POLITECNICO
DI TORINO

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

Tesi di Laurea Magistrale

Tecnologia Blockchain:
strumento per le reti industriali di domani

Relatore: *Federico Piglione*

Candidato: *Marcello Pulcher*

Anno accademico 2019 / 2020

INDICE

Introduzione

Nella teoria imprenditoriale, l'innovazione dirompente (o distruttiva) è un'innovazione che crea un nuovo mercato. Infatti, mentre provoca l'estinzione di un mercato o di una rete di valori esistenti, essa produce altresì una nuova rete di valori mediante la progressiva sostituzione di prodotti, aziende e leader dei settori.
Il termine è stato definito per la prima volta nel 1995 dallo studioso americano Clayton M.Christensen, definito in seguito come *"l'idea imprenditoriale più influente del XXI secolo"* [37] .

Non tutte le innovazioni sono *dirompenti* come sopraindicato, sebbene indiscutibilmente rivoluzionarie. Per fare un esempio su tutti, le prime automobili, prodotte alla fine del XIX secolo, non furono un'innovazione dirompente, dal momento che, stante l'evidente connotazione di "prodotti di lusso", destinati pertanto ad una limitatissima fetta di mercato, non concorsero in modo realmente competitivo coi veicoli trainati da cavalli. Infatti il mercato dei trasporti rimase sostanzialmente immutato fino al noto debutto, nel 1908, della Ford Model T ad un prezzo decisamente più basso delle concorrenti, grazie alla produzione in serie, utilizzando una delle prime catene di montaggio. Di fatto, l'innovazione distruttiva in questo caso non è la Ford Model T [40], bensì l'innovazione della catena di montaggio che ha permesso di contraddistinguere la Model T, grazie alla produzione in massa e al suo prezzo di mercato, ben più che competitivo. Tale innovazione ha costretto i colossi del mercato automobilistico ad evolversi con impianti moderni, adattandosi al nuovo sistema di produzione in massa.

Anche l'epoca in cui viviamo è sempre più caratterizzata da un forte impulso verso nuove tecnologie, alcune delle quali sono paragonabili all'avvento della catena di montaggio nei sistemi produttivi di inizio 900'. Tra queste sono senz'altro da considerare: l'Intelligenza Artificiale (AI), la Realtà Aumentata (AR), i droni, l'Internet of Things (IoT), i robot, la Realtà Virtuale (VR), le stampanti 3D e ovviamente la Blockchain.
Con il rapido progresso della digitalizzazione, le organizzazioni sia pubbliche che private, con l'intento di apportare migliorie ai propri processi e ai prodotti e servizi relativi, si trovano sempre più spesso ad affrontare l'implementazione di queste tecnologie digitali. Allo stesso tempo, queste tecnologie emergenti possono anche sconvolgere gli attuali

modelli di business e cambiare le aspettative esterne. Fra tutte, merita particolare attenzione la tecnologia blockchain, un sistema decentralizzato basato su reti *peer–to–peer*, senza intermediari, nato funzionalmente con il Bitcoin, allo scopo di creare un sistema di pagamento basato su valute digitali, anche dette criptovalute.

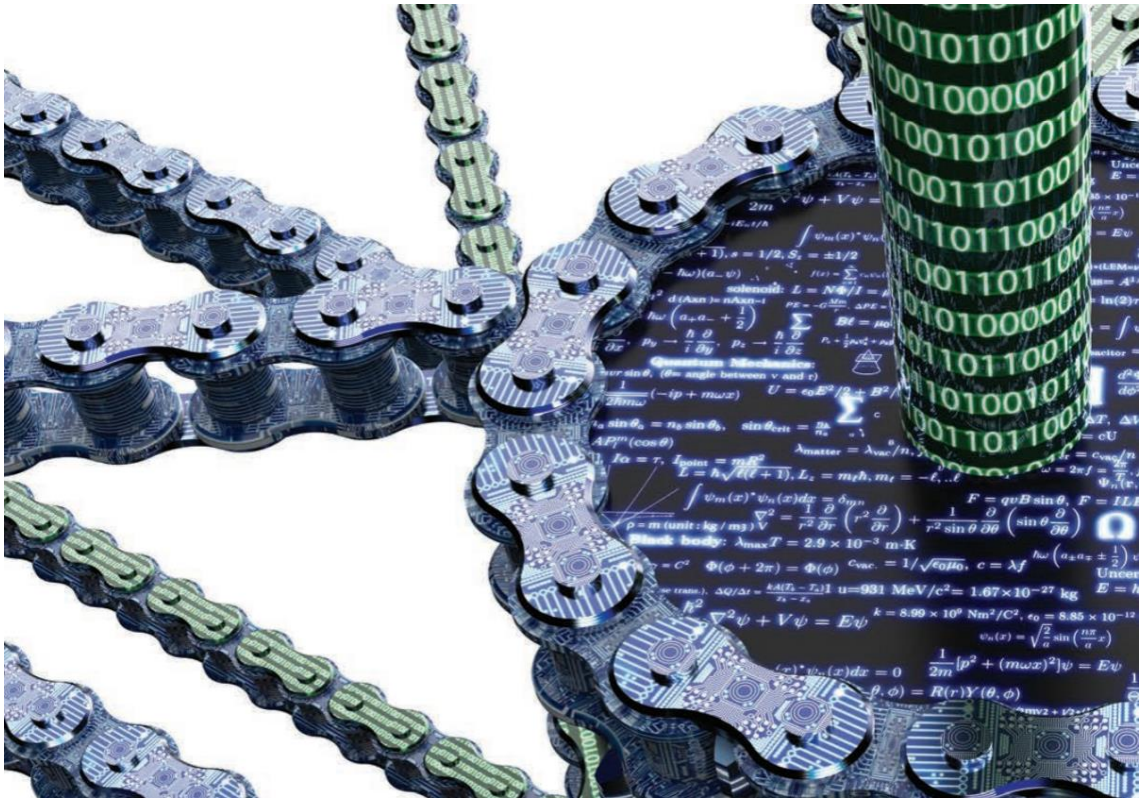

Figura 1. Idealizzazione della c.d. Blockchain

Tra le principali società di consulenza, prevale l'opinione che la Blockchain rientri tra le nuove tecnologie emergenti da monitorare, poiché potrebbe avere, con buona probabilità, un grande impatto sull'economia mondiale.

I ricercatori ed gli esperti del settore credono fortemente nel potenziale della Blockchain, e, tra essi, alcuni sostengono che possa avere lo stesso sviluppo che Internet ha ottenuto negli ultimi decenni. Esattamente come internet, la Blockchain ha creato nuove opportunità e nuovi modelli di business per lo scambio di valore ed informazioni, così come, allo stesso modo, dovrebbe assicurare nuove opportunità di scala non dissimili. Fondamentalmente questa nuova fase dell'era digitale sta portando a molte sfide per la

società, ma anche a nuovi pericoli in un futuro incerto, poiché il cambiamento sta avvenendo molto velocemente e tuttora con un'accelerazione esponenziale. Una ipotesi da considerare è che non tutti – o, per meglio dire, i più – sapranno o avranno la possibilità di adattarsi al cambiamento che l'era digitale comporta.

Con la presente tesi si vuole dare un quadro generale del funzionamento della Blockchain e delle tecnologie a supporto di quest'ultima, come ad esempio gli *Smart Contract* o i dispositivi *IoT*, presentando pertanto le principali piattaforme esistenti, andando ad analizzare le tipologie di utilizzo e le loro criptovalute. Nei capitoli che seguono verranno trattate le opportunità di utilizzo di tali tecnologie a supporto dei principali settori produttivi della società moderna, per poi passare ad un'analisi approfondita delle soluzioni e delle problematiche relative ai processi di *supply chain*, in diversi ecosistemi industriali.

CAPITOLO 1

INTRODUZIONE E FUNZIONAMENTO DELLA BLOCKCHAIN

1.1 Origine della Blockchain

Sono gli anni 80' e 90' ed il mondo si sta preparando ad entrare nell'era della digitalizzazione.

La rivoluzione digitale (anche detta rivoluzione informatica) è il passaggio della tecnologia meccanica ed elettronica analogica a quella elettronica digitale che, iniziata durante i tardi anni Cinquanta, con l'adozione e proliferazione di computer e memorie digitali nei paesi industrializzati del mondo, negli anni avvenire avrebbe poi cambiato l'intero sistema economico e ancor di più quello sociale [39] .

Con l'avvento dei computer e delle seguenti tecnologie, il mondo si è anche popolato, a supporto di questo nuovo mercato rivoluzionario, di programmatori ed hacker. Di questi, molti 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 sin dai suoi inizi, per questo nacquero gruppi di programmatori ed hacker ribelli interessati a creare una privacy assoluta nel mondo informatico, tra questi c'erano i "The Cypherpunks".

I Cypherpunk [38] si specializzarono nella criptografia 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, c'era un certo Eric Hughes, matematico americano, programmatore di computer che attraverso il Manifesto Cypherpunk [100] 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. Tuttavia, pur avendo l'idea, non sono mai riusciti a creare un tecnicismo per realizzare una vera esperienza peer-to-peer. Solo dopo il crollo del mercato azionario del 2008, il mondo era pronto per una rivoluzione *digital finanziaria*.

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" (Bitcoin: un sistema di cassa elettronico peer-to-peer), firmato sotto lo pseudonimo di Satoshi Nakamoto [1].

Mentre l'attenzione mondiale era riposta 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'obbiettivo 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 e portando così ad una vera e propria rivoluzione finanziaria [68] .

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.

Nel 2008 fu divulgato il paper sopracitato, mentre soltanto il 3 gennaio del 2009 fu condivisa una prima versione del software client, ovvero la prima versione del software disponibile al pubblico, ufficializzando così la nascita del Bitcoin, e con esso della prima criptovaluta [38] .

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* [9] .

Invece del dollaro Usa, o dell'euro Europeo, il valore viene scambiato in una valuta digitale, chiamata Bitcoin o suoi similari. 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.

Inizialmente, la comunità di crittografi e programmatori non comprese la potenzialità del Bitcoin di Satoshi Nakamoto, solo un programmatore di computer californiano di nome Hal Finney ne vide le capacità ed a prendere sul serio Nakamoto. Accettò di lavorare gratuitamente sul progetto Bitcoin e dalla loro collaborazione si arrivò al precedentemente citato lancio della criptovaluta al pubblico.

Negli anni a seguire, sono stati l'informatica e la crittografia le "scienze" maggiormente attratte dal fascino di questa nuova tecnologia, le quali hanno cercato di approfondirne maggiormente lo studio, fino a quando il decollo degli scambi commerciali dei Bitcoin ha catturato l'attenzione di un pubblico più vasto. Infatti, coerentemente con la teoria della curva di adozione dell'innovazione (Curva S) di Everett Rogers, il generale processo di interesse e adozione verso una nuova tecnologia, o meglio innovazione, è caratterizzato da alcuni anni di lenta adozione per poi sfociare in una crescita esponenziale. 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 come rimedio al fenomeno del Double Spending

Nel dizionario Treccani, il concetto di criptovaluta viene così definito [42] :

"*Strumento digitale impiegato per effettuare acquisti e vendite attraverso la crittografia, al fine di rendere sicure le transazioni, verificarle e controllare la creazione di nuova valuta*".

Bitcoin è la prima delle cosiddette criptovalute, monete basate su un'architettura computerizzata decentralizzata. Di fatto, il nome bitcoin indica non solo il nome della valuta di riferimento del sistema, ma è anche di riferimento alla rete ed al protocollo su cui si basa. 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, di cui parleremo più avanti. Ognuna di esse contraddistinta dal proprio protocollo e dalle innumerevoli applicazioni che offrono.

Il corretto funzionamento di queste piattaforme informatiche dipende, come verrà descritto dettagliatamente in seguito, 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* [44] .
Ai fini della definizione, il problema della doppia spesa è 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.
Il double spending è definibile come un difetto in un sistema per criptovalute, il rischio che una valuta digitale, possa essere spesa più di una volta nel mercato digitale in cui si trova, ovvero una transazione utilizza lo stesso input di un'altra transazione già trasmessa in rete [46] .

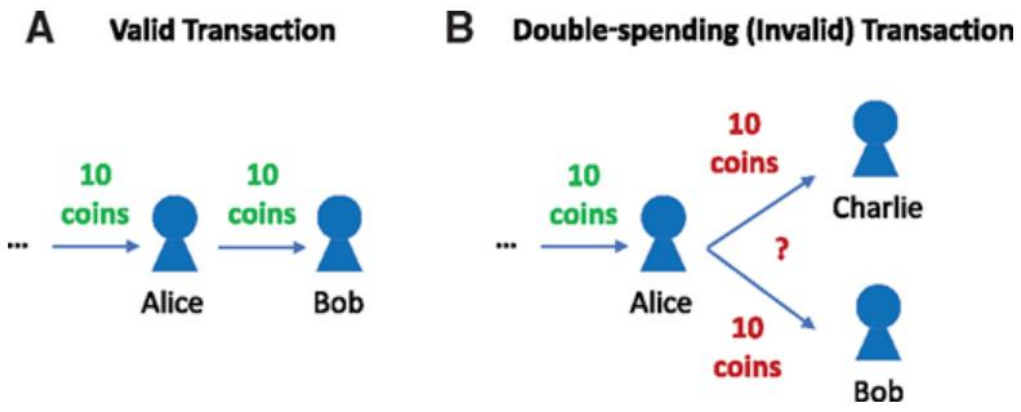

Figura 2. Presentazione grafica di una transazione correttamente eseguita (A) ed un caso di transazione Double Spending (B)

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. 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 e 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. Di seguito esamineremo entrambi i casi, ricordando però che non solo sono inusuali ma anche dalla difficilissima esecuzione e scarse probabilità di successo.

1.2.1 Brute Force Attack

Come detto in precedenza, il responsabile di un Brute Force Attack [47] necessiterà 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% [44] . Tuttavia, se il malintenzionato non riuscisse nell'operazione e l'attacco non andasse a buon fine, i fondi per coprire i costi della transazione vengono prelevati del responsabile ed inviati all'esercente, come fosse avvenuta una normale operazione all'interno della piattaforma.

1.2.2 Il 51% Attack

Il 51% Attack, anche formalmente definito come il Majority Attack. 51% [48] 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 mainers, 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"* (in italiano 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, come altcoins sia una minaccia possibile.

1.3 La crittografia a servizio della Blockchain

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. La crittografia è la disciplina che studia come rendere le informazioni sicure, ossia confidenziali ed integre, prendendo un testo detto in chiaro e trasformandolo in testo cifrato, che risulta incomprensibile a chi non conosce i dettagli della trasformazione [5] . La confidenzialità è un concetto simile alla privacy ma ne rappresenta solo una componente: si riferisce alla capacità di proteggere dati da chi non è autorizzato a leggerli. L'integrità invece si riferisce alla capacità di proteggere dati da modifiche non autorizzate.

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, chiara ed intellegibile. 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.

Tra le molteplici tecnologie relazionate alla blockchain, la crittografia ed i conseguenti algoritmi di consenso sono quelli di maggior rilievo e, sicuramente, sono i mezzi su cui la *distributed ledger* definisce la sua natura *trustless.* 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 [46] .

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 (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 (questo implica un maggiore livello di privacy).
La chiavi private, come dice la parola stessa, vengono condivise esclusivamente con gli utenti di riferimento/proprietari del *wallet digitale*, mentre la chiavi pubbliche, a seconda del protocollo del sistema, potrebbero eventualmente essere condivise anche con gli altri utenti appartenenti alla blockchain.
La chiave pubblica è fondamentale per lo scambio di criptovalute [101] , la chiave privata invece è utilizzata per "firmare" le transazioni, come fosse il mezzo di convalida per le operazioni. Mentre il codice alfanumerico delle chiavi private viene generato in modalità pseudo casuale, la chiave pubblica è data dalla funzione:

$$K = k \times G$$

Dove (k) indica la chiave privata e la chiave pubblica (K) 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 (moltiplicazione), mentre è praticamente impossibile da ricostruire (divisione), pur conoscendone il risultato. Pertanto, anche se qualcuno conoscesse la chiave pubblica (K) e la funzione stessa (G), non avrebbe modo di calcolare la chiave privata (k). Una volta determinata la chiave pubblica, è possibile dedurre l'indirizzo (Bitcoin), fondamentale per effettuare la transazione. In sostanza l'indirizzo (A) viene determinato applicando una funzione di doppio hash alla chiave pubblica (K). Detto semplicemente, 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.

L'hash è prodotto da una funzione aritmetica che prende come input ogni bit (0 o 1) della stringa iniziale e ne modifica totalmente l'output in modo irriconoscibile, anche se un singolo bit viene modificato o aggiunto. Prendendo come esempio, la funzione hash più comunemente utilizzata SHA-256 , e le due stringhe "abcdefghilmno" e "abcdefghilmns", due stringhe che differiscono solo nell'ultima lettera (la lettera "o" sostituita con una "s"), l'output che otterremo potrebbe essere di questo genere:
Per abcdefghilmno → rs10204tr1dfr3456e1e3ppp2784t5rsgt58970f345
Per abcdefghilmns→ yy245hfd4567wqr45t9f096004jf89o1p11r235lx

Mentre le chiavi 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

Nel più semplice dei termini, la parola blockchain significa catena di blocchi o catena bloccata, è un database distribuito decentralizzato che sfruttando la tecnologia *peer-to-peer*, valida le transazioni tra due parti in modo sicuro, verificabile e permanente. Definiamolo come un libro mastro strutturato come una catena di blocchi, contenenti transazioni, correlati 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.

Dalla fusione, per così dire, di queste tre scienze e usando tecnologiche già disponibili, Satoshi Nakamoto ha saputo creare un sistema economico chiuso autogovernato ed essenzialmente nelle mani di nessuno.
È difficile classificare la blockchain con un'unica definizione, di per sé, possiamo dire che il suo scopo sia quello di fornire certezze in quanto tracciabilità e trasparenza, con l'intenzione di aprire a nuove metodologie di storage di dati e transazioni. È una tecnologia di base attraverso la quale è possibile tracciare delle informazioni, tokenizzare dei beni o reperire fondi attraverso i sistemi di crowdfunding digitale. Diverse sono le caratteristiche che contraddistinguono la blockchain [51] :

- decentralizzazione;
- immutabilità;
- sicurezza;
- programmabilità;
- anonimato;
- unanimità;
- time-stamped;

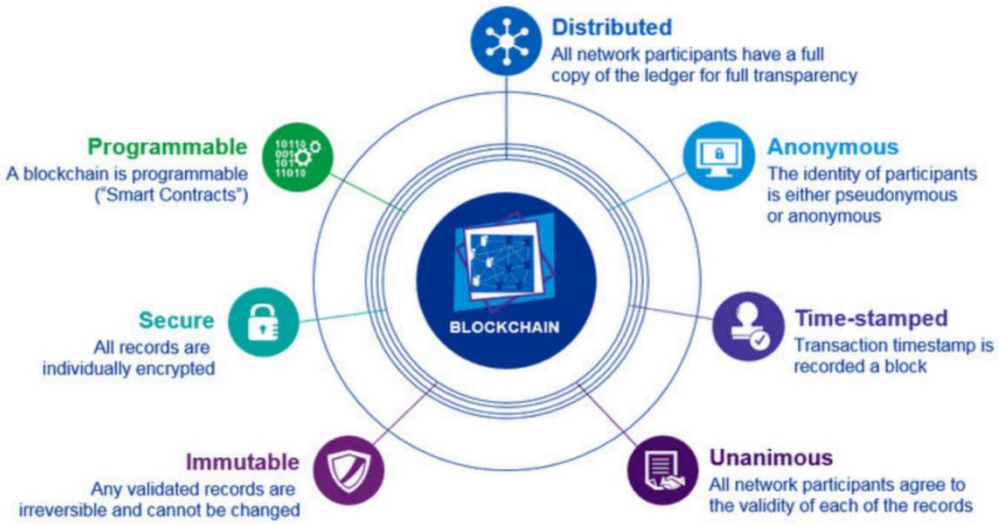

Figura 3. Peculiarità dei sistemi blockchain.

