>

[7] Wubing Chen, Zhiying Xu, Shuyu Shi, Yang Zhao, Jun Zhao, A Survey of Blockchain Applications in Different Domains, the project "Secure databases based on SGX" of Alibaba-NTU Singapore Joint Research Institute, 2018.

[1911.02013.pdf \(arxiv.org\)](1911.02013.pdf)

[8] Wang, W., Hoang, D. T., Xiong, Z., Niyato, D., Wang, P., Hu, P., and Wen, Y. , A Survey on Consensus Mechanisms and Mining Management in Blockchain, Feb 2019.

[1805.02707.pdf \(arxiv.org\)](1805.02707.pdf)

[9] UNECE, White Paper Blockchain in Trade Facilitation, 2019.

[WhitePaperBlockchain.pdf \(unece.org\)](WhitePaperBlockchain.pdf)

[10] Milan Sallaba, Alexander Mogg, Mirko René Gramatke, Ralf Esser, Jens Herrmann Paulsen, Blockchain @ Media A new Game Changer for the Media Industry?, Deloitte, 2017.

[PoV Blockchain Media interaktiv.indd \(deloitte.com\)](PoV_Blockchain_Media_interaktiv.indd)

[11] Erik Kornelson, Blockchain Applications in the Media and Advertising Industry, 2019.

[12] Merlinda Andonia, Valentin Robua, David Flynn, Simone Abramb, Dale Geachc, David Jenkins, Peter McCallumd, Andrew Peacockd, Blockchain technology in the energy sector: A systematic review of challenges and opportunities. ScienceDirect, Nov 2018.

<Blockchain technology in the energy sector: A systematic review of challenges and opportunities - ScienceDirect>

[13] Benoit Laclau, Why the energy sector must embrace blockchain now. Ernest&Young April 2018.

[Why the energy sector must embrace blockchain now | EY - Global](#)

[14] Balázs Bodó, Daniel Gervais, João Pedro Quintais, Author Notes. Blockchain and smart contracts: the missing link in copyright licensing?. International Journal of Law and Information Technology, Volume 26, Issue 4, Winter 2018, Pages 311- 336, <https://doi.org/10.1093/ijlit/eay014>. September 2018
<https://academic.oup.com/ijlit/article/26/4/311/5106727>

[15] Seyednima Khezr, Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. MDPI, April 2019.

[Applied Sciences | Free Full-Text | Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research \(mdpi.com\)](#)

[16] Gijbert Bulk. How blockchain could transform the world of indirect tax. Ernest&Young, April 2018.

[Tax services | EY - Global](#)

[17] CHRISTINE LEONG, TAL VISKIN and ROBYN STEWART. TRACING THE SUPPLY CHAIN. How blockchain can enable traceability in the food industry. Accenture Article, 2018.

[Accenture-Tracing-Supply-Chain-Blockchain-Study-PoV.pdf](#)

[18] Kamanashis Biswas, Vallipuram Muthukkumarasamy and Wee Lum Tan. Blockchain Based Wine Supply Chain Traceability System. School of Information and Communication Technology Griffith University Gold Coast, Australia, 2017.

[\[PDF\] Blockchain Based Wine Supply Chain Traceability System \(researchgate.net\)](#)

[19] Stefan Schrauf and Philipp Bertram. How digitization makes the supply chain more efficient, agile, and customer-focused. PWC Article, 2016.

[how-digitization-makes-the-supply-chain-more-efficient-pwc-2016.pdf](#)

[20] Mark Deimel, Mechthild Frentrup and Ludwig Theuvsen. Transparency in food supply chains: empirical results from German pig and dairy production. GeorgAugust University Goettingen, Department of Agricultural Economics and Rural Development, 2008.

[Transparency in food supply chains: empirical results from German pig and dairy production \(wageningenacademic.com\)](#)

[21] Pankaj Dutta, Tsan-Ming Choi, Surabhi Somani and Richa Butala. Transportation Research Part E: Logistics and Transportation Review: Blockchain technology in supply chain operations: Applications, challenges and research opportunities. ScienceDirect, October 2020.

[Blockchain technology in supply chain operations: Applications, challenges and research opportunities - ScienceDirect](#)

[22] Arman Jabbari and Philip Kaminsky. Blockchain and Supply Chain Management. College Industry Council on Material Handling Education (CICMHE). January 2018.

[blockchain-and-supply-chain-management.pdf \(mhi.org\)](#)

[23] Journal: Supply Chain Management: an International Journal. Blockchain Technology: Implications for operations and supply chain management. Emerald Publishing, Sept. 2018.

[PDF_Proof.pdf \(lancs.ac.uk\)](#)

[24] Gregor Blossey, Jannick Eisenhardt and Gerd J. Hahn. Blockchain Technology in Supply Chain Management: An Application Perspective. Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019.

[\[PDF\] Blockchain Technology in Supply Chain Management: An Application Perspective | Semantic Scholar](#)

[25] Ali Dorri, Salil S. Kanhere, and Raja Jurdak. Blockchain in Internet of Things: Challenges and Solutions. Ali Dorri and Salil S. Kanhere are with The University of New South Wales (UNSW); Raja Jurdak is with CSIRO Brisbane.

[Microsoft Word - Final_AD_SK.docx \(arxiv.org\)](#)

[26] Nick Szabo, Smart Contracts: Building Blocks for Digital Markets. White Paper. 1996.

[Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf \(truevaluemetrics.org\)](#)

SITOGRAFIA

- [27] https://it.wikipedia.org/wiki/Innovazione_distruttiva
- [28] [Chi è Satoshi Nakamoto, l'uomo che ha inventato il Bitcoin - Blockchain 4innovation](#)
- [29] https://it.wikipedia.org/wiki/Rivoluzione_digitale
- [30] [Catena di montaggio - Wikipedia](#)
- [31] [La decentralizzazione è il fattore più importante della Blockchain | HTML.it](#)
- [32] [criptovaluta in Vocabolario - Treccani](#)
- [33] [https://it.bitcoinwiki.org/wiki/Double-spending_\(doppia_spesa\)](https://it.bitcoinwiki.org/wiki/Double-spending_(doppia_spesa))
- [34] [Bitcoin: potenzialità e limiti del fenomeno delle criptovalute | Salvis Juribus](#)
- [35] [How does a block chain prevent double-spending of Bitcoins? \(investopedia.com\)](#)
- [36] https://en.wikipedia.org/wiki/Brute-force_attack
- [37] <https://www.investopedia.com/terms/1/51-attack.asp>
- [38] [Mining criptovalute e Bitcoin: cos'è, come farlo \(cloud e non\) e guadagni \(blockchain4innovation.it\)](#)
- [39] <https://medium.com/>
- [40] [Blockchain: cos'è, come funziona e applicazioni oggi \(blockchain4innovation.it\)](#)
- [41] [Che cosa sono e come funzionano le Blockchain Distributed Ledgers Technology - DLT - Blockchain 4innovation](#)
- [42] [La classificazione delle Blockchain: pubbliche, permissioned e private \(spindox.it\)](#)
- [43] [The difference between public and private blockchain IBM Supply Chain and Blockchain Blog](#)
- [44] [Token: cos'è e come viene utilizzato nelle criptovalute - Blockchain 4innovation](#)
- [45] [Criptovalute, tokens e coins: sono la stessa cosa? \(fintastico.com\)](#)
- [46] <https://medium.com/fraglie-digitali/la-classificazione-dei-token-f1551aed0b09>
- [47] <https://cryptonomist.ch/2018/12/01/classificazione-token/>
- [48] <https://www.ethereum-italia.it/community/322/>
- [49] <https://www.pmf-research.eu/smart-contracts-e-implicazioni-blockchain/>
- [50] [What is a Smart contract and how does it work? \(cointelegraph.com\)](#)
- [51] <https://blockgeeks.com/guides/ethereum-gas/>
- [52] <https://nirolution.com/decentralized-autonomous-organization/>
- [53] <https://blockchainhub.net/dao-decentralized-autonomous-organization/>
- [54] <https://www.multichain.com/blog/2016/06/smart-contracts-the-dao-implosion/>
- [55] [Homepage - solofinanza.it](#)
- [56] <https://medium.com/@coinsociety/la-nascita-di-bitcoin-4c0b2e4213ce>

- [57] https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni
- [58] [Blockchain: cos'è, come funziona e applicazioni oggi \(blockchain4innovation.it\)](#)
- [69] [Qual è la Differenza tra Blockchain e Bitcoin? | Binance Academy](#)
- [70] <https://www.money.it/Ethereum-cos-e-come-funziona>
- [71] <https://www.preethikasireddy.com/post/how-does-ethereum-work-anyway>
- [72] <https://medium.com/@micheledaliessi/how-does-ethereum-work-8244b6f55297>
- [73] <https://etherevolution.eu/consenso-blockchain/>
- [74] [Announcing Oxygen - the First Crypto Repo Trading Platform \(aithority.com\)](#)
- [75] [Tecnologia blockchain migliora la customer e le assicurazioni riducono i costi Assinews.it](#)
- [76] [Aigang \(AIX\) the Autonomous Insurance Network — Fully Automated Insurance for IoT Devices and a Platform for Insurance Innovation Built around Data | by Crypto Research by William Thrill | Medium](#)
- [77] [Blockchain e digital advertising: ecco come tutelare i dati dei consumatori - Agenda Digitale](#)
- [78] [La Blockchain nel Digital Advertising e nel mondo del Marketing \(osservatori.net\)](#)
- [79] [Il copyright nel mondo digitale | Pearson](#)
- [80] [Energia e blockchain: come cresce il mercato e in quali ambiti applicativi - Blockchain 4innovation](#)
- [81] <https://musicoin.org/>
- [82] <https://coinswitch.co/info/musicoin/what-is-musicoin>
- [83] [Energia e blockchain: come cresce il mercato e in quali ambiti applicativi - Blockchain 4innovation](#)
- [84] [Blockchain per il settore sanitario: casi d'uso e trend futuri - Agenda Digitale](#)
- [85] [Blockchain per il settore sanitario: casi d'uso e trend futuri - Agenda Digitale](#)
- [86] <https://guardtime.com/>
- [87] <https://www.cbinsights.com/research/report/blockchain-election-security/>
- [88] [E-Voting e blockchain, sì o no: i casi internazionali - Agenda Digitale](#)
- [89] <https://www.fintricity.com/blockchain-tax-fraud/>
- [90] [Il copyright nel mondo digitale | Pearson](#)
- [91] <https://cryptoinsider.media/musicoin-music-industry-artists-listeners-rewarded/>
- [92] [Il copyright nel mondo digitale | Pearson](#)
- [93] [Supply Chain Management: cos'è e perché è importante per le aziende \(digital4.biz\)](#)
- [94] <https://applicature.com/blog/blockchain-technology/blockchain-scalability>
- [95] https://it.wikipedia.org/wiki/Agente_intelligente
- [96] [Cypherpunk - Wikipedia](#)
- [101] [Bitcoin: come funziona il sistema | by Andrea Ferraresso | Medium](#)