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.

A loro volta i blocchi per entrare a fare parte della catena vengono sottoposti a un processo di validazione che si basa sul principio del consenso distribuito, consenso che rende superflua la figura di un supervisore che ne assicuri la legittimità. Di fatto, 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.

Successivamente andremo ad analizzare le tre caratteristiche che più di altre permettono alla tecnologia blockchain di distinguersi e la porteranno ad essere implementate ed utilizzata su larga scala in futuro.

1.4.1 Decentralizzazione

A differenza dei vecchi registri centralizzati, nella blockchain sono i vari nodi della rete a essere i detentori delle informazioni. 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 potere che li autorizzi e che detenga il monopolio delle transazioni [2] . 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.

Nella blockchain ogni nodo ha una funzione attiva e passiva, è nello stesso tempo creatore e validatore. Ogni utente della catena possiede una propria copia dell'intera documentazione appartenente alla blockchain, non ne esiste una ufficiale e nessun utente è più credibile dell'altro, questo assicura la trasparenza della tecnologia. Ogni transazione è sorvegliata da una relazione di nodi che ne garantiscono la legittimità e la conservazione sin dalla sua nascita, un apparato democratico dove le informazioni sono ugualmente accessibili a tutti ed altrettanto verificabili. Questo è il principio della "fiducia distribuita". La blockchain è un sistema che non necessita di un'autorità centrale, poiché 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. Viene per questo associata spesso al concetto di Distributed Ledger, proprio perché la blockchain si basa sull'idea di fiducia distribuita tra i vari utenti, ed in seguito andremo a definire meglio cosa siano le Distributed Ledger Technology (DLT) e le annesse tecnologie di supporto.

1.4.2 Immutabilità

Accanto alla decentralizzazione, l'immutabilità del dato è un'altra delle caratteristiche peculiari di questa tecnologia. La blockchain è un registro non modificabile. I record memorizzati all'interno dei blocchi, grazie all'uso di crittografie a chiave pubblica, non possono essere alterati o cancellati dai nodi della rete [2] . Invece, come già detto, per 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. Di fatto se si volesse "truccare" una generica blockchain non basta intervenire su un singolo blocco per rendere questa modifica valida, bisogna intervenire su tutti i blocchi di una catena e per farlo si stima che sarebbe necessaria la potenza di un computer 6000 volte più potente dei 500 super computer più veloci al mondo. Questo perché ogni partecipante o nodo è possessore di una copia unica e autentica dello storico di transazioni e servizi avvenuti all'interno del blocco di competenza, sottolineando di nuovo il concetto di trasparenza e fiducia distribuita.

1.4.3 Sicurezza

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'ingresso 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. Questa tecnologia ha il potenziale quindi di effettuare una vera e propria trasformazione degli obsoleti modelli di business fino ad ora utilizzati, velocizzando i processi e riducendo i costi. Basti pensare all'applicazione che può avere nella certificazione dei prodotti agroalimentari o nella verifica della correttezza degli atti all'interno di un sistema politico [2] .

1.5 Componenti della Blockchain

Andiamo ad analizzare meglio alcuni tecnicismi per comprendere meglio il funzionamento di una blockchain. La suddetta tecnologia si compone di [51] :

- Transazioni;
- Nodi;
- Wallet;
- Blocchi;
- Ladger;
- 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 [5] . 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. Mentre la chiave privata è utilizzata per ricevere fondi, identificare l'account degli utenti nel network e può essere tranquillamente condivisa con altri utenti.

1.5.4 Ladger

Il Ledger è un "Libro Mastro" [70] , definibile come una delle basi della nostra civiltà, attraverso cui vengono gestite ed interpretate le relazioni o transazioni tra persone o tra organizzazioni. Si può ricondurne la nascita con quella della scrittura, attraverso cui la società ha iniziato a prender forma lasciando memorie delle proprie azioni ai posteri attraverso registri e archivi. In altre parole, 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 [70] , di per sé, sono il raggruppamento di una serie di transazioni, e solitamente possono contenere fino ad un massimo di 1 MegaByte ciscuno. 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*: la marca temporale, indica la data è 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 [11] . 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.

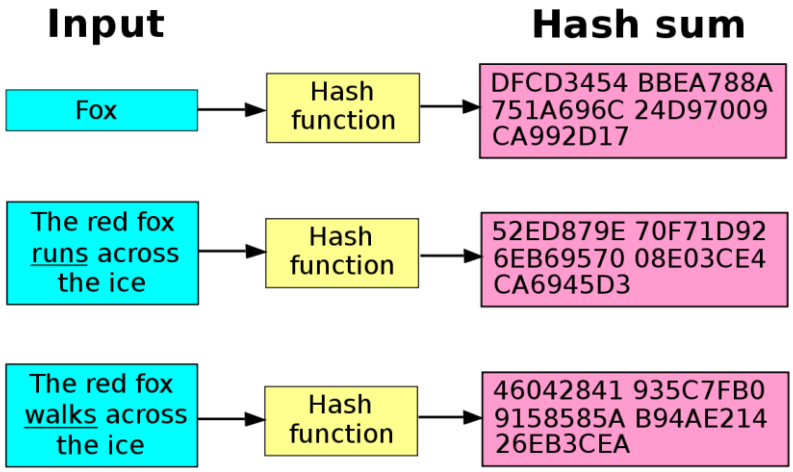

Figura 4. L'immagine presenta la totale trasformazione di un input in un codice alfanumerico hash.

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 [49] [70] 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 a favore 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 approcciare 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 di energetico. Per questo motivo PoW non è considerata una soluzione efficiente nell'ambito imprenditoriale [10] .

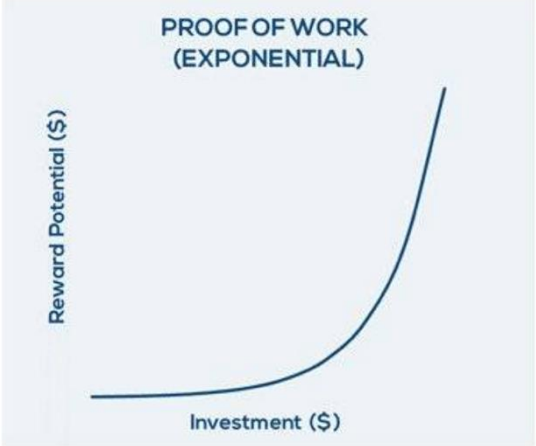

Figura 5. L'andamento della curva presenta i profitti dei miners a fronte dell'investimento fatto in un'operazione di PoW.

I sistemi 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 basano 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

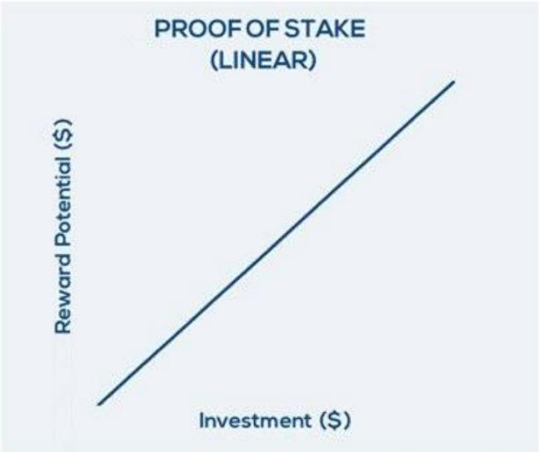

Figura 6. L'andamento della curva presenta i profitti dei miners a fronte dell'investimento fatto in un'operazione di PoS.

detiene, per esempio un ente che detiene l'1% delle criptovalute del sistema avrà la possibilità di estrarre fino all'1% dei blocchi del sistema. 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.

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 Fork [70] 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.

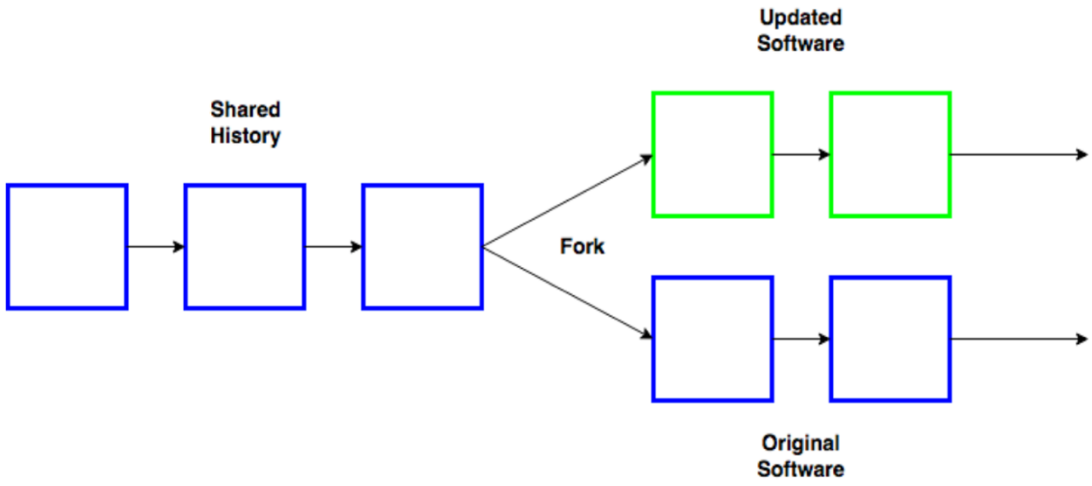

Figura 7. L'immagine presenta la biforcazione di un sistema blockchain ed il proseguimento dei due gruppi in parallelo.

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, sarebbe 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 [51] :

- Centralizzato;
- Decentralizzato;
- Distribuito;

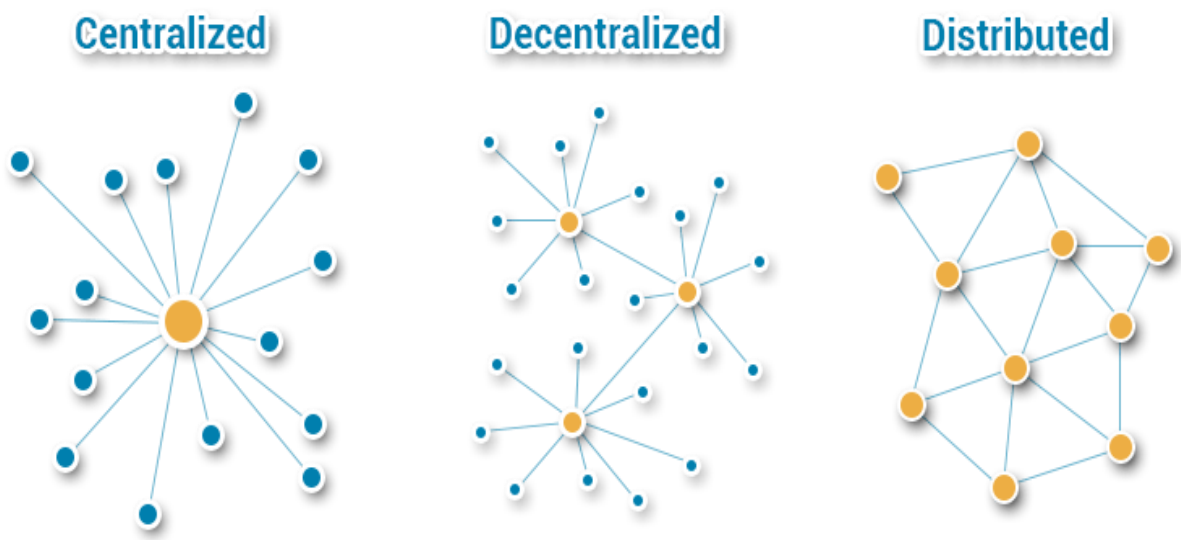

Figura 8. Vengono presentate le tre strutture utilizzate nei più classici sistemi digitali.

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 una 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

D'altro canto, i Decentralized Ledger [41] 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* (abbreviata P2P) 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 ché 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 [43] , 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 senza intoppi.
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.

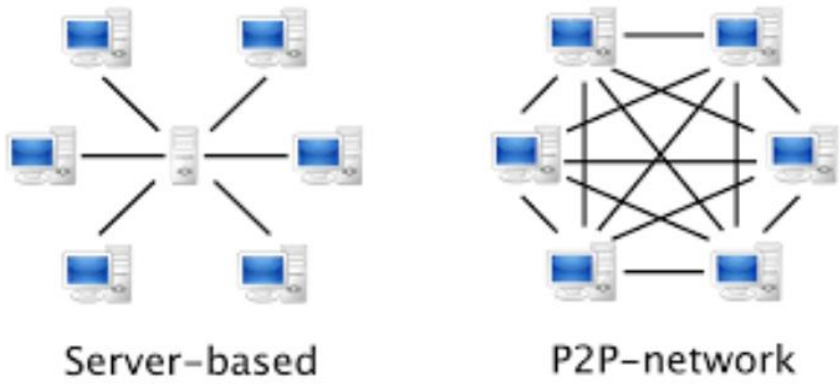

Figura 9. Affiancamento grafico di una classica rete centralizzata ed una rete peer-to-peer.

1.7 Blockchain pubbliche o private

Hai giorni nostri, due sono le tipologie di Blockchain prese in considerazione, la pubblica (*Unpermissioned Ledger*) e la privata (*Permissioned Ledger*) [52] [53] [54] . 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 [4] . Nonostante siano due prodotti con 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 da gli 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 affidando a blockchain pubbliche, sono anche le più popolari ad oggi, Bitcoin ed Ethereum.

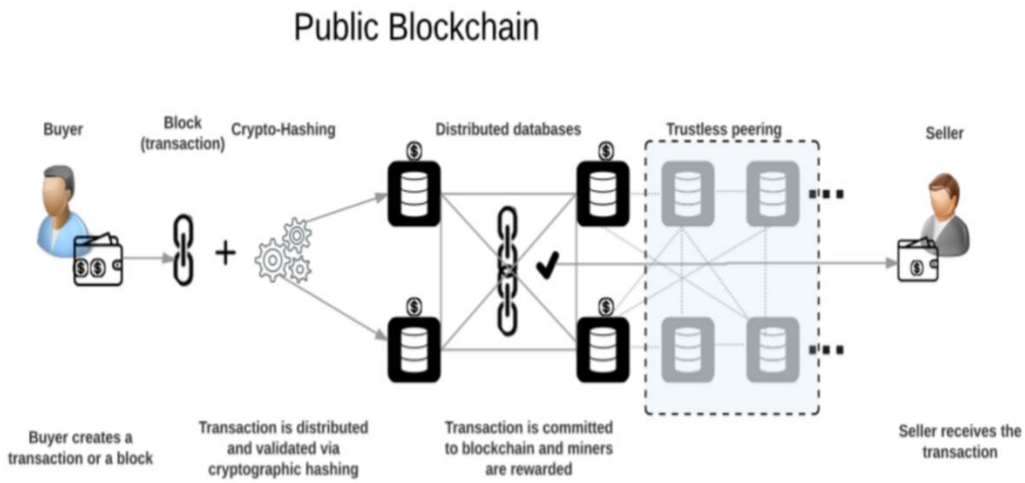

Figura 10. Funzionamento di una Blockchain pubblica.

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 distribuited ledger technology senza rendere pubblici i dati;

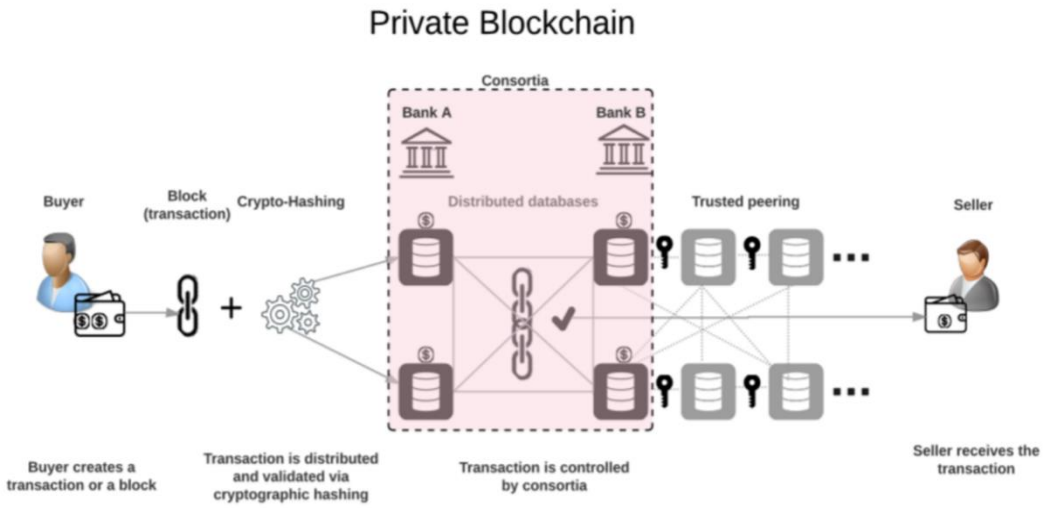

Figura 11. Funzionamento di una Blockchain privata.

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 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 dei proprio business. Per queste ragioni nei prossimi anni, con lo sviluppo di nuove soluzioni tecnologiche, è probabile che queste imprese di rivolgeranno ad una blockchain privata piuttosto che pubblica.

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 da affiancare il primo significato di token a quello delle criptovalute basate su blockchain, dove i token sono semplicemente frazioni di una criptovaluta, per questo motivo è più consono definirle *token coin* (come farò da qui in poi per evitare confusione). 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, a differenza dei sopracitati coins, i token non necessitano di un registro proprio per esistere, ma trovano appoggio su piattaforme come Ethereum mediante gli smart contracts [55] .

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 di fuori del sistema blockchain.

Quindi, un token è definibile come un asset digitale che gli tenti 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;
- permette 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, siccome 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 [6] [57] [58] [59] ad oggi più comuni:

1. Asset Token: rappresentano il diritto di proprietà di un determinato asset materiale o immateriale che sia. Gli asset posso 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: conferisco 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

SMART CONTRACTS

2.1 Nascita degli Smart Contracts

Le teorie alla base di Smart Contracts e blockchain riflette la sorprendente mancanza di fiducia negli esseri umani, specialmente in materie economico giuridiche, poiché, storicamente considerati come intrinsecamente di parte ed inaffidabili. I computer, invece, possono essere considerati come enti più oggettivi, dotati di maggiore infallibilità ed affidabilità. L'idea stessa di contratti intelligenti è quindi indissolubilmente legata all'eliminazione del giudizio umano, alla riduzione della dipendenza dalla finanza, alla riduzione degli intermediari e, in molti casi, un distacco dall'ordinamento giuridico a favore di sistemi informatici dotati di un giudizio oggettivo ed egualitario.

Nel il 1996, un informatico statunitense, di nome Nick Szabo delinea il concetto di Smart Contract, nel White Paper "Smart Contracts: Building Blocks for Digital Free Markets" [36] . Nel primo Smart Contract di Szabo venne teorizzato un primo modello di vending machine, dove il software e l'hardware della macchina distributrice gestivano la vendita di un certo bene. Dove, verificando che al rispettarsi di alcuni dati contrattuali all'interno del softwre, venisse consegnato al cliente il prodotto desiderato. Ciononostante, nel 1994 mancava la tecnologia e la necessità perché gli smart contracts potessero svilupparsi e diventare un mezzo di uso quotidiano [60] .

Tecnicamente lo smart contract è la trasposizione in codice di un contratto che ha la capacità di verificare in forma automatizzata l'avverarsi di determinate condizioni e di eseguire azioni o dare disposizioni in merito. Nello specifico, per smart contract si intende la **"**traduzione" o "trasposizione" in codice di un contratto. Lo scopo è facilitare il controllo sull'avverarsi di determinate condizioni e di auto-eseguire azioni nel momento in cui si raggiungono o si verificano presupposti determinati dalle parti. In altre parole, è basato su un codice che "legge" sia ogni clausola contrattuale sia gli obblighi operativi nelle quali devono verificarsi le condizioni concordate e si esegue automaticamente nel momento in cui c'è concordanza tra i dati riferiti alle situazioni reali e i dati riferiti alle condizioni e alle clausole concordate.

Si presume che gli smart contracts siano i protocolli informatici creati per facilitare, verificare, o far rispettare le negoziazioni o le esecuzioni di un contratto. In origine, erano utilizzati prevalentemente nell'ambito finanziario, non era previsto il loro utilizzo in un più ampio ambito operazionale. Tuttavia, nonostante inizialmente la complessità della tecnologia alla base degli smart cantracts abbia reso difficile valutare le loro effettive capacità e reali potenzialità, l'implacabile crescita tecnologica degli ultimi 30 anni, ha reso, quello che è iniziato come fenomeno di nicchia, in una tecnologia pronta a cambiare l'intero panorama commerciale.

È auspicabile che i contratti intelligenti abbiano le potenzialità per snellire il processo di contrattazione, ridurre notevolmente i costi di transazione eliminando gli intermediari e semplificare l'applicazione delle norme senza dover chiedere ricorso alle istituzioni tradizionali, come tribunali e banche.

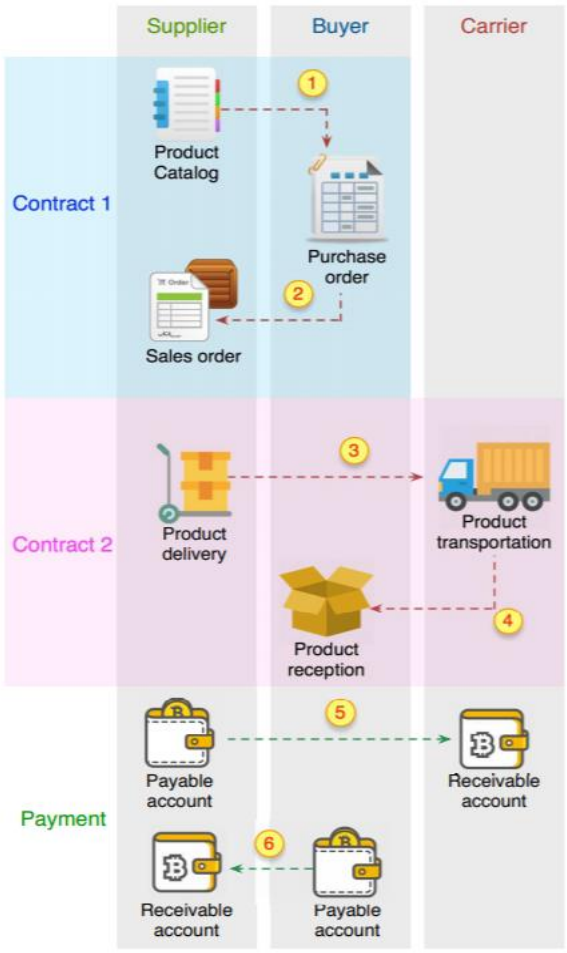

Figura 12. Esempio di utilizzo di uno smart contract tra un acquirente ed un fornitore.

2.2 Relazione tra Smart Contracts e Blockchain

Solo nel 2009, con la nascita del Bitcoin e l'introduzione di un primo prototipo della tecnologia blockchain, gli smart contracts (contratti intelligenti in italiano) trovano spazio tra le tecnologie digitali del nuovo secolo. Anche se teorizzati quasi vent'anni prima, per l'introduzione dei contratti intelligenti nel mondo digitale, all'epoca mancava una tecnologia come la blockchain che rendesse questi contratti sicuri ed affidabili. Questi, possono essere considerati un grande progresso per la tecnologia blockchain, e viceversa. La struttura decentralizzata della blockchain fa da garante, affinché le clausole dei contratti restino invariate, mentre gli smart contracts fanno sì che le condizioni stabilite dalle due parti vengano rispettate [61] . La cooperazione tra queste due tecnologie offre agli utenti, i seguenti vantaggi [62] :

- *Autonomia:* eliminano gli intermediari, lasciando pieno controllo agli utenti che fanno parte della rete;
- *Fiducia*: le informazioni contenute nel ledger condiviso non possono essere né rubate né modificate da malintenzionati. Questo, oltre l'imparzialità dei sistemi digitali, permette di riporre la fiducia degli utenti nella rete stessa;
- *Risparmio*: annullando la necessità di terzi come intermediari per stipulare ed onorare tali contratti, permette di risparmiare nella compensazione di queste figure professionali;
- *Sicurezza*: se correttamente implementata, la crittografia, garantisce l'impossibilità di hackeraggio delle informazioni;
- *Efficienza*: il processamento automatizzato di documenti ed informazioni permette un grande risparmio di tempo rispetto a quello manuale;

I termini e le e condizioni di tali contratti sono trasparenti, ovvero visibili ed accessibili da tutte le parti coinvolte, questo comporta che, una volta firmato digitalmente lo smart contrat, questo diventa esecutivo e non vi è più possibilità di contestarne a livello legale le clausole, esso si occuperà in automatico della fase di monitoraggio per l'adempimento di tali clausole. Un esempio realistico per l'utilizzo di tale tecnologia è legato agli acquisti di servizi multimediali rateizzati. Una volta inserite tutte le informazioni del contratto ed

i dati della transazione nella blockchain, lo smart contract si occuperà delle fasi di verifica in autonomia, controllando ciascuna delle condizioni facenti parte del contratto. Ipotizzando il mancato pagamento di una quota, e quindi un'insolvenza da parte dell'acquirente, il sistema, sempre in autonomia, si preoccuperà di bloccare l'erogazione dei servizi a quest'ultimo.

Pertanto, non è difficile immaginarsi che siano innumerevoli le possibilità di impiego degli smart contracts sulla piattaforma blockchain, e di come, in una visione non troppo futuristica, le realtà professionali che sapranno sviluppare le competenze tecniche necessarie alla creazione degli smart contracts, avranno un grosso vantaggio competitivo sui più comuni mezzi burocratici o legali [2] .

2.3 *Ciclo vita di uno Smart Contract*

Di seguito analizzeremo meglio le fasi di creazione ed applicazione di uno smart contract, distinguendo in 4 fasi l'intero ciclo vita di tale tecnologia [7] , che si suddividono in:

- Creazione;
- Implementazione;
- Esecuzione;
- Completamento;

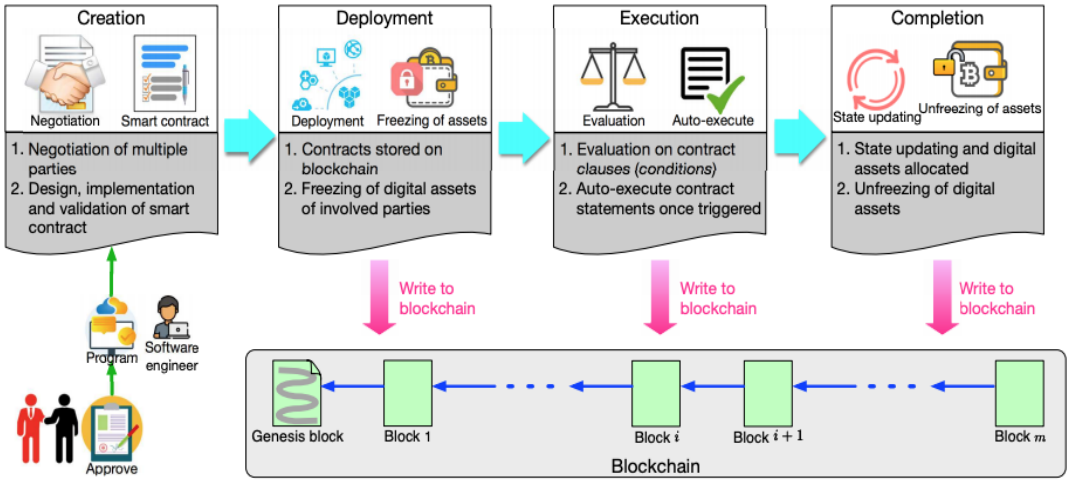

Figura 13. Il ciclo vita di uno Smart Contract.

1. *Creazione dei contratti*: Nella creazione di uno smart contract diverse parti vengono coinvolte, tra utenti, consulenti, avvocati ed ingegneri. In questa prima fase, si affronteranno diversi cicli di contrattazione per il raggiungimento di un accordo che sia adegui alle parti coinvolte. Qui gli avvocati, si occuperanno di redigere un accordo iniziale, dove vengono determinate quali saranno i diritti, gli obblighi ed i divieti che meglio si adeguano alle necessità degli utenti. In seguito, gli ingegneri informatici convertiranno il contratto scritto in forma naturale in uno smart contract, traducendone il contenuto sotto forma di linguaggio informatico

(algoritmo) per il software. Tale procedura prevede una fase di progettazione, una di implementazione ed una di validazione.

2. *Implementazione dei contratti*: Una volta superata la fase di validazione i contratti vengono implementati sulla piattaforma blockchain di riferimento, così da garantirne l'immutabilità e sicurezza. Superata questa fase la consultazione dei contratti avverrà direttamente dalla piattaforma blockchain e le parti, ed i beni di corrispondenza verranno identificati grazie ai loro *wallet* digitali.
3. *Esecuzione dei contratti*: in seguito all'implementazione, si passa ad una fase di monitoraggio e valutazione delle clausole contrattuali. Uno smart contract può essere considerato come una serie di condizioni, a cui, se correttamente rispettate, corrispondono una serie di azioni logiche. Quindi, nel momento in cui una condizione contrattuale viene rispettata, la corrispondente funzione viene eseguita, per poi passare alla validazione della transazione da parte dei miners. Ogni informazione riguardante le transazioni viene memorizzata e custodita nella rete blockchain.
4. *Completamento dei contratti*: Una volta che le condizioni degli smart contracts vengono rispettate, si passa ad una fase di aggiornamento delle rispettive parti interessate. Quindi, le transazioni sono già custodite nella blockchain, bisogna solo aggiornare il passaggio dei beni digitali da un utente all'altro, per esempio il passaggio di criptovalute dal wallet digitale dell'acquirente a quello del fornitore. U na volta avvenuto lo scambio di beni si può dire che la transazione sia terminata e che il ciclo vita dello smart contract di per sé si è concluso, e le informazioni riguardanti la transazione rimangono salavate sulla blockchain.

2.4 Ethereum e gli Smart Contracts

Nel 2013 uno sviluppatore russo appassionato di *cryptocurrency,* di nome Vitalik Buterin, dà vita ad Ethereum [60] . Il progetto parte nel 2015, dopo una fase di crowfunding, a scopo di trovare i fondi per completare Ethereum e renderla pubblica online.
Ethereum è una piattaforma digitale che adotta la tecnologia blockchain introdotta da Bitcoin, e ne espande l'uso per accogliere un'ampia varietà di altre applicazioni, con l'obiettivo di creare un veicolo per applicazioni decentrate e collaborative.
Effettivamente, mette a disposizione dei suoi utenti una serie di operazioni predefinite e standardizzate, nonché permette di crearne di nuove proprie, Ethereum è quindi definibile come una Programmable Blockchain. Più specificatamente, Ethereum mette a disposizione dei suoi utenti le risorse computazionali di cui dispone in cambio di una remunerazione in Ether.

L'Ether (ETH) [72] è fondamentalmente un token, la criptovaluta alla base della rete, che può essere utilizzato per effettuare transazioni sul software, esattamente come per il bitcoin, esiste come parte di un sistema finanziario autonomo peer-to-peer, libero dalla supervisione e dall'intervento del governo. Come per il bitcoin, questa criptovaluta ha visto crescere il suo valore di scambio in un brevissimo lasso di tempo.
Nel gennaio 2016, una unità di ether aveva un valore di circa 1 dollaro americano. A settembre 2017, questo prezzo era salito a 290 dollari ad oggi si aggira intorno ai 600 euro. Quindi, mentre ether si limita ad essere una delle centinaia di valute crittografiche, è anche una delle poche con un significativo e mediamente stabile valore di mercato. Questa moneta virtuale svolge un doppio ruolo nel sistema blockchain di Ethereum: da un lato è la valuta di scambio tra i suoi utenti per effettuare le transazioni, dall'altro funge da moneta per pagare la capacità elaborativa messa a disposizione dal sistema, necessaria per stilare uno smart contract e per usufruire più in generale dei servizi che offre Ethereum.

Tornando alla piattaforma Ethereum [74] [75] , essa nasce come una piattaforma di Distributed Computing open source, nella forma di blockchain pubblica, con lo scopo di mettere a disposizione dei suoi utenti la possibilità di creare, pubblicare e gestire smart

contracts. È definibile come una blockchain programmabile, ovvero, offre ai suoi utenti la possibilità di modificare e riadattare le sue applicazioni in modo da adeguarsi alle differenti necessità degli utenti. Si comporta come un Computing Distiribuito, attraverso il quale è possibile per gli utenti creare diverse tipologie smart contracts, usando Solidity come linguaggio di programmazione. In senso figurato, gli smart contracts sono il modo in cui le cose vengono fatte nell'ecosistema di Ethereum. Quando un'utente della rete vuole portare a termine un compito particolare, una transazione o operazione in Ethereum, avvia uno smart contract con una o più persone. Di fatto Ethereum è definibile come un *Turing complete*, ovvero una macchina in grado di eseguire un qualsiasi programma e processare le relative funzioni di calcolo. Una volta creato lo smart contract, viene caricato e fatto girare sulla Ethereum Virtual Machine (EVM), che è sia il motore che l'ambiente di sviluppo e gestione della piattaforma, rappresenta di fatto l'*ambiente di runtime* per lo sviluppo e la gestione di Smart Contract [8] .

Si deduce che vista la flessiblità che offre Ethereum nella creazione di contratti intelligenti personalizzati, ognuno di essi necessiti una differente capacità computazionale per la sua creazione ed esecuzione, nonché una certa rimunerazione per i miners che la eseguono. Per questo, Ethereum, si avvale dei *Gas* [63] , come unità di misura sulla quantità di sforzo computazionale necessario per eseguire un'operazione. Ogni operazione che prende parte a Ethereum, che siano transazioni o smart contracts, per la sua esecuzione richiede una certa quantità di gas. Il costo totale di una transazione può essere calcolato come [73] :

Limite di Gas × Prezzo del Gas

Dove il limite di gas indica la quantità massima di gas necessaria per generare un blocco ed il prezzo del gas è il costo per unità di gas (in ETH). Ad oggi il tasso di conversione per una unità di gas in ether è di 0,00315628 ETH .

Figura 14. Il grafico presenta l'andamento annuale del valore del Gas rispetto alla criptovaluta Ether.

In sostanza, Ethereum si affida a Gas come sistema di gestione per ridistribuire le risorse in modo adeguato, valutando la potenza computazionale necessaria per ogni operazione richiesta ed ottimizzare le risorse dell'intero sistema.

2.4.1 Il caso DAO

Le DAO [64] [65] nascono nel 2016, come organizzazioni create su Ethereum [2] con lo scopo di raccogliere fondi tramite lo scambio di DAO token ed Ether, e lanciare proposte di progetti imprenditoriali tra la community. In breve tempo DAO ottenne una base di investimento di circa 150 milioni di dollari, dei quali circa la metà vennero rubati a causa di un hackeraggio del sistema. Un hacker scoprì un difetto nel codice dei contratti nel DAO, il che gli permise di rubare buona parte degli Ether investiti al suo interno. Questo specifico evento ha condotto la comunità di Ethereum a dividersi attraverso un fork e la U.S Securities and Exchange Commission (SEC) ad intervenire sulla vicenda. L'istituzione statunitense valutò i DAO token come delle securities, e quindi sotto la giurisdizione della legge federale e dei principi generali rispetto al diritto degli strumenti finanziari. Tale decisione, presa dalla SEC ha fatto da evento scatenante per le successive regolamentazioni prese da altri enti giuridici, evidenziando la necessità di delineare un

quadro giuridico internazionale, volto alla regolamentazione e sicurezza dei nuovi mercati finanziari digitali.

DAO è l'acronimo di Decentralized Autonomous Organization, e può esser considerato come la prima applicazione su larga scala di smart contracts a servizio di una piattaforma programmabile come Ethereum [66] . Definibile come una organizzazione imprenditoriale su blockchain, che opera in modo totalmente autonomo, grazie ai suoi protocolli gestiti da smart contracts. Diversamente dalle imprese tradizionali, basate su strutture centralizzate con pochi utenti al comando, nei sistemi DAO non esiste un sistema gerarchico, questi vengono definiti di forma decentralizzata, attraverso smart contracts che ne determinano i processi, regole e premi tramite clausole. Questo permette di creare imprese virtuali altamente efficienti, sicure ed autonome dove, nel caso si voglia cambiare la direzione strategica, basta modificare il codice sorgente dei contratti.

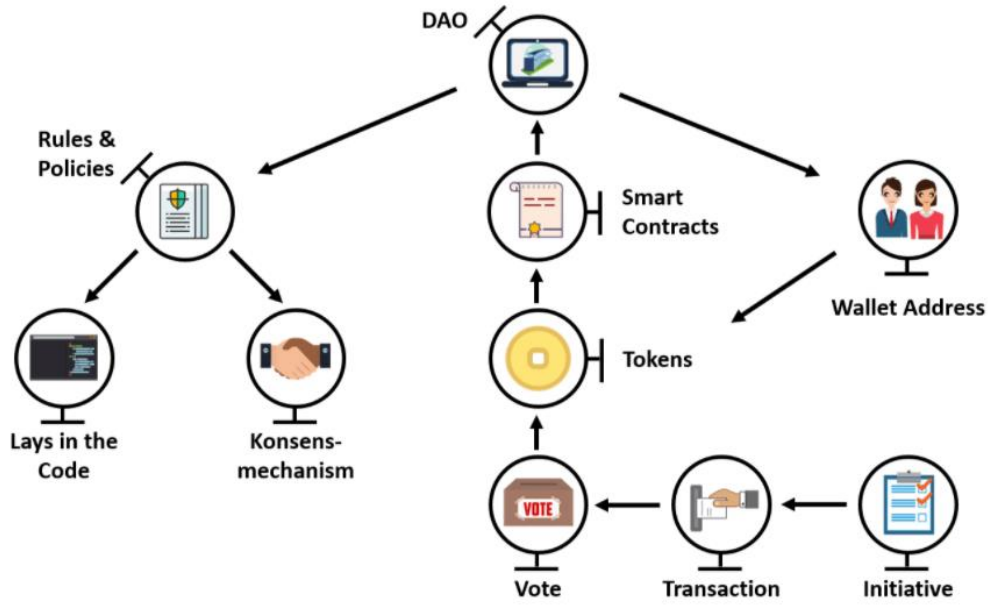

Figura 15. Processo di validazione di un DAO.

L'idea alla base delle DAO è reperire capitali da reinvestire su progetti che vengono valutati da un comitato e poi portati a votazione dagli investitori, i quali possono esprimere il proprio voto a favore o contro una qualsiasi operazione. L'accettazione o meno di una proposta è legata al raggiungimento del 51% dei voti, e va ricordato che

l’influenza di ogni voto è proporzionale al capitale investito in DAO token da ogni utente/investitore, che partecipa all’operazione. La vera sfida nell’implementazione delle DAO è mettere un insieme di regole di consenso efficiente ed automatizzato, che metta d’accordo i suoi partecipanti e risolva i complessi problemi di coordinamento per ottenere investimenti vantaggiosi agli utenti del network.

2.5 Tokenizzazione e Smart Contract

Abbiamo già discusso precedentemente cosa sia un Token ed i suoi diversi utilizzi per i sistemi blockchain, ma ribadendone in breve il concetto, un token è un insieme di informazioni digitali registrate su una blockchain, le quali rappresentano per il suo proprietario un diritto o un valore.

Ne consegue che la tokenizzazione [55] [67] sia la conversione dei diritti di un bene in un token (informazione digitale), dove la corrispondenza di valore tra bene reale e token è collegato e garantito tramite l'utilizzo di uno smart contract. Possiamo quindi dire che la tokenizzazione sia il processo di creazione di un token e di collegamento di questo ad un bene fisico, servizio o evento mediante l'uso di smart contracs [2] . Semplificando, potremmo paragonare un bene tokenizzato ad un puzzle, dove tutti i pezzi possono avere lo stesso valore, oppure ogni singola unità può avere un valore diverso. La frammentazione del valore di un bene porta con sé numerose possibilità, ognuna di queste "quote", grazie agli smart contracts, è caratterizzata da un suo ID che, non solo lo collega alla frazione di bene corrispondente, ma anche al legittimo proprietario. Così facendo, oltre a collegare la quota fisica al token su piattaforma, andrà ad escludere anche la possibilità di censura, interruzioni, frodi o interferenze di terzi. Il procedimento di tokenizzazione prevede la conversione di tutti o parte dei diritti di proprietà su un bene in token, che verranno emessi su piattaforma blockchain per esser scambiati con criptovalute. L'acquirente, comprando tali token, è come se acquistasse delle quote di proprietà del bene in questione, divenendo quindi acquirente non di un bene fisico, ma di un certificato di proprietà digitale. Grazie a blockchain la transazione verrà gestita direttamente dalle parti in causa, che potranno verificare in tempo reale il processo di scambio ed incassare di forma immediata, uno la liquidità, e l'altro i token.

Seppur basandosi su sistemi estremamente complessi, questo genere di attività porta con sé numerosi vantaggi, aprendo le porte a nuove possibilità di investimento in qualsiasi settore, alcuni di essi sono:

- basandosi su un processo democratico, questo genere di distribuzione di valore di un bene permetterebbe ai piccoli investitori di divenire azionistisw o entrare in co-proprietà di averi, che in altri casi gli sarebbero preclusi;

- velocizzazione dei processi di compra vendita ed incassi istantanei;
- sicurezza e trasparenza garantite dai sistemi blockchain;
- il proprietario di una quota, seppur piccola, potrebbe usufruire dei vantaggi collegati al bene di riferimento;
- eliminazione di intermediari per tali operazioni;
- esclusione di mutui o altre fonti di finanziamento per coloro che vogliano entrare in possesso di beni al di sopra delle proprie possibilità economiche;
- creazione di mercati di investimento alla portata di tutti;

Il punto di forza della tokenizzazione risiede nella sua peculiarità di poter frammentare il valore di qualsiasi bene altrimenti indivisibile, o gestire asset ingessati da eccessiva burocrazia. Godendo di tanta flessibilità, permette di digitalizzare qualsiasi bene in totale sicurezza grazie ai token ed alla struttura blockchain su cui lavorano, aprendo ad iniziative commerciali prima impossibili.
È assai verosimile pensare che presto vivremo in un'economia interamente tokenizzata, dove ogni forma di archiviazione di valore e registrazione pubblica diventa un token con un valore di mercato fluttuante e scambiabile globalmente mediante apposite piattaforme digitali.

CAPITOLO 3

AMBITI DI APPLICAZIONE E PRINCIPALI SETTORI

3.1 Ambiti di applicazione

La tecnologia Blockchain ottenne il suo riconoscimento a livello mondiale grazie all'applicazione Bitcoin. Il futuro di tale tecnologia, che possiamo dire si trovi in una fase molto precoce nel mercato, è accompagnato, da una parte, da scetticismo e dall'altra, da uno spirito di svolta. Ad oggi, gran parte dell'entusiasmo, che circonda il tema della blockchain, è determinato principalmente da speculazioni sulle moderne criptovalute. Tuttavia, lo sviluppo delle blockchain, per la sua applicazione in ambito aziendale e pubblico, è ancora molto lontano dalle sue possibili 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, insieme all'utilizzo di smart contracts, 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;

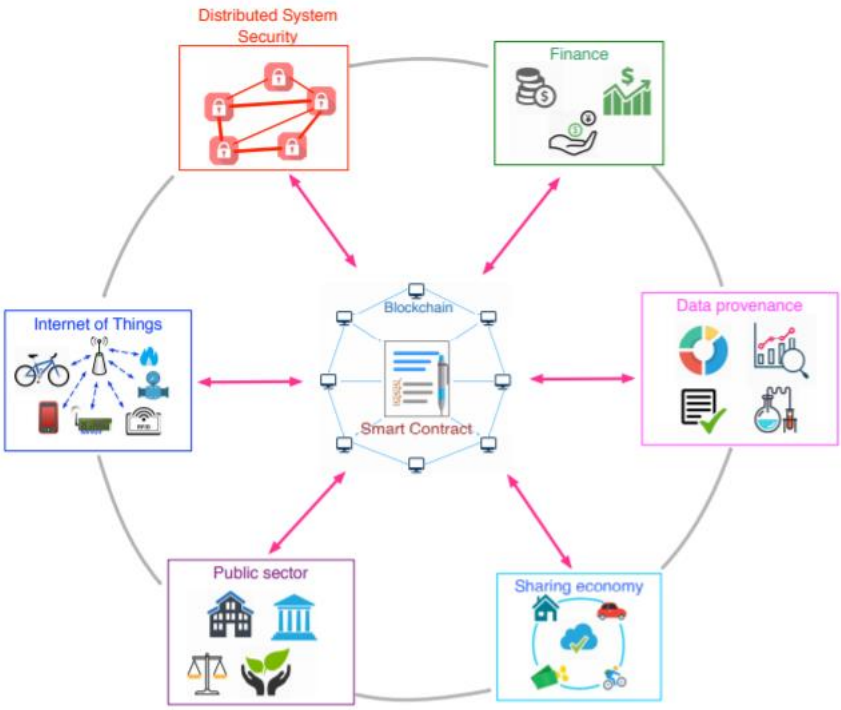

Figura 16. La versatilità del connubio tra Blockchain e Smart Contract.

3.1.1 Finanziario

La nascita del Bitcoin, può essere definito un evento scatenante, se andiamo a vedere l'ingente numero. di criptovalute nate d'allora, ed ognuna distinta da funzionalità proprie. Presumibilmente, dall'introduzione sul mercato del primo Bitcoin e con esso della blockchain come strumento tecnologico, possiamo dire che sia stato il settore finanziario l'area più proattiva nell'introduzione di quest'ultima nei suoi modelli.
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 valora si aggira intorno ai 13.000 dollari per unità. Allo stesso modo, altre criptovalute, con caratteristiche molto differenti, hanno trovato spazio nel mercato ed hanno contribuito al boom di questo settore.

Per esempio, in Inghilterra, la banca Santander, per ottimizzare il processo di pagamenti veloci per i suoi clienti, ha iniziato ad affidarsi a Ripple, che, grazie ai suoi protocolli di pagamento ed al suo network di scambio, consente di effettuare pagamenti ed inviare denaro in tempo reale, senza limiti, e a un costo decisamente ridotto.
Oppure, Fidor Bank, una banca online con sede in Germania, che creando una collaborazione con una società di compra-vendita di valute digitali di nome Karken, nel 2013 è diventata la prima banca a sperimentare le criptovalute e ad offrire il cambio di euro in Bitcoin in Europa. Anche il gigante finanziario Citigroup, nel 2015, dichiarò di esser intenzionato ad implementare la blockchain a supporto dei propri servizi finanziari

Inoltre, l'unione tra blockchain e smart contract ha portato ad un ancor più amplio utilizzo di questi strumenti tecnologici, comprendendo l'elaborazione di "contratti intelligenti", passaggi di proprietà, l'Internet of Things e la *Sharing Economy* (Economia collaborativa).
Oxygen [76] , una società di trade, con sede a Londra, ha annunciato il lancio della prima piattaforma decentralizzata di trading repo per la cripto-economia. Un sistema di riacquisto, che si appoggia smart contract e blockchain per la gestione dei propri contratti di acquisti automatizzati.

Si possono considerare le blockchain e gli smart contracts come dei veri *game changers*, i quali avvalendosi di modelli peer-to-peer e di una collaborazione di massa tra i suoi utenti, permette un'enorme riduzione dei costi di transizione nel suo network, rendendo ridondanti molti sistemi organizzativi esistenti basati su metodi decisionali centralizzati. Non mancano analisti pronti ad affermare che, in futuro, l'impatto della blockchain per il settore finanziario potrebbe essere paragonato ai cambiamenti che vi ha portato internet negli anni 90'.

Peculiarità come anonimato, verificabilità, decentralizzazione e meccanismo di consenso ne hanno permesso la rapida divulgazione nel mondo finanziario ed un sempre crescente interesse da parte di investitori pubblici e privati. Infatti, l'utilizzo della blockchain non si è limitato alle criptovalute, ma ha trovato sempre più utilizzo in vari sistemi finanziari, come in borsa, bonifici internazionali a costi ridotti e identità digitali.

Uno degli esempi più comuni, come è già stato detto, è Ripple, una blockchain basata sul modello dello Shared Decentralized Ledger, utilizzata prevalentemente per scambi interbancari. Come fosse un network globale, attraverso il quale è possibile eseguire trasferimenti di qualsiasi valuta nel mondo in forma economica ed estremamente veloce. In questo tipo di struttura i miners validatori vengono preselezionati e solitamente coincidono con le banche che hanno deciso di utilizzare questo sistema, mentre i blocchi vengono validati da un sistema fondato sul voto. Grazie a Ripple le istituzioni finanziarie possono elaborare i pagamenti dei propri clienti in qualsiasi parte del mondo in maniera economica, istantanea e sicura. Per le transazioni viene utilizzato l'asset digitale XRP, una sorta di sistema valutario privato a cui i partecipanti hanno espresso il loro consenso, e il cui impiego ha lo scopo di semplificare le transazioni, abbassare i costi e velocizzare i tempi di lavorazione.
Nonostante banche ed istituti finanziari siano estremamente lente nell'adozione di queste tecnologie, non vi è dubbio, che i pagamenti in tempo reale siano il futuro per questo genere di transazioni e, di fatto, Ripple si pone l'obbiettivo di andare a sostituire gli odierni, e quasi obsoleti, metodi di invio di denaro SWIFT o Western Union.

Attualmente sono molti gli istituti bancari che hanno iniziato a fare affidamento sulla blockchain per molti dei loro servizi finanziari. 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.

3.1.2 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 grosso cambiamento. Inevitabile che in molti abbiano visto nel connubio tra tecnologia blockchain e smart contract una grossa opportunità per apportare miglioramenti, non solo nella customer experience, ma anche nella fase di gestione di tali polizze. Il mercato delle assicurazioni digitali è proiettato a raggiungere un valore intorno ai 40 miliardi di dollari entro il 2022, per questo si trovano numerose iniziative sulle possibili applicazioni in ambito assicurativo.

A tal proposito sono nate collaborazioni come B3i Services AG, nata nel 2018, un consorzio che comprende 19 delle principali compagnie del marcato assicurativo, tra cui Allianz, Zurich, China Pacific Insurance Company, Aegon, Generali e Mapfre, con l'obbiettivo di creare sistemi assicurativi autonomi, che sfruttano una base di dati estremamente ampia, dedita 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.

In Italia, per esempio, il progetto sviluppato all'interno dell'*Insurance Blockchain Sandbox,* nato dalla collaborazione dell'Università Cattolica e Reply, sotto la

supervisione di Ivass e con il coinvolgimento di colossi delle assicurazione come Mediolanum, Cargeas, Reale Mutua, Ubi Banca, si pone l'obbiettivo di analizzare come la digitalizzazione del mondo assicurativo e la scalabilità intrinseca della blockchain possano accelerare nella diffusione delle istantanee *polizze smart* per apportare una rapida automatizzazione dell'intero settore.
Le sperimentazioni, fin qui, indicano un tempo medio di 6 minuti per sottoscrizione di una polizza smart, a seguito di un alto indice di soddisfazione per i clienti nei confronti dell'intera piattaforma e dei prodotti. 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.

3.1.3 Marketing e Digital Advertising

Una recente pubblicazione *dell'AdAge Marketing Fact Pack 2020* [79] 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. Aumentando la trasparenza all'interno della supply chain dei media, 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.

Basandosi su un distribuited ledger, immutabile e trasparente, la blockchain pare una soluzione naturale per la pubblicità digitale. Le frodi pubblicitarie, l'inefficienza e la mancanza di trasparenza nel settore sono sempre state problematiche da risolvere. Analizzando le aspettative principali nell'adozione della blockchain nell'advertising, a parte i vantaggi generici individuati da una maggiore trasparenza nelle transazioni, nella riduzione degli sprechi e nell'ottimizzazione del fatturato advertising, avrà probabilmente il maggiore impatto sui processi di base del settore, come ad esempio:

- Processi di audit;
- Regolarizzare i pagamenti;
- Gestione delle royalties;
- Mitigazione di frodi;
- Regolazione fiscale;
- Trasparenza finanziaria;

I marketer potranno costruire profili dei propri clienti più affidabili [80] . 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. Queste possibilità sarebbero d'aiuto a migliorare il piano marketing di qualsiasi impresa, nonché un più preciso sistema di targeting e di analisi dei risultati, risolvendo anche il problema della privacy, restituendo la proprietà dei propri dati agli utenti che potranno quindi avere controllo su chi può avere accesso ai loro dati, avendo l'opzione di scegliere con chi condividerli gratuitamente o in cambio di un compenso in criptovalute.
Inutile dire che oltre a migliorare significativamente la gestione del proprio business per le imprese, questo approccio potrà essere usato anche per migliorare sensibilmente l'esperienza del consumatore.

3.1.4 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 [83] .

Il commercio di energia richiede operazioni dove più parti vengono coinvolte, durante una transazione un fornitore potrebbe ritrovarsi ad interagire con banche, borse, broker, agenzie regolatrici e numerose altre controparti [3] . Sulla base della tecnologia blockchain, è possibile semplificare sia i flussi di lavoro interni che i processi con i mercati esterni, che possono cambiare completamente gli accordi di energia.

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"* [14] , ovvero micro-produttori e consumatori di energia. Lo sviluppo tecnologico lascia presumere un aumento nella produzione privati di energia nei prossimi anni, portando nei singoli casi

un eccesso di produzione che se non ridistribuito 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 esuberi e limitare gli sprechi [16] . In parole semplici, significherebbe dare la possibilità ai presumer di vendere ai propri vicini di casa l'energia prodotta in eccesso.

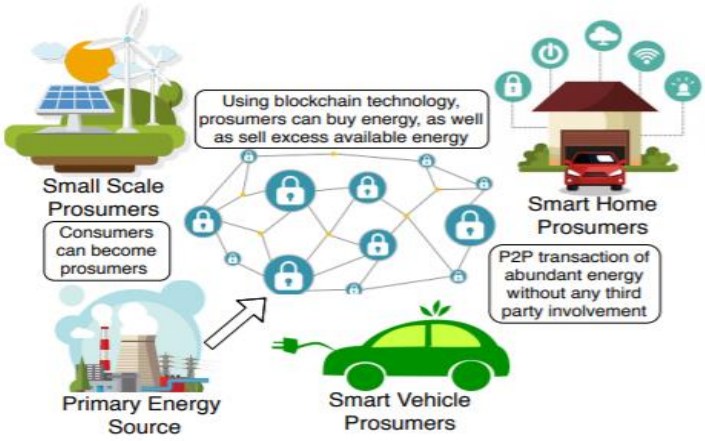

Figura 17. Reti ellettriche supportate da Blockchain.

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. La blockchain svolgerebbe un ruolo centrale in tali operazioni che tramite l'utilizzo di opportuni smart contracts, permetterebbe a due o più utenti di effettuare transazioni di tipo energetico di forma veloce, efficiente e dimensionata alle necessita del caso gestite successivamente di forma automatica, offrendo così i mezzi necessari per ricreare una organizzazione produttiva e distributiva decentralizzata a supporto dei micro-produttori. La stessa decentralizzazione viene rappresentata dalle *Smart Grids*, ovvero un insieme di reti elettriche supportate da dispositivi tecnologici, che grazie allo scambio

reciproco di informazioni, permettono di gestire e monitorare la distribuzione di energia elettrica di forma efficiente tra tutti i suoi utenti. Il concetto di smart grid nasce nel 2006 [14] , ma fino a poco tempo fa la sua applicazione era considerata eccessivamente difficile per mancanza di mezzi tecnologi ed eccessiva complessità operativa. La blockchain riduce questa complessità, permettendo di avere transazioni tra individui e potendo anche garantire affidabilità e trasparenza.
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.

3.1.5 Copyright

Indipendentemente dal settore, il Copyright [82] 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, per qualsivoglia progetto, 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 [17] .
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.

Prendendo foto o immagini online come esempi, le maggiori problematiche per i creatori e detentori di tali contenuti dopo la condivisione online si riassumono nella totale

mancanza di controllo su di essi, ovvero nel non avere la possibilità di tracciare chi fa uso di tale contenuto senza licenza. Simili problematiche non permettono la corretta remunerazione dei possessori dei diritti d'autore, per questo l'utilizzo a scopo commerciali di tali contenuti protetti da copyright senza una licenza solitamente costituisce fare un illecito. Qui è dove la blockchain, insieme agli smart contracts, potrebbe venire in soccorso ai detentori di copyright [3] [12] .

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. Ne è un esempio Binded, la prima piattaforme a protezione dei copyright al mondo, basata su tecnologia blockchain. Qui, una volta caricati i contenuti, viene creato un codice crittografico hash univoco, che permette ai titolari del copyright di controllare digitalmente i propri contenuti ed il loro utilizzo su siti online, comprese le principali piattaforme di social media.

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. Il settore musicale conta circa 1.2 miliardi di streaming giornalieri, questo ne rende difficile se non impossibile il tracciamento, non permettendo una corretta remunerazione per chi ne detiene i diritti d'autore. Il metodo di determinazione dei diritti d'autore nel business della musica è sempre stato un compito complicato, ma con l'ascesa di internet questo processo è diventato ancora più complesso. A fronte di un così amplio volume di transazioni su base giornaliera un registro decentralizzato, sotto forma di libro mastro pubblico, su base crittografica è la soluzione per ricreare un sistema commerciale correttamente regolamentato dove autori di canzoni, artisti, editori, fornitori di servizi di streaming e molti altri soggetti coinvolti del settore vengono correttamente retribuiti.
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. Inoltre, l'utilizzo di smart contracts permetterebbe la ripartizione delle royalties per ogni opera musicale, una distribuzione

equa dei copyrights sul prodotto garantirebbe una più giusta ripartizione dei profitti ed eliminerebbe l'intermediazione dell'industria, permettendo agli artisti di creare e catturare più valore dalle loro tracce musicali.

A questo scopo nascono piattaforme come Musicoin [18] [84] [85] , basata su una piattaforma decentralizzata che combina una rete di condivisione di file peer-to-peer per lo streaming musicale su blockchain, con lo scopo di gestire il tracciamento dei file multimediali sovrascritti e permettere di compensare in modo equo musicisti, miners e sviluppatori. Musicoin nasce da un fork sulla piattaforma Ethereum, dove vengono usati smart contracts per concedere le licenze sui contenuti condivisi nei suoi database ed attraverso la valuta Musicoin ($ Music) vengono effettuati i pagamenti automatici delle royalties ai detentori dei diritti d'autore. Questa metodologia di pagamento è sempre basata sul sistema Pay-per-Play (PPP) [92] , quindi per ogni ascolto di una traccia il detentore dei copyrights viene remunerato di 1 $ Music, trasferito dall'account dell'ascoltatore a quello dei vari beneficiari secondo le percentuali prestabilite tra band, coristi, tecnici del suono e miners. Per creare un ambiente di remunerazione equo all'interno della piattaforma, Musicoin, ha creato un modello chiamato Universal Basic Income (UBI), con lo scopo di garantire una compensazione equa per ogni partecipante seguendo una proporzione delle shares basata sul contributo dato. L'UBI pool, è come fosse una cassa comune di raccolta dei $ Music, alimentata per lo più dai miners, che attraverso le azioni di verifica e creazione di blocchi vengono ricompensati in Token di $ Music.

3.2 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 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 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;

3.2.1 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. 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. Gli inadeguati servizi di condivisone di informazione ad oggi non solo limitano il lavoro dei medici, ma anche la qualità della ricerca scientifica, così come ritardi nella lotta a malattie rare o pandemia. Va ricordato che nel settore sanitario vengono generati ogni giorno grandi volumi di dati sensibili per la salute pubblica, l'assenza di un registro unico nazionale delle cartelle cliniche dei cittadini comporta una mancanza di informazioni importante per i medici o per la ricerca scientifica, impossibilitati di svolgere al meglio il proprio lavoro.

Le applicazioni della blockchain per la sanità può ridefinire ed essere di supporto a sei operatori del settore [19] [20] [86] [87] :

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 uno 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'obbiettivo di risolvere numerose problematiche di auditing fornendo nuove opportunità per la gestione dei dati sia per il personale sanitario che per i pazienti. L'architettura peer-to-peer utilizzata nelle blockchain consente di sincronizzare le cartelle cliniche e dare vita ad un registro unico di dati sanitari, promettendo sicurezza ed immutabilità, dando accesso ad ogni nodo autorizzato del network nel rispetto della privacy dei pazienti. Semplificando quindi la condivisione dei dati ed offrendo maggiore accessibilità e trasparenza agli utenti registrati.

3.2.2 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 [7] .

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, per garantire ciò, limitare l'accesso ai dati solo a determinati individui 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'obbiettivo principale della protezione dei dati e comprendere come inserirlo nel contesto politico in cui si trova il paese di riferimento. Nel contesto democratico in cui si trovano i paesi più sviluppati, è la trasparenza ad avere la precedenza sulla riservatezza. Garantire trasparenza e riservatezza in un sistema blockchain comporta numerose difficoltà computazionali dovendo ricreare protocolli di sicurezza estremamente complessi.

Prendiamo come esempio l'Estonia come termine applicativo e comprendere meglio i frutti che può portare l'utilizzo della blockchain in uno stato di e-governance. Prima di tutto bisogna sapere che l'Estonia e leader nello sviluppo di sistemi di e-governance su scala globale, di fatto il paese sta vivendo in uno status di trasformazione digitale da circa vent'anni. L'obbiettivo del paese è di migliorare il benessere generale dei cittadini e dell'economia del paese promuovendo un apparato governativo più efficiente e trasparente basato su politiche a sostegno del digitale e burocraticamente più agevoli.
Per farlo il governo estone si è affidato ad una piattaforma chiamata *KSI Blockchain (Keyless Signature Infrastracture),* sistema fornitogli dalla compagnia Guardtime [89] , ed integrato in numerosi registri governativi.
KSI è stata concepita come una piattaforma blockchain volta alla totale protezione del network e dei dati estoni, ed alla individuazione di qualsiasi modifica, che venga fatta dall'interno o da un attacco esterno al sistema. Quando un documento viene scritto nel database, solo il suo valore hash viene inviato a KSI Blockchain, l'informazione originale non lascia mai il server. Questo aiuta a garantire la riservatezza dei dati, consentendo al contempo all'autorità di tracciare e rintracciare qualsiasi modifica dei dati sul sistema.

Si può capire perché il governo estone utilizzi piattaforme blockchain a protezione dei dati digitali del paese. 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.
Visto l'incredibile successo ottenuto tra la popolazione estone, oggi altri paesi come Cina, Stati Uniti, Giappone, Inghilterra e Svizzera sono in fase di sviluppo ed implementazione di sistemi blockchain come soluzione all'e-governance.

3.2.3 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 [91] , 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 risoltati elettorali. Prima di un'elezione, le opinioni politiche degli elettori possono essere plasmate dai media a cui siamo costantemente esposti. Campagne di disinformazione mirate posso 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.

Nonostante ci siano tutt'ora degli scettici, in molti sostengono che la risposta alle problematiche di voto elettronico trovino soluzione nei sistemi blockchain. Per questo motivo la società statunitense CBInsights ha sviluppato una ricerca volta a delucidare in che mondo le piattaforme blockchain potrebbero fronteggiare correttamente le problematiche di sicurezza legate all'e-voting, elencando in 3 punti le migliorie che apporterebbe all'intero sistema [90] :

1. **Tecniche crittografiche per la verifica delle fonti**. La crittografia può essere utilizzata come strumento di filtraggio delle fonti, gestendo così l'influenza mediatica a cui ogni utente e soggetto. In sostanza, verrebbero forniti agli elettori esclusivamente articoli contrassegnati da un identificatore crittografico, che permette di dimostrarne la fonte e quindi l'attendibilità.

2. **Identità digitali.** La gestione di elezioni con sistemi blockchain richiederebbe un assortimento di dati di ogni singolo individuo intento a votare. ID emessi dal governo e dati biometrici raccolti in fase di registrazione online verrebbero utilizzati per dimostrare l'identità degli elettori.

3. **Audit post-elettorali.** Utilizzando una blockchain pubblica ogni elettore avrebbe la possibilità di controllare ogni scheda elettorale e confermare quindi l'accuratezza dei dati riportati. Ad oggi, sistemi di voto come Votem e Voatz basati su blockchain offrono agli elettori di verificare i propri voti attraverso codici QR legati ai singoli cittadini, assicurandosi così che il loro voto venga registrato correttamente.

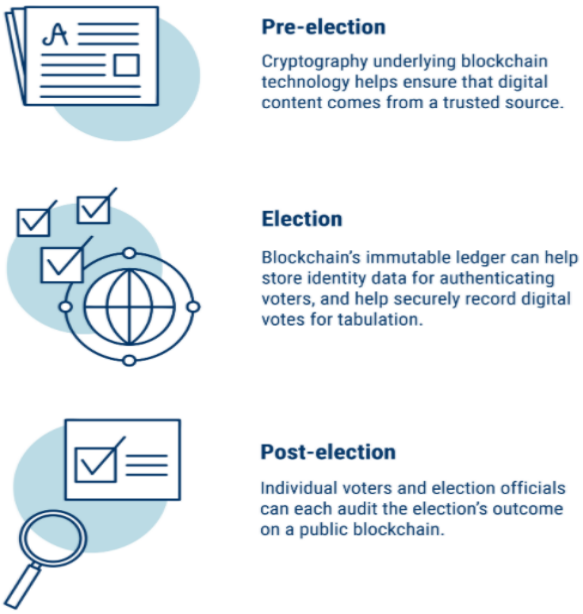

Figura 18. Le tre fasi d'intervento.

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. È certo però, che questa tecnologia ponga delle buone basi per un cambio radicale nel modello elettorale di molti paesi, infatti come l'Estonia altri paesi stanno studiando come implementare la blockchain a supporto dei propri sistemi elettorali [88] .

3.2.4 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 [22] . Ciò è dovuto alle opportunità di mitigazione nel numero di frodi e di errori grazie all'unione tra blockchain e smart contract.

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 soldi delle imposte 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 [22] . In molti paesi l'evoluzione tecnologica ha portato il settore pubblico a dover individuare nuove modalità di riscossione delle imposte dai suoi cittadini. Un'applicazione della blockchain che promette di trasformare il business sono gli smart contracts programmabili, i quali permettono l'auto-esecuzione delle clausole contrattuali dei documenti. Queste tecnologie potrebbero veramente riorganizzare fortemente la contabilità ed il funzionamento dell'intero sistema fiscale. Troviamo già degli esempi negli Emirati Arabi o nel Regno Unito, entrambi pianificano di implementare un sistema fiscale digitalizzato in pochi anni [21] .

Prevedendo alcune applicazioni future sulla riscossione delle tasse, potremmo immaginare uno scenario dove il pagamento e la gestione degli stipendi di ogni impiegato siano controllati da uno smart contract. Quindi gestiti da clausole dettate dai contratti i quali potrebbero estrarre dal salario le tasse e farsi carico della gestione burocratica senza errori in totale autonomia, riducendo ampliamente gli oneri e le tempistiche che queste pratiche prendono al cittadino. Inoltre, ogni informazione verrebbe registrata di forma permanente su blockchain, creando così una fonte affidabile, indiscutibile e dal facile accesso su cui le autorità possono fare affidamento.

I cittadini invece, grazie alla crittografia legata ad ogni transazione, accedendo alla blockchain di riferimento avrebbero la possibilità di vedere dove andranno ridistribuiti ed usati i soldi delle proprie tasse, massimizzando così la trasparenza dell'intero sistema statale.

CAPITOLO 4

BLOCKCHAIN PER IL SUPPLY CHAIN MANAGEMENT

4.1 Cenni storici sulla logistica

Per comprendere meglio il concetto di logistica ed i possibili sviluppi che potrebbe intraprendere tale disciplina in futuro, è opportuno fare una breve introduzione all'evoluzione storica che ha subito dall'origini fino agli ultimi anni.

La base dei sistemi logistici odierni può esser stimata addirittura ai tempi delle guerre romane, quando per far fronte alla costante espansione dell'Impero Romano nel bacino del Mediterraneo, gli ufficiali militari dovettero trovare soluzioni efficaci volte ad operazioni di rifornimento per le proprie legioni. Di pari passo all'espansione dei territori romani, gli ufficiali romani, chiamati anche "Logistikas", dovettero reiventare i sistemi d'allocazione ed approvvigionamento delle loro legioni, dovendo marciare velocemente e sempre più lontano.

Possiamo dedurne che la logistica nasce come una disciplina militare, e fin dai suoi inizi il concetto di logistica poteva essere affiancato al concetto di organizzazione, coordinamento e gestione delle risorse allo scopo di ottenerne la massima efficienza. Negli anni, tale disciplina ha saputo evolversi costantemente ed ha apportato grossissimi vantaggi competitivi a chi fosse stato in grado di applicarne correttamente i metodi, ciononostante la logistica non ha saputo discostarsi dagli scopi militari fino alla seconda metà del 900'. Di fatto prima degli anni 50' del secolo passato, la logistica era considerata esclusivamente in termini militari, basata su complesse sfide in termini gestionali sull'approvvigionamento, manutenzione e trasporti di strutture militari, materiali e personale [25] .

Negli anni a seguire della seconda guerra mondiale tali abilità organizzative del concetto logistico vennero riportate nel settore economico-industriale. Alcune figure imprenditoriali iniziarono ad affiancare i costi dei trasporti a quelli di stoccaggio, ed a discutere dei vantaggi derivanti dall'avere le materie giuste, nel posto giusto al momento giusto. Nel ventennio successivo alla grande guerra la logistica si limitava alla

distribuzione del prodotto finito, generalmente, con il ruolo di supportare attività legata all'organizzazione dei magazzini e dei trasporti.
Fu intorno alla metta degli anni 70' che si incominciò a riscontrare una prima evoluzione logistica, passando da ruolo marginale ad un insieme strutturato di attività volto all'ottimizzazione dell'intero ciclo distributivo, dal magazzino al cliente finale. Nei successivi anni ottanta si assiste, per così dire, ad una piccola rivoluzione grazie all'introduzione di nuove logiche gestionali nelle imprese, come il *Just in Time* (JIT) o il *Material Requirenments Planning* (MRP).

Il Just in Time (in italiano Giusto in Tempo) è una politica di gestione introdotta dalla Toyota Production System nei propri sistemi di fabbricazione a fine anni 50' ed esportata in tutto il mondo. Tale metodo si fonda sull'idea di dover produrre esclusivamente ciò che è necessario per soddisfare la domanda, evitando sovrapproduzione e quindi sprechi. Più che altro si è capito che un corretto flusso di materiali a magazzino e l'ottimizzazione dei processi all'interno della catena produttiva possa portare ad una consistente riduzione dei costi legati alla produzione.

Sempre in questi anni viene introdotto il Materials Requirements Planning, che sta per pianificazione dei fabbisogni di materiali, è una tecnica che tiene conto delle giacenze a magazzino, della domanda di marcato e dei lead time produttivi e d'acquisto e permette di calcolare i fabbisogni netti dell'impresa pianificando ordini di produzione e d'acquisto garantendo il corretto coordinamento dei flussi di materiali e la minimizzazione delle scorte. Offrendo la possibilità di passare da:

- una strategia produttiva *Push*, dove la gestione dei processi produttivi è basata sulla previsione della domanda e quindi sull'accumulo di prodotti finiti a magazzino per poi pensare alla vendita (*Make to Stock*);
- ad una logica *Pull,* dove la produzione del prodotto finito è molto rapida il che permette di produrre esclusivamente ciò che è già stato venduto/ordinato (*Make to Order*) evitando costi di stoccaggio;

L'attenzione aziendale riposta nella gestione dei materiali all'interno del settore industriale, porta alla coniazione dell'espressione "logistica dei materiali". Terminologia

usata per indicare tutte le attività d'approvvigionamento, movimentazione e gestione dei materiali volte a garantire il corretto e provvidenziale rifornimento per supportare le attività produttive ed aziendali.

Giungendo alla fine degli anni ottanta si arriva ad un radicale cambiamento nell'interpretazione di logistica, che da insieme di attività operative viene riconsiderata come un sistema inter-funzionale, che integrato tra gli attori della supply chain, si pone l'obbiettivo di raggiungere elevati livelli prestazionali volti ad una miglior organizzazione delle risorse aziendali con lo scopo di ottimizzare l'efficienza e l'efficacia dell'intero sistema. Passando da una concetto di gestione della logistica aziendale ad un concetto di logistica integrata, definito dal Council of Logistics Management:come segue:

"Il processo di pianificazione, implementazione e controllo dell'efficiente ed efficace flusso e stoccaggio di materie prime, semilavorati e prodotti finiti e delle relative informazioni dal punto di origine al punto di consumo con lo scopo di soddisfare le esigenze dei clienti"

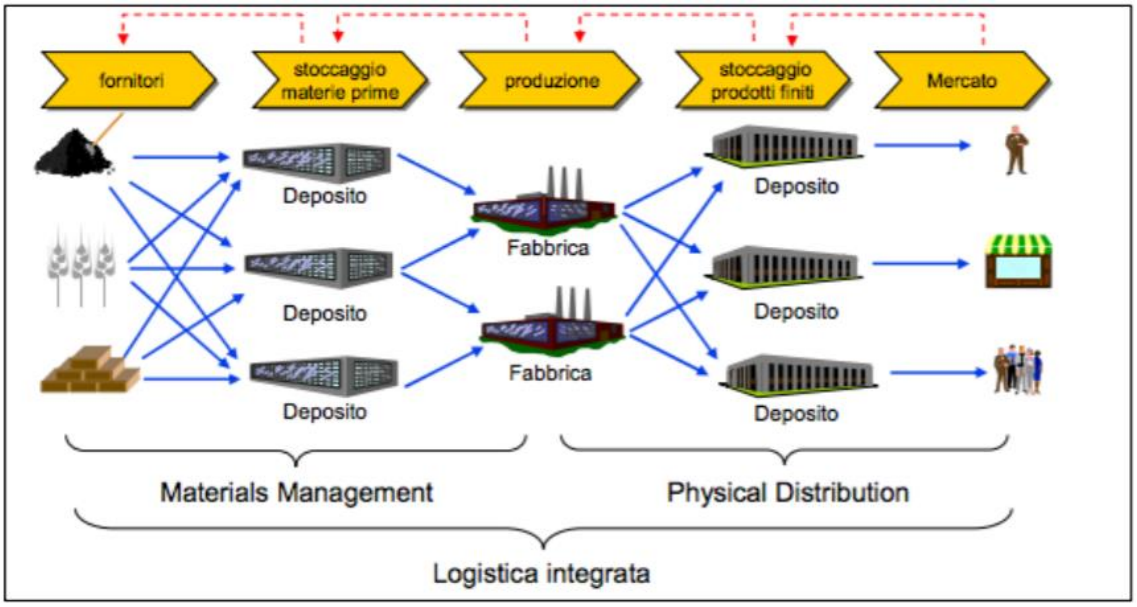

Figura 19. Flusso dei materiali attraverso un sistema logistico integrato.

La definizione soprastante ci permette di intuire che la logistica integrata non si limita all'esclusiva gestione del flusso fisico della catena, ma inizia ad affiancarsi il concetto di

flusso informativo, volto alla gestione dei dati raccolti sui diversi livelli aziendali al fine di elaborare previsioni sulla domanda futura ed ottenere una solida pianificazione di ordini e produzione. Da qui in poi, la logistica non viene più considerata come un'attività autonoma e distacca all'interno dell'impresa, ma parte integrante di essa, che necessita di collaborazione su più livelli aziendali per permettere la corretta gestione dei flussi interni così da generare un vantaggio competitivo per il conseguimento degli obbiettivi da essa prestabiliti.

La somma di questi eventi che si sono susseguiti negli anni hanno portato le imprese a dover operare nel contesto competitivo attuale, estremamente influenzato dalla globalizzazione, che ha portato con sé ad un grande ampliamento del mercato in cui le imprese operano, una maggiore incertezza della domanda e ad un profondo cambiamento nella logistica imprenditoriale, che ha dovuto man mano adattarsi.
A questo va sommata l'innovazione tecnologica ed informatica, che oltre ad introdurre nuovi mezzi di comunicazione ne ha anche abbattuto i costi, rendendo la transazione di dati praticamente istantanea, cambiando drasticamente il modo di fare impresa e l'approccio di questa alla logistica. Il ché porta all'ultimo stadio del processo evolutivo della disciplina logistica, il Supply Chain Management (SCM), dove le aziende prendono coscienza di come il miglioramento della logistica e dei flussi produttivi interni siano strettamente interdipendenti con gli attori esterni. Ovvero, la logistica non può prescindere dalla considerazione e dal coinvolgimento attivo di fornitori e clienti, oltre a saper mantenere i rapporti con entrambi se vuole apportare valore su tutta la catena produttiva. Più specificatamente, la supply chain è un insieme di approcci utilizzati per integrare in modo efficiente fornitori, produttori, distributori, clienti e punti vendita, in modo che la merce venga prodotta e distribuita in giuste quantità, nel posto giusto ed al momento giusto, con l'obbiettivo di minimizzare i costi su tutta la catena e contemporaneamente aumentare il valore per il cliente.
Spesso i termini "logistica" e "supply chain" vengono utilizzati come sinonimi o considerati l'uno la sottocategoria dell'altra, mentre effettivamente sono due aree distinte ed ognuna coinvolge processi, ruoli e responsabilità specifiche. Di fatto la logistica può esser considerato uno degli attori principali all'interno della supply chain, che però coinvolge aspetti e processi più ampli e complessi.

Il supply chain management si ritaglia un ruolo centrale per le aziende, la quale ormai riconosce il suo successo non solo dalle capacità interne, ma anche dalle proprie capacità di cooperare con gli attori della catena con cui collabora. Il supply chain management non è un sinonimo di logistica integrata, ma un approccio in cui l'azienda è parte di una rete di entità organizzative che integrano i propri processi per fornire prodotti, servizi e informazioni che aumentano il valore per il cliente.

Il percorso evolutivo della logistica l'ha portata dall'essere una attività di sussidio a ricoprire un ruolo strategico nel core business aziendale per il suo successo, permettendo a queste di adattarsi ai numerosi cambiamenti di mercato avvenuti negli anni, grazie ad una maggiore flessibilità nella struttura produttiva e ad una minimizzazione di sprechi e costi. Più avanti andremo ad approfondire il concetto di supply chain (management), analizzandone le caratteristiche e funzionamenti.

4.2 Supply chain Management

Trattandosi di un sempre più ampio insieme di metodologie, relativamente recenti ed in costante cambiamento per soddisfare le esigenze crescenti della catena d'approvvigionamento a livello globale, non si è ancora data una definizione univoca di Supply Chain Management per tutti. Tuttavia, per metter chiarezza, ci possiamo affidare alla definizione data dal *"The Council of Supply Chain Management Professionals"* (CSCMP) [93] nel 2007:

"Il Supply Chain Management è quella disciplina che comprende la pianificazione e la gestione di tutte le attività coinvolte nella ricerca, nella fornitura, nella conversione e nella gestione delle attività logistiche. Include, inoltre, la coordinazione, l'integrazione e la collaborazione con i partner della supply chain, che possono essere fornitori, intermediari, fornitori di servizi, e clienti. In sostanza, la SCM integra e coordina la supply chain e la gestione dei rapporti tra i vari attori della supply chain stessa".

Fondato nel 1963, il CSCMP è un'associazione di livello globale, conta circa 9000 membri esperti del settore di supply chain e si dedica al progresso ed alla diffusione delle conoscenze e delle innovazioni di tale settore.

Come precedentemente sottolineato, l'ambito di interesse strategico della catena di distribuzione e cambiato negli anni. Precedentemente le aziende si concentravano maggiormente sui funzionamenti imprenditoriali interni, in modo di agire sul mercato come un'entità a sestante, evitando interazione sostanziali con le altre entità del mercato. In seguito all'avvento capillare di internet ed il conseguente ampliamento di mercato si è dovuto sviluppare un'interconnessione imprenditoriale tra tutte le attività appartenenti al processo di distribuzione e logistica, per la realizzazione di un prodotto finale coerente con la domanda che è venuta a crearsi.
Nello specifico, la supply chain ad oggi conta nove attività principali che, solitamente, si svolgono in questo preciso ordine [25] :

- Marketing;
- Rapporti con i fornitori;

- Approvvigionamenti;
- Gestione e stoccaggio delle scorte di materie prime;
- Produzione;
- Gestione e stoccaggio di prodotti finiti;
- Gestione degli ordini di acquisto;
- Gestione delle consegne;
- Logistica di restituzione e resi;

Lo scopo principale della supply chain è avere il controllo delle prestazioni di ogni operazione e migliorarne l'efficienza con l'obbiettivo di ottimizzare il livello di servizio offerto al cliente finale, cercando in parallelo di ridurre i costi operativi e limitare il capitale di investimento. In breve, lo scopo di tale disciplina si può riassumere in operazioni che ti portano ad ottenere il massimo con il minimo impiego di risorse possibile.

Una supply chain efficiente e ben organizzata comporta un grande vantaggio competitivo, in quanto permette di ottimizzare le risorse a disposizione, evitare gli sprechi, offrire prodotti ad un prezzo più competitivo ed essere più veloci ad entrare nel mercato ed a soddisfare le richieste dei clienti. Ad oggi, è divenuta una attività fondamentale per l'aumento della propria competitività e differenziazione sul mercato, questo anche grazie all'avvento di internet ed il supporto delle *Tecnologie dell'Informazione e della Comunicazione* (ICT) che hanno semplificando e velocizzato la coordinazione, comunicazione ed integrazione di informazioni tra i membri che operano lungo tutta la supply chain. L'immediatezza nello scambio di dati ed informazioni ha cambiato radicalmente il servizio offerto al cliente, permettendo alle aziende di comprender meglio le esigenze dei consumatori ed avere quindi una precisa previsione della domanda.
La pianificazione puntuale della domanda a livello aziendale si traduce in:

- piani d'azione più precisi ed attendibili;
- riduzione nel numero di resi e quindi nei costi aggiuntivi;
- ottimizzazione nell'utilizzo di risorse;
- previsione della capacità produttiva in un dato periodo;
- pianificare la fornitura di materie prime a magazzino;

- riduzione negli sprechi;

Il settore del Supply Chain Management ormai è enorme e si può dire essere lo scheletro di ogni struttura industriale. Tuttavia, gli odierni sistemi di supply chain tradizionali non sono abbastanza versatili e trasparenti per fronteggiare le crescenti esigenze del mercato dei prossimi anni, né le conseguenti spese in termini di gestione degli errori, costi, amministrazione e gestione delle frodi.

4.3 Digitalizzazione a favore di tracciabilità e trasparenza

Negli ultimi anni il crescente interesse dei clienti nel conoscere la provenienza di un prodotto ha di fatto portato la trasparenza ad acquisire sempre più importanza per le supply chain. Di conseguenza, l'Unione Europea ha introdotto e continua ad introdurre nuove norme legislative per favorire l'adozione di processi che permettano di migliorare la tracciabilità e trasparenza dei prodotti. Da evidenziare come tracciabilità e trasparenza siano dei mezzi estremamente efficaci per costruire un rapporto fiducia con i propri consumatori, che usufruendo di informazioni attendibili possono verificare la qualità dei prodotti prima dell'acquisto oltre a determinare l'affidabilità del fornitore/produttore [27].

Dovendo fronteggiare mercati sempre più competitivi e complessi, soggetti ad una rapida evoluzione, non solo i clienti, ma anche le imprese percepiscono il vantaggio commerciale portato da un sistema di questo genere. La chiave del successo di una supply chain è determinata dall'efficienza nello scambio di informazioni tra gli attori che la compongono. Ecco perché l'obiettivo generale della catena di fornitura digitale è quello di aprire la rete di fornitura alla vista di tutti. I mercati B2C stanno spingendo le aziende a fornire questo livello di visibilità, richiedendo maggiori informazioni sugli arrivi delle spedizioni con aggiornamenti in tempo reale. Informazioni di trasporto costantemente aggiornate e affidabili possono migliorare significativamente la soddisfazione del cliente finale oltre che aiutarne la gestione per il produttore.

La digitalizzazione all'interno delle operazioni logistiche è un processo tutt'ora in via di sviluppo, con lo scopo di ottenere un elevato grado di trasparenza nel sistema e quindi permettere alle aziende non solo di risparmiare in termini di tempo ma anche di costi complessivi di gestione, favoriti da una efficienza complessiva maggiore. Nel processo evolutivo che stiamo vivendo che ci ha portato all'Industria 4.0 ed all'Internet of Things, la maggior parte dei processi aziendali dovrà divenire digitalizzato per permettere ai dispositivi tecnologici di comunicare correttamente e rapidamente tra loro e raggiungere il livello di trasparenza desiderato. Un elemento critico sarà l'evoluzione delle catene di fornitura tradizionali verso un ecosistema di supply chain connesso, intelligente e altamente efficiente. Le organizzazioni dovranno inevitabilmente digitalizzarsi per avere

accesso anch'esse alla interoperabilità dei dati, rendendo simultanei i flussi informativi tra stakeholders riducendo i tempi morti e dando completa visibilità sui processi.

Questo darà modo di individuare rapidamente le problematiche o le aree critiche che necessitano di una più attenta gestione, onde evitare situazioni di vulnerabilità nel sistema produttivo e non subire ripercussioni economiche incisive da esse. Una amplia fonte di informazioni risulterebbe uno strumento estremamente efficace e consentirebbe alle aziende di ottimizzare le strategie da intraprendere in diverse condizioni, utilizzando le informazioni per avvertire i centri produttivi, i magazzini e i clienti dei tempi di arrivo o dei rischi per intraprendere tempestive azioni di mitigazione. La visibilità sia sullo stato dei trasporti che sugli impatti esterni previsti sui tempi di consegna, e la possibilità di modificare i piani di conseguenza, sarà strumentale per le aziende che cercano di utilizzare le loro catene di fornitura a vantaggio della concorrenza, e di gestire con più attenzione i numerosi rischi associati alle attività di supply chain.

Con l'avvento della supply chain digitale, i segnali di domanda e offerta avranno origine in qualsiasi punto e viaggeranno immediatamente in tutta la rete. Informazioni come i bassi livelli di materia prima, la chiusura di un importante impianto, un improvviso aumento della domanda dei clienti saranno visibili da tutti gli attori del sistema, in tempo reale. La trasparenza consentirà alle imprese non solo di reagire alle interruzioni, ma anche di anticiparle, modellando la rete, creando scenari "what-if" e adeguando immediatamente la catena di fornitura al cambiamento delle condizioni, ottenendo enormi vantaggi in termini di servizio al cliente, flessibilità, efficienza e riduzione dei costi [27].

Gli esperti stimano che la digitalizzazione nei sistemi di supply chain apportino significativi vantaggi, sia a livello economico con incrementi nelle entrate intorno al 2,9% annuo, sia a livello logistico con un aumento nell'efficienza dei processi del 4,1% annuale [26] . La digitalizzazione industriale è un processo inevitabile se si vuole che la catena diventi un ecosistema completamente integrato e trasparente per tutti gli attori coinvolti e la tecnologia blockchain appare come lo strumento più idoneo per supportare questa rivoluzione e rispondere alle esigenze dell'Industria 4.0.

4.5 Benefici dell'utilizzo della Blockchain per il SCM

Il Supply Chain Management, come è stato precedentemente discusso, è riuscito negli anni a diventare un settore enorme, nonché la struttura di qualsiasi industria e promette di radicare i suoi concetti ancora più nel profondo del sistema economico moderno, ma non prima di vivere un passaggio di trasformazione interna. L'integrazione della blockchain supportata dagli smart contracts si pone l'obbiettivo di trasformare la struttura della supply chain garantendo la collaborazione di tutti gli attori coinvolti, per ricreare settori lavorativi più versatili e trasparenti.

Nell'era dell'industria 4.0, la blockchain viene proposta come mezzo per organizzare i documenti in modo distribuito appoggiandosi ad un meccanismo di consenso. Ha il potenziale per trasformare il supply chain management attraverso le sue caratteristiche di trasparenza, autenticità, fiducia e sicurezza, riduzione dei costi, disintermediazione, operazioni efficienti e riduzione degli sprechi. Si ritiene quindi che la natura distribuita supporti la blockchain a mitigare i rischi nella supply chain associati a pirateria, hacking, vulnerabilità, costosa conformità alle norme governative e controversie contrattuali [29] .

Ci sono molti esempi di trasformazioni di successo nelle supply chain con la tecnologia blockchain, ma esistono ancora barriere in termini di facilità d'utilizzo, scalabilità, privacy e costi [23] . Tuttavia, è proprio grazie alla sua struttura che la blockchain potrebbe rivelarsi lo strumento perfetto per garantire la sicurezza e la trasparenza necessarie per i moderni sistemi di supply chain management. Per esempio, creando un nuovo quadro BPR (Business Process Reengineering) si potrebbe avere una reingegnerizzazione dei processi delle supply chain, per favorire una ristrutturazione nel metodo di eseguire transazioni in questi sistemi e con il sostegno delle tecnologie IoT riprogrammare percorsi e processi favorendo velocità e sicurezza. La blockchain gode di un immenso potenziale per trasformare ogni fase dei della supply chain, dall'approvvigionamento delle materie prime alla distribuzione ai consumatori.

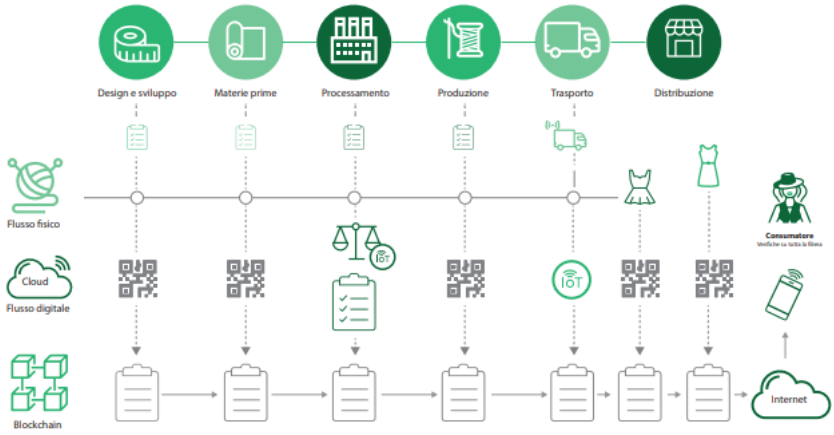

Figura 20. Rappresentazione di un flusso digitale di beni ed informazioni.

Attualmente la capacità di rintracciare le origini dei beni o di acquisire maggiori conoscenze su di essi è quasi inesistente. Tuttavia, la blockchain fornisce una piattaforma sicura per gli attori per condividere e scambiare informazioni relative alle loro merci e prodotti. L'etichettatura delle merci o del mezzo di trasporto crea un'entità che può essere posizionata sul libro mastro e consente di rintracciare il bene. Il successo del sistema dipende dal coordinamento tra gli attori della supply chain. Con la collaborazione il produttore incorporerebbe il prodotto con un codice, che verrebbe poi trasmesso alla blockchain per garantirne l'esistenza e l'originalità.

Per assicurare che il trasporto sia in alleanza con l'accordo contrattuale, gli attori possono avvalersi di smart contract, con la funzione di controllo su ogni pagamento o adeguamento del pagamento, il quale verrebbe effettuato automaticamente se le clausole del contratto non sono soddisfatte. Allo stesso tempo, un contratto concluso darebbe inizio all'esecuzione del pagamento del servizio o della merce non appena la consegna è completata. Se una clausola del contratto di trasporto non è soddisfatta, questa sarà registrata sulla catena di blocco e non saranno effettuate ulteriori attività fino a quando la clausola non sarà soddisfatta o il contratto non sarà adeguato. L'utilizzo degli attori di smart contracts basati sulla blockchain escluderebbe o ridurrebbe drasticamente i costi di transazione, che sul mercato attuale sarebbero costosi, soprattutto per gli attori più piccoli. I contratti intelligenti sarebbero vantaggiosi sia per il cliente che per il trasportatore perché il cliente avrebbe la certezza di ricevere il trasporto sostenibile che ha richiesto e

per il quale sta pagando, mentre il trasportatore riceverebbe la tariffa concordata che potrebbe includere l'assicurazione. Ciò è possibile grazie alle funzioni di ricodifica e di audit della catena di blocco e al suo tracciamento quasi in tempo reale della transazione. La funzione successiva esegue il pagamento automaticamente o i diritti di proprietà non appena la consegna viene ricevuta e registrata sul libro mastro.

La blockchain grazie alla sua natura decentralizzata, immutabile e sicura ha già influenzato numerosi settori, come abbiamo già ampiamente discusso nel terzo capitolo di questa elaborato. In seguito all'introduzione al mondo logistico ed all'avvento della supply chain come discipline di supporto alle imprese, tratteremo ora come la blockchain potrà cambiare ed evolvere ulteriormente tali discipline.

4.4 Industria 4.0 e IoT

Dietro al grande potenziale della Digital Suupply Chain (DSC) si nasconde una quarta rivoluzione industriale, definita appunto, come l'Industria 4.0 [26] . Il processo di trasformazione nei sistemi produttivi e nell'automazioni di questi ebbe inizio introno alla seconda metà del 700' con l'introduzione delle macchine a vapore e la prima, così detta, rivoluzione industriale (Industria 1.0). Proseguendo circa un secolo più tardi con l'introduzione dei prodotti chimici, il petrolio ma soprattutto dell'elettricità (Industria 2.0). In tempi più recenti invece, ci si riferisce ad una fase di introduzione massiccia di elettronica, telecomunicazioni e sistemi informatici nel settore industriale come alla terza rivoluzione industriale (Industria 3.0) [27] .

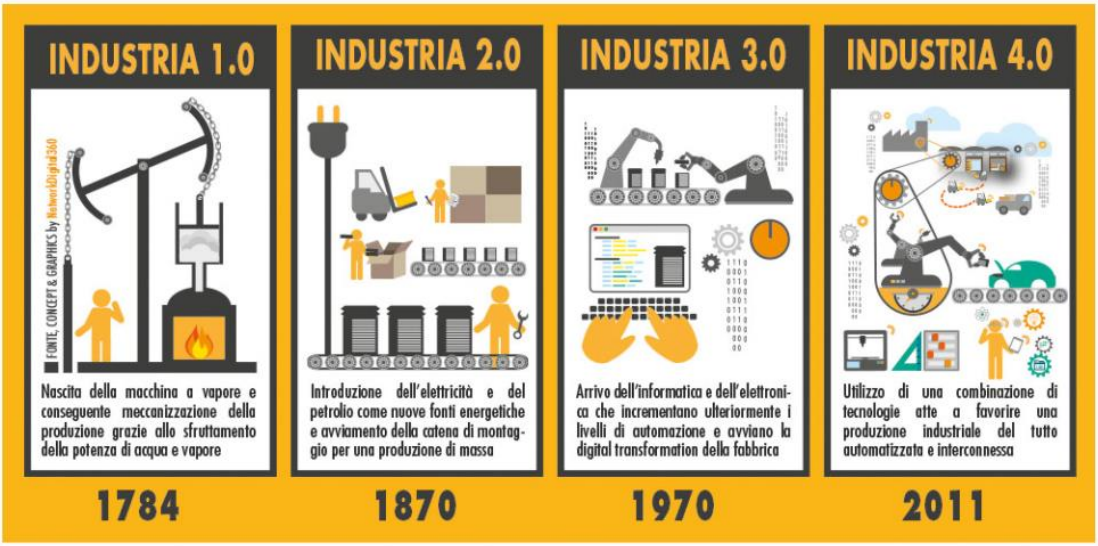

Figura 21. Le quattro rivoluzioni industriali.

Il processo di digitalizzazione invece è ciò che contraddistingue l'Industria 4.0 dai precedenti, volto a ricreare un ecosistema basato sull'implementazione di una vasta gamma di tecnologie digitali interconnesse tra loro. Di queste troviamo L'IoT, la stampa 3D, il VR (Virtual Reality), i big data, la Blockchain ed altre ancora.

In generale, come per l'industria, anche la blockchain ha già vissuto delle fasi evolutive dal 2008 ad oggi. Definiremo la prima come Blockchain 1.0, è generalmente associata al

boom delle criptovalute digitali ed ai moderni servizi di pagamento online, mentre la Blockchain 2.0 è associata ai servizi finanziari digitali automatizzati grazie all'utilizzo di smart contracts. Infine, la più recente tendenza è la Blockchain 3.0 che è incentrata sulle esigenze della società digitale, come le IoT e l'Industria 4.0.

Le tecnologie dell'informazione e della comunicazione (ICT) sono destinate a svolgere un ruolo chiave per l'industria 4.0 ed è quindi verosimile immaginarsi la blockchain, tra le sopracitate, come una delle principali tecnologie a favorire tale cambiamento, poiché strumento/mezzo di supporto che permetterebbe di usufruire il massimo delle potenzialità dalle altre tecnologie. Tuttavia, resta internet la tecnologia più critica dell'Industria 4.0 in quanto la maggior parte degli altri driver tecnologici dell'Industria 4.0 dipendono da essa, specialmente i sistemi blockchain. Per esempio, la condivisione in tempo reale delle informazioni tra varie entità attraverso una rete di comunicazione digitale o sfruttando la potenza di calcolo e la capacità di memorizzazione di dati con dei computer a distanza su scala di magazzino è abilitata attraverso internet. L'intelligenza di un sistema si ottiene attraverso l'integrazione di oggetti, prodotti e operatori e la consapevolezza del contesto tramite internet. Da questa filosofia di pensiero nasce l'Internet of Things (IoT), la qua sta vivendo una crescita esponenziale nella ricerca e nell'industria, ma soffre ancora di vulnerabilità della privacy e della sicurezza. Gli approcci convenzionali alla sicurezza e alla privacy tendono ad essere inapplicabili per l'IoT, soprattutto a causa della sua topologia decentralizzata e dei vincoli di risorse della maggior parte dei suoi dispositivi [36] .

Ciononostante, essendo la blockchain un meccanismo di consenso distribuito, il quale permette ai suoi enti partecipanti di essere informati di ogni evento o transazione molto velocemente attraverso un record inconfutabile nel ledger pubblico, questa potrebbe ritagliarsi un ruolo chiave in questa fase di evoluzione economica e sociale a supporto delle tecnologie dell'internet of things. L'insieme di tali tecnologie porteranno l'industria per come la conosciamo a proporre nuovi modelli di business, dove troveremo prodotti e servizi derivati da supply chain rinnovate, cui ogni anello della catena del valore viene integrato e digitalizzato, dal luogo di lavoro e produzione, ai metodi ed i canali di distribuzione fino alla gestione delle relazioni con i clienti. Le blockchain consentono

l'aggregazione decentralizzata di grandi quantità di dati generati dai dispositivi IoT e garantiscono una condivisione più equa dei benefici tra i partner di scambio della supply chain. È proprio dal connubio tra blockchain e IoT che l'industria 4.0 pone le sue radici per un profondo cambiamento nella struttura impresariale e sociale. Nella figura riportata sotto, vengono riportati i punti di maggiore impatto dovuti all'affiancamento dell'IoT con la tecnologia Blockchain, tra cui la scalabilità, la sicurezza, l'immutabilità e l'auditing, l'efficacia e l'efficienza del flusso di informazioni, la tracciabilità e l'interoperabilità, e la qualità [28] .

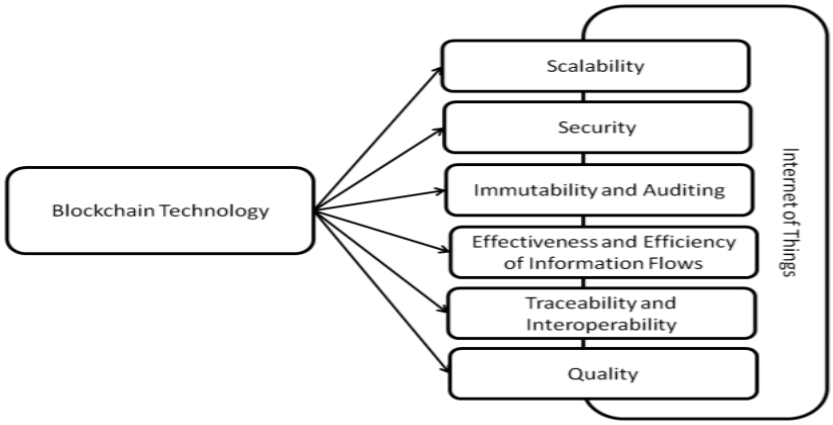

Figura 22. L'impatto dell'IoT e Blockchain sui sistemi di supply chain.

I sistemi blockchain mirano a raggiungere un elevato livello di sicurezza, tuttavia, per lo sviluppo futuro e per una più ampia diffusione della blockchain, è fondamentale poter garantire realmente tali livelli di sicurezza, soprattutto per sistemi estremamente ampli e complessi. Allo stesso tempo tecnologie come l'IoT ed il cloud computing sono strutture in cui il rischio operativo dev'essere minimo, per questo l'integrazione dell'architettura blockchain a tali sistemi non solo permetterebbe di ottenere il massimo da questi ma ne ridurrebbe anche il rischio di manomissioni o errori di sistema.

4.4.1 Scalabilità

Con il termine "Scalabilità" si fa riferimento all'abilità di un sistema di crescere e soddisfare una domanda in aumento. Nel mondo blockchain funziona in modo verosimile,

infatti parlando di scalabilità ci riferiamo all'abilità di crescita dei sistemi blockchain per soddisfare la crescente domanda di validare transazioni in entrata, traducibile come la domanda. I sistemi blockchain offrono numerosi vantaggi e per questo motivo sono già state sviluppate numerose soluzioni per l'implementazione di tale tecnologia, per soddisfare i requisiti di scalabilità dettati dall'ingente mole di dispositivi nell'IoT. La problematica principale da affrontare deriva dall'immensa capacità di calcolo necessaria per soddisfare le diversificate applicazioni dell'IoT, il che per il momento rende le attuali strutture blockchain una soluzione non sempre compatibile con l'industria in cui le si vuole implementare. I più importanti problemi di scalabilità per i sistemi blockchain sono riassumibili in 4 punti [94] :

- Limitazioni;
- dimensione dei blocchi;
- tempi di risposta;
- costi di validazione;

1. **Limitazioni:** Quando una nuova transazione viene elaborata, ogni nodo aggiunge informazioni su di essa al libro mastro. In questo modo, con l'aumento della cronologia per il numero di transazioni, c'è il pericolo che il sistema nel suo complesso venga messo in difficoltà. Tutti i dati devono essere registrati con precisione, altrimenti il livello di affidabilità può essere compromesso.
2. **Dimensione dei blocchi:** Un altro importante problema di scalabilità nelle blockchain è determinato dalla capacità di immagazzinamento dei blocchi che la compongono. Inizialmente, la capacità di ogni blocco nella più comuni blockchain era di 1 Mb, e ogni blocco poteva contenere all'incirca 2.000 transazioni. Tuttavia, il numero di transazioni derivato dal connubio tra blockchain ed IoT comporta un sostanziale aumento nel numero di transazioni da gestire nella rete, causando un'problema di scalabilità dovuto al lungo processo di validazione delle transazioni.
3. **Tempi di risposta:** Nella rete, ogni transazione deve passare attraverso un processo di convalida. In termini di tempo, le transazioni in coda, di solito devono aspettare all'incirca 10 minuti per ricevere la convalida del blocco di cui fanno parte. Vien da sé che più transazioni sono presenti in coda, più tempo ci vuole perché queste vengano elaborate ed inserite nella catena di blocchi.

4. **Costi di validazione:** Man mano che la popolarità delle criptovalute cresce più la complessità del processo di conferma delle transazioni cresce, questo perché i processi di estrazione mineraria richiederanno potenza di calcolo maggiore. Inevitabilmente ogni pagamento richiede commissioni di transazione ed in alcune piattaforme blockchain è stata data agli utenti l'opzione di pagare una sovrattassa per poter prioritizzare le proprie transazioni. Con l'espansione della rete, ed un conseguente allungamento nei tempi di gestione delle transazioni, molti utenti vogliono prioritizzare le loro transazioni creando code sempre più profonde nella rete e portando così a disuguaglianze sempre più percepibili tra gli utenti di un network blockcahin.

A differenza dei nodi minerari dei dispositivi di crittografia dell'IoT, come i sensori, i nodi minerari della blockchain hanno una capacità di calcolo limitata, che è difficile e molto costosa da migliorare. Sono state sviluppate e introdotte diverse soluzioni blockchain per soddisfare i requisiti di scalabilità dell'IoT nelle supply chain. A seconda del tipo di industria, i meccanismi di consenso e le strutture blockchain potrebbero essere più o meno compatibili con le applicazioni dell'IoT. A questo proposito, per le applicazioni sulle supply chain vengono considerate altamente più idonee le blockchain private, poiché il numero limitato di nodi preselezionati insieme agli smart contracts consento di applicare un filtraggio di dati molto più rapido e mirato, a favore di una scalabilità maggiore nell'utilizzo delle due tecnologie.

Inoltre, l'evoluzione dell'architettura blockchain porta alla nascita di soluzioni di scalabilità *"off-chain"*. Tra queste vi sono i cosiddetti sidechain, che sono catene di transazioni che corrono in parallelo alla blockchain e permettono il trasferimento di valore tra di loro. I dati sempre crescenti generati dai dispositivi IoT nella catena di fornitura possono essere criptati e memorizzati nei sidechain, e un riferimento ad essi può essere aggiunto nella blockchain principale. Questa funzionalità aiuta a ridurre significativamente la complessità di archiviazione scaricando la responsabilità di elaborazione dei dati, in termini di transazioni da convalidare.

Anche se nella sua infanzia e con una mancanza di standard di interoperabilità, la comunicazione inter-blockchain promette livelli di scalabilità più elevati, ampliando la portata dei suoi utilizzi a favore di maggior controllo sulla qualità. Esempi di transazioni che possono essere eseguite sui sidechain includono la vendita rapida nei sistemi di

pagamento e la distribuzione di criptovalute, il trasferimento di beni digitali e la generazione di ID. Tuttavia, la coerenza e l'efficienza dell'intercomunicazione tra i frammenti di blockchain rimangono un compito impegnativo da mantenere. Ad esempio, la necessità di un registro distribuito scalabile per i dispositivi IoT ha portato anche alla nascita di strutture dati alternative alla blockchain, come l'IOTA. A differenza delle blockchain tradizionali, lo IOTA è un'architettura distribuita costruita su un DAG (Directed acyclic graph) chiamato Tangle [28] . DAG è un diverso tipo di struttura di dati, pensatelo come un database che collega insieme diverse informazioni, se pensi a una blockchain come una sorta di catena di blocchi collegata, il DAG sarebbe più simile a un albero, con diversi rami che collegano una transazione ad un'altra. Il groviglio serve come struttura dati che offre una serie di vantaggi significativi, tra cui l'efficienza della scalabilità, l'assenza di commissioni e le transazioni in tempo reale. Ogni nodo che registra una transazione deve verificare altre due transazioni prima che la sua transazione sia verificata, il che accelera significativamente il processo di validazione. Il Tangle soddisfa i requisiti di memorizzazione di enormi quantità di dati e di accesso ad alta velocità ad essi. Inoltre, il suo design introduce un nuovo approccio per raggiungere il consenso e risolve i costi (spesso proibitivi) per le transazioni su microscala richiesti dai casi d'uso di rilevamento e attuazione dell'IoT. Ciò implica che le applicazioni dell'IoT nella supply chain saranno abilitate da una piattaforma di supporto che si muove verso una più efficiente e molto più economica interazione macchina-macchina. Nel caso di catene di fornitura multidirezionali e strettamente integrate, ciò potrebbe portare a potenziali risparmi sui costi e opportunità di generare nuovi flussi di reddito.

Oppure, lo sharding, che è un nuovo meccanismo per alleviare la scalabilità distribuendo i contenuti di un database tra i nodi di una rete, cioè un sistema basato sulla suddivisione del lavoro tra sottoinsiemi di nodi al fine di aumentare il throughput dell'intero sistema. Il partizionamento di una blockchain potrebbe essere particolarmente adatto per le supply chain che si affidano ai dispositivi dell'IoT, dove la catena principale gestisce eventi globali meno frequenti un esempio può essere il monitoraggio globale delle operazioni di trasbordo dei container e dei piani di emergenza, mentre le catene secondarie sono stabilite per registrare le transazioni locali frequenti e gli eventi logistici di interesse solo

per le reti regionali, per esempio, monitoraggio della produzione e della logistica in entrata ed a controllo dell'inventario.

Tutti questi metodi mirano a migliorare la scalabilità modificando gli elementi fondamentali della transazione blockchain, compreso l'aumento della dimensione dei blocchi, l'uso di nuovi o specifici protocolli di rete leggeri appositi per dispositivi IoT, blockchains modificabili o tecniche di sharding. Allo stesso modo, molte altre soluzioni innovative e più scalabili sono ancora in fase di sviluppo per fare della tecnologia blockchain un catalizzatore chiave delle supply chain nel prossimo futuro e per l'allocazione efficiente delle risorse tra le reti IoT.

4.4.2 Sicurezza

La crescente complessità delle catene d'approvvigionamento e l'ampliamento del numero di partner con cui avere relazioni commerciali, spinge le imprese a proteggere gli scambi di informazioni, nonché l'integrità degli oggetti fisici e prodotti a tutela di furti e varie forme di commercio illecito come la contraffazione.
Anche in questo caso, la tecnologia blockchain si candida come lo strumento idoneo per fronteggiare questo genere di problematiche essendo un sistema che consente l'autenticazione, la privacy, il controllo degli accessi e la tracciabilità dei dati e delle risorse nonché garantendo l'integrità nei servizi che fornisce. Inoltre, permetterebbe la formazione di un quadro analitico di controllo del rischio, con il quale studiare lo stato di connessione tra business, informazione ed ingegneria così da raccogliere una prospettiva analitica concreta sulla digitalizzazione implementata sulla supply chain di riferimento.
Di seguito elenchiamo tre possibili casi di utilizzo della blockchain per fornire sicurezza:

1. Sicurezza nell'Internet of Things: Il sistema tradizionale su cui si basano i sistemi IoT oggi è una network centralizzato, che ad oggi non può garantire la totale sicurezza e corretta interazione tra i dispositivi in costante aumento, specialmente per supply chain troppo complesse. Mentre la blockchain si struttura di regole e algoritmi di consenso per l'archiviazione dinamica dei dati, la sicurezza della

trasmissione dei dati end-to-end e la tracciabilità e il monitoraggio dei prodotti, caratteristiche che contribuiscono nel migliorare la sicurezza dei dispositivi dell'IoT e ne facilitano il flusso delle transazioni e delle informazioni. Inoltre, per sua natura, la blockchain è meno soggetta a manomissioni e frodi di identità in quanto fornisce una piattaforma di condivisione decentralizzata per la verifica dei dati oltre ad offrire una struttura di contabilità immutabile. La combinazione di blockchain e IoT introduce un sistema peer-to-peer più resiliente, reattivo e distribuito, con la capacità di interagire con gli altri utenti della rete in modo sicuro ed istantaneo. Ancor più importante, la blockchain è in grado di mettere a frutto i potenziali benefici dell'internet of things e di colmare il divario di interoperabilità tra dispositivi e dati, mantenendo al contempo sicurezza, privacy e affidabilità.

2. Sistema di rilevamento delle intrusioni: La tecnologia blockchain facilita la risoluzione di diverse sfide di sicurezza come l'identificazione univoca. Può limitare l'accesso di alcuni dispositivi selezionati e minimizzare le possibilità di accesso non autorizzato aiutando a creare dei sistemi di rilevamento delle intrusioni collaborativi, in cui i codici dei prodotti possono interagire tra loro e scambiare dati durante tutto il loro percorso. Allo stesso modo, i dispostivi dell'IoT fungono da collegamento tra il mondo fisico e quello digitale. Consentendo agli user appartenenti alla catena di fornitura di ricevere informazioni affidabili direttamente dagli oggetti fisici tracciati sulla blockchain. Questa capacità, a sua volta, garantisce la condivisione di informazioni uniche e autentiche dai dispositivi, favorendo un ambiente di fiducia e trasparente tra i suoi utenti.

3. Sicurezza Radio-Frequency Identification (RFID) [24] : I sistemi RFID sono tecnologie per l'identificazione e memorizzazione automatica di informazione inerenti a oggetti, animali o persone basata sulla capacità di memorizzazione di dati da parte di particolari etichette elettroniche chiamate Tag o Transponder, capaci di rispondere all'interrogazione a distanza da parte di appositi apparati chiamati reader. Questi esistono poiché oggetti fisici come i prodotti o i sensori e dispositivi dell'IoT tendenzialmente sono elementi a rischio manomissione. Per

esempio, l'etichetta di un prodotto abilitata all'IoT collega il prodotto fisico alla sua identità virtuale, ma questo non riflette necessariamente la sua completa tracciabilità. Un sistema integrato che incorpori codici a barre, etichette RFID, sensori e blockchain potrebbe facilitare i consumatori a rifiutare l'acquisto di prodotti contraffatti, anche nel caso questo avesse un'etichetta autentica, il venditore che non possiede la proprietà (digitale) dei prodotti riconosciuta attraverso sistema blockchain non può garantirne l'autenticità. Tracciabilità e trasparenza dei prodotti viene garantita utilizzando un protocollo di autenticazione reciproca di peso ultraleggero RFID.

La RFID è utilizzata principalmente per la tracciabilità di prodotti e servizi in supply chain che può essere migliorata drasticamente con la sua integrazione con blockchain

4.4.3 Immutabilità e auditing

Dato che l'immutabilità della blockchain assicura la sua integrità transazionale, cioè l'archiviazione corretta e permanente dei blocchi e delle transazioni all'interno della blockchain, essa è di fondamentale importanza per la sicurezza della blockchain stessa, e rappresenta la pietra angolare dei suoi valori di affidabilità e di resistenza alla censura.

L'integrazione della tecnologia blockchain insieme ai dispositivi IoT fa progredire l'automazione all'interno dei sistemi supply chain e crea un ecosistema costituito da transazioni immutabili che consentono di migliorare le operazioni di audit [28] . I partner di scambio delle supply chains traggono vantaggio dall'applicazione combinata delle due tecnologie grazie allo scambio di dati transazionali sicuro e verificabile, all'interno di un contesto estremamente eterogeneo e consapevole, oltre a creare uno storico immutabile utile per tracciare il prodotto e verificarne la provenienza. Queste caratteristiche hanno suscitato l'attenzione dei produttori e fornitori di tecnologia IoT che stanno adattando le loro soluzioni perché possano essere supportate da sistemi blockchain. Nell'automatizzare diverse attività della supply chain, la blockchain può includere e sfruttare gli smart contracts, i quali garantiscono la privacy oltre a semplificare i processi, permettendo a tutti gli attori della supply chain di trarre il massimo vantaggio dall'efficienza

dell'automazione. Questo vantaggio è evidente nella capacità di elaborare le informazioni trasmesse dai dispositivi e dalle reti dell'internet of things senza tempi di inattività o interventi umani e di supportare le transazioni tra i dispositivi in modo sicuro. Questi contratti possono essere eseguiti e memorizzati nel sistema blockchain e garantiscono l'esecuzione delle regole in modo predefinito, così da supportare i processi di auditing. Tuttavia, il costante ampliamento dei nuovi ambienti di business e con essi la crescente mole di dati da immagazzinare e quindi del ledger, apporta una sempre maggiore complessità nella gestione delle informazioni, che spesso porta ad una scarsa qualità complessiva dei dati prodotti lungo le reti di supply chain. Da qui nasce l'idea di blockchain mutabili, sistemi dove è data la possibilità di cancellare, invertire o inserire nuovi blocchi di transazioni nel network. Dal momento che le supply chain stanno sperimentando la proliferazione dell'uso dei dispositivi IoT, l'utilizzo di blockchain modificabili potrebbe affrontare gli errori dovuti al passaggio di dati causati durante questa fase nascente di forte digitalizzazione. In quanto tali, le transazioni generate da fonti IoT e replicate attraverso le reti blockchain potrebbero essere modificate o rimosse mantenendo una traccia di controllo immutabile. Attualmente, le aziende stanno esplorando la possibilità che le blockchains mutevoli cambino il modo in cui i puntatori hash linkano i blocchi in modo che solo le parti autorizzate possano modificare i blocchi già registrati nel sistema. Nonostante siano intuitivamente in contraddizione con l'immutabilità come attributo chiave di tale tecnologia le blockchains mutevoli creano nuove opportunità ma sollevano anche nuove questioni relative alle regolamentazioni ed alla governance per l'esecuzione di modifiche e azioni correttive.

4.4.4 Efficienza nei flussi di informazioni

Le applicazioni blockchain creano nuove opportunità per quanto riguarda il tracciamento di beni fisici e merci nei sistemi supply chain su più livelli. Tutti gli utenti verificati appartenenti alla supply chain di riferimento verrebbero informati su beni, prodotti o merci rilevanti, che questi siano online, in transito o in negozio. Quando vengono informati sulla movimentazione di beni fisici (casse, pallet, container), materie prime o ingredienti, componenti o prodotti di consumo finale, le aziende ottengono un migliore controllo su tutta la catena produttiva. Di conseguenza, le aziende facilitano sempre più

l'accesso dei consumatori alle informazioni relative ai prodotti online o attraverso dispositivi mobili dell'IoT. Ad esempio, i consumatori possono utilizzare uno smartphone per scansionare un codice a barre o un codice QR sull'imballaggio primario di un prodotto alimentare e accedere ai dati rilevanti registrati sui sistemi blockchain [28] . Ciò potrebbe includere informazioni quali informazioni sul prodotto e sul marchio, allergeni, ingredienti, origine del prodotto, tracciabilità, metodo di lavorazione, trasporto e il suo percorso verso il mercato. La capacità del fornitore del prodotto di assicurare l'autenticità della transazione e di registrare e fornire un rapporto aperto sul trasferimento di proprietà rimane uno dei vantaggi fondamentali della tecnologia blockchain. A titolo di esempio, l'uso dell'internet of things insieme alla blockchain per lo stoccaggio e la distribuzione di prodotti alimentari deperibili si sta rivelando fondamentale per riflettere l'effetto positivo ottenuto dall'utilizzo di queste tecnologie. Quest'ultima azienda monitora ogni anello della catena del freddo in base all'utilizzo dei dispositivi IoT. Ogni problema che si verifica viene immediatamente identificato e i partner di scambio della supply chain vengono informati di conseguenza per consentire un'azione rapida. I sensori che combinano l'uso del GPS, i dati di temperatura e i contratti intelligenti sono sfruttati per automatizzare il processo e aggiornare il profilo digitale di un prodotto ogni volta che vengono rilevate anomalie durante la fase di distribuzione. Di conseguenza, le applicazioni mobili sono sempre più utilizzate dai consumatori per scansionare le etichette dei prodotti al fine di localizzare la storia di un prodotto.

Inoltre, i dati di soglia critici catturati con i sensori e memorizzati automaticamente su un sistema blockchain potrebbero essere utili per la gestione delle apparecchiature dell'impianto, per la previsione dei guasti, la programmazione di riparazioni e manutenzioni proattive appropriate prima che i gusti si verifichino. I fornitori di macchinari o di parti di ricambio, così come i fornitori di servizi di riparazione e manutenzione, potrebbero ottenere l'accesso condiviso ai registri delle apparecchiature e fornire ispezioni e certificazioni in modalità remota. Pertanto, la combinazione di queste tecnologie si presume possa divenire un catalizzatore per un aumento delle interazioni tra la diagnostica remota delle macchine, l'analisi reciproca dei dati e le interazioni tra macchina e fornitore, con il risultato di migliorare la sostituzione dei pezzi di ricambio e le pratiche generali di manutenzione.

4.4.5 Tracciabilità

Sono in fase di sviluppo diversi progetti per applicare una combinazione di blockchain e IoT per migliorare tracciabilità e interoperabilità, aiutando a definire la provenienza granulare dei beni fisici prodotti lungo le supply chains, mirando specialmente a settori come l'alimentare, il farmaceutico, dell'abbigliamento o dei beni di consumo.
Inoltre, la progettazione di protocolli di consenso specifici orientati ai contenuti consentendo, in questo modo, un dialogo sicuro e senza attrito tra i registri distribuiti dei sensori e i database, per ottimizzare la visibilità della supply chain e la garanzia della qualità. Il framework di provenienza che utilizza blockchain, memorizza tutte le informazioni critiche lungo la supply chain, assicura l'accesso ai dati in base ai ruoli e salvaguarda i dati attraverso la crittografia sicura.

E già stato accennato come la tecnologia blockchain attualmente venga utilizzata in combinazione con le etichette RFID [24] [30] a prova di manomissione per aiutare a verificare la provenienza (geografica o l'origine) e l'autenticità di un prodotto. Per fare un esempio, nelle bottiglie di vino pregiato i tag sono apposti sul tappo di sughero e mirano ad eliminare i tentativi di rabboccare le bottiglie di vino con un prodotto più economico. Registrando i dati su una piattaforma blockchain e verificando la tracciabilità e la provenienza dei prodotti, il consumatore può verificare la storia e l'autenticità di un suo acquisto inserendo il codice identificativo del prodotto nel sistema. Va notato che la certezza assoluta sull'autenticità di qualsiasi prodotto alimentare o bevanda può essere ottenuta solo utilizzando metodi di analisi del prodotto stesso basati su prove scientifiche, piuttosto che affidarsi a caratteristiche di sicurezza nascoste o palesi sulla confezione esterna.

4.4.6 Qualità

Mettendo a disposizione una traccia permanente delle operazioni fatte, raggruppate all'interno di blocchi che una volta validati non possono più essere alterati, la blockchain si propone come strumento alternativo ai più classici metodi di tracking cartacei o ai sistemi di ispezione manuale.

Oltre a facilitare tracciabilità e provenienza di un dato prodotto, una delle applicazioni più suggestive per la blockchain è l'utilizzo di database per supportare le transazioni macchina a macchina. Con la diffusione dell'Internet of Things e l'aumento del livello di complessità dei mercati, cresce la necessità che la registrazione dei dati, generati dall'interazione tra macchine, avvenga con maggiore qualità.

La qualità delle informazioni in tali sistemi digitali ed automatizzati, sicuramente dipende sia dalla qualità dei mezzi di comunicazione tra macchine ma anche dai, così detti, *Intelligent Agents* (Agenti Intelligenti) [95] . Nel campo dell'intelligenza artificiale un obbiettivo fondamentale e la realizzazione degli agenti intelligenti. Nella fattispecie un agente si definisce intelligente se fa la cosa giusta al momento giusto. Un agente è definibile come una qualsiasi entità in grado di percepire l'ambiente che lo circonda attraverso dei sensori che offrono alla macchina la possibilità di avere delle "percezioni" e di eseguire delle azioni attraverso degli attuatori. Ne è un esempio l'essere umano, i cui occhi ed orecchie rappresentano i sensori, mentre mani e braccia sono gli attuatori.

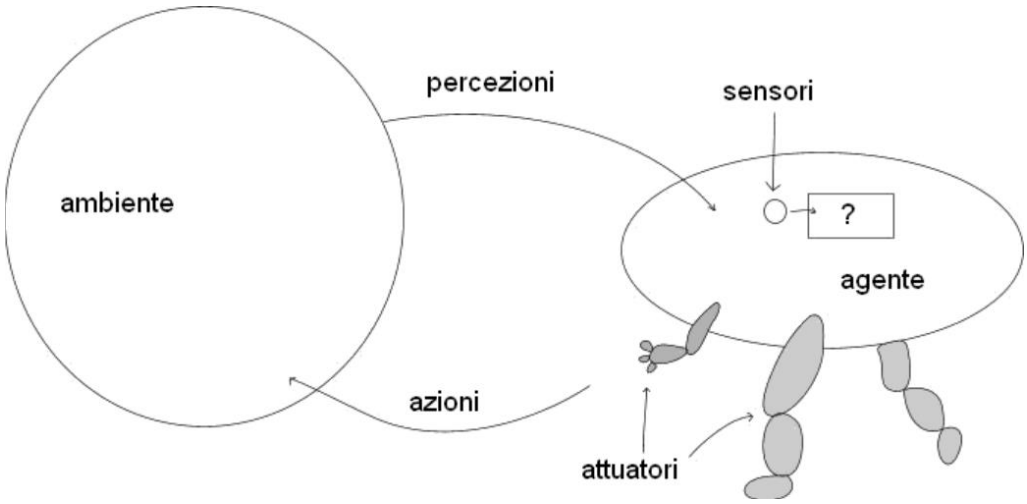

Figura 23. Possibili interazioni ambiente - macchina.

L'utilizzo dei dispositivi IoT fa si che qualsiasi prodotto venga tracciato digitalmente, dall'azienda distributrice di materie prime fino al cliente finale, creando un sistema di tracciamento dei prodotti che prende in considerazione ogni dettaglio del suo ciclo vita.

Ogni singola informazione garantisce una serie di dati critici che possono rivelare problemi relativi alla conformità qualitativa ed integrità del prodotto. Le informazioni che i dispositivi devono registrate durante le varie operazioni della supply chain vengono prestabilite da i membri del network aziendale. Questi sistemi non richiedono necessariamente di cambiare totalmente le metodologie in cui operano le aziende, ma che aggiungano dispositivi tecnologici ed automazione, per migliorare accuratezza dei dati oltre che il flusso delle informazioni da registrare su blockchain.

L'introduzione di tali tecnologie non renderà obsoleti il controllo di qualità, tracciabilità e auditing, piuttosto garantirà uno scenario più sicuro in cui operare. In linea di principio la blockchain, oltre a fornire un percorso di migrazione decentralizzato per i dati affronta il problema della qualità di quest'ultimi ed offre una soluzione pratica per avere un accesso diretto alle informazioni di ogni singola fase di un processo, di forma sicura e trasparente che non richiede interventi di entità esterne.

Essa integra la necessità di mantenere una provenienza coerente dei dati che descriva da dove provengono i dati di interesse, chi li possiede e quali trasformazioni posso aver subito nel tempo. In questo modo, i metadati pubblicati su blockchain sono protetti da compromessi e dalla divulgazione non autorizzata, le informazioni classificate come riservate rimangono tali assegnando diversi livelli di autorizzazione ai singoli utenti. Ad esempio, la tecnologia blockchain è adatta per il cloud storage distribuito. La fusione della tecnologia nell'ambiente cloud può portare a una migliore provenienza dei dati, dove i nodi cloud registrano i dati su una rete distribuita con un registro a tolleranza di errore e una forte crittografia. Da qui, il così detto *blockcloud*, un uso combinato della blockchain e del cloud computing, il quale apre la strada alla gestione e alla proprietà dei dati da parte del governo autonomo, consentendo l'accesso privato e contestuale ai dati dell'IoT, ospitati attraverso i livelli del cloud. Si tratta infatti di una vera e propria rivoluzione nel sistema di storage informativo che, allo stesso tempo, rende la blockchain una tecnologia applicabile a qualsiasi settore produttivo.

CONCLUSIONE

Fatta un po' di chiarezza, per quanto possibile in questa sede, 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.
Inoltre, si è data una definizione di *Smart Contracts* e sono state esaminate le ampie possibilità di utilizzo che gli stessi offrono, se correttamente implementati alla tecnologia blockchain, approfondendo la loro natura e la relazione intercorrente tra le due tecnologie, tentando di indagare le possibili opportunità che sistemi blockchain programmabili, come Ethereum, propongono.
In seguito, è stato riassunto come questa combinazione di tecnologie abbia recentemente portato ad una fase acuta, se non concitata, di ricerca e sviluppo e, in alcuni casi, anche all'implementazione delle stesse nei settori produttivi di maggior rilievo, con particolare attenzione a quelli che potrebbero esserne maggiormente impattati.
Infine, vengono presentate le attuali tendenze e potenziali opportunità future che il connubio tra Blockchain ed IoT può offrire ai moderni sistemi di supply chain, per introdurre le imprese e, più in generale, l'economia nell'era dell'Industria 4.0.

Per definizione, la tecnologia Blockchain è una catena di blocchi contenenti informazioni su ogni genere di transazione. Essa pertanto può essere considerata come un libro mastro condiviso, pubblico ed immutabile, che consente agli attori della rete di accedere ai dati in modo decentralizzato e sicuro.
Sono anche state analizzate le varie problematiche tipiche dei sistemi distribuiti e di come la blockchain sia in grado di approcciarle e risolverle. Ciò che può dirsi fondamentale nel descriverne il funzionamento è che, indipendentemente dal settore, i suoi protocolli e le sue strutture sono in grado di fornire grandi opportunità di sviluppo, oltre che garantire agli utenti del suo network benefici chiave come trasparenza, autenticità, sicurezza e immutabilità.
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. Tuttavia, sempre più piattaforme e tecnologie di sostegno alla blockchain sono in fase di sviluppo per affinare la tipologia di soluzioni proposte, che sappiano adeguarsi alle nuove necessità e tendenze di mercato, come l'Internet of Things..

Come si è avuto modo di desumere trattando l'ultimo capito, la gestione strategica del supply chain management è di primaria importanza per qualsiasi azienda che voglia avere successo nel proprio business. I mercati, in costante cambiamento ed evoluzione, richiedono maggiore flessibilità alle imprese che vogliono essere competitive, se non addirittura per sopravvivere, senza perdere i livelli qualitativi di prodotto e/o servizio, a cui i clienti sono abituati.

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. La sua introduzione necessità però una ridefinizione dei processi inerenti al supply chain management, volti a snellire tutte le interminabili procedure burocratiche e a migliorare l'efficienza di tutte quelle attività che richiedono, ad oggi, un lasso di tempo ancora troppo lungo di processamento in rapporto allo scarso valore del prodotto o servizio finali. Questo spiega il perché la tecnologia blockchain trova una delle sue applicazioni più interessanti proprio nella supply chain. È opinione comune che la Blockchain, affiancata alle giuste tecnologie, abbia il potenziale per trasformare radicalmente i sistemi di supply chain, sia a livello locale che globale, migliorando l'efficienza operativa, la gestione dei dati, la reattività, la trasparenza e la gestione intelligente dei contratti. Proprio gli smart contracts insieme all'IoT sono un ottimo punto di partenza per creare delle infrastrutture che possano aprire le porte verso lo sviluppo di frameworks ed ambienti lavorativi volti alla modernizzazione di numerosi settori.

E ancora, nonostante gli enormi progressi fatti negli ultimi cinque anni, la tecnologia blockchain si può considerare in uno stato embrionale poiché, ad oggi, funge ancora esclusivamente come strumento di supporto per le aziende, che non possono affidarsi totalmente ad una gestione autonoma e indipendente di tutte le fasi della supply chain. Ciononostante, volendo 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, forse e non senza riserve, un po' di certezza ed ordine in più 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 blockhain*, Documents de Travail du Centre d'Economie de la Sorbonne , May 2017. Public Blockchain versus Private blockhain (archives-ouvertes.fr)

[5] Giusy Cardinale, *Bitcoin: potenzialità e limiti del fenomeno delle criptovalute*, Società,
Maggio 2018.
http://www.salvisjur ibus.it/bitcoin-potenzialita-e-limiti-del-fenomeno-delle-criptovalute/

[6] Giuseppe Brogna, *Le 3 categorie di token secondo le linee guide della FINMA*, Etherevolution, Marzo 2018.
https://etherevolution.eu/le-tre-categorie-di-token-secondo-le-linee-guida-della-finma/

[7] 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

[8] 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

[9] 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)

[10] 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.
https://arxiv.org/pdf/1805.02707.pdf

[11] UNECE, *White Paper Blockchain in Trade Facilitation, 2019.* *http://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain.pdf*

[12] Milan Sallaba, Alexander Mogg, Mirko René Gramatke, Ralf Esser, Jens Herrmann Paulsen, *Blockchain @ Media A new Game Changer for the Media Industry?,* Deloitte, 2017.
https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/deloitte-PoV-blockchain-media.pdf

[13] Sebastiano Cappa, Michele Marzan, Giordano Buttazzo*, BLOCKCHAIN & ADVERTISING*, IAB Italia, Novembre 2018.
White_Paper_Blockchain__Advertising_Nov2018-3.pdf

[14] Tejasvi Alladi, Vinay Chamol, Joel J. P. C. Rodrigues, Sergei A. Kozlov. *Blockchain in Smart Grids: A Review on Different Use Cases*. MDPI , Nov 2019.
file:///C:/Users/elisa/Downloads/Blockchain_in_Smart_Grids_A_Review_on_Different_Us.pdf

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

[15] Merlinda Andonia, Valentin Robua, David Flynna, Simone Abramb, Dale Geachc, David Jenkins, Peter McCallumd, AndrewPeacockd, *Blockchain technology in the energy sector: A systematic review of challenges and opportunities*. ScienceDirect, Nov 2018.
https://www.sciencedirect.com/science/article/pii/S1364032118307184

[16] Benoit Laclau, *Why the energy sector must embrace blockchain now.* Ernest&Young April 2018. https://www.ey.com/en_gl/digital/blockchain-s-potential-win-for-the-energy-sector

[17] 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

[18] Camila Sitonio and Alberto Nucciarelli. *The Impact of Blockchain on the Music Industry.* Department of Economics and Management, University of Trento. July 2018.

file:///C:/Users/elisa/Downloads/TheImpactofBlockchainontheMusicIndustryRDConference.pdf

[19] Tsung-Ting Kuo, Hyeon-Eui Kim, Lucila Ohno-Machado. *Blockchain distributed ledger technologies for biomedical and health care applications*. Journal of the American Medical Informatics Association, *Volume* 24, Issue 6, November 2017, Pages 1211–1220, September 2017. https://academic.oup.com/jamia/article/24/6/1211/4108087

[20] Seyednima Khezr, Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri. *Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research.* MDPI, April 2019. https://www.mdpi.com/2076-3417/9/9/1736

[21] Gijsbert Bulk. *How blockchain could transform the world of indirect tax.* Ernest&Young, April 2018.https://www.ey.com/en_gl/trust/how-blockchain-could-transform-the-world-of-indirect-tax

[22] Ernest Frankowski, Piotr Barański and Marcjanna Bronowska. *Blockchain technology and its potential in taxes*. Deloitte, Dec 2017. https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-EN.PDF

[23] CHRISTINE LEONG, TAL VISKIN and ROBYN STEWART. *TRACING THE SUPPLY CHAIN. How blockchain can enable traceability in the food industry.* Accenture Article, 2018. https://www.accenture.com/_acnmedia/PDF-93/Accenture-Tracing-Supply-Chain-Blockchain-Study-PoV.pdf#zoom=50

[24] 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. https://www.researchgate.net/publication/321474197_Blockchain_Based_Wine_Supply_Chain_Traceability_System

[25] Ronald H. Ballou. *The Evolution and Future of Logistics and Supply Chain Management.* Weatherhead School of Management Case Western Reserve University Cleveland, Ohio USA, July 2007. EvolutionandFutureofLogisticsrevised.pdf

[26] Stefan Schrauf and Philipp Berttram. *How digitization makes the supply chain more efficient, agile, and customer-focused.* PWC Article, 2016. https://www.pwc.ch/en/publications/2017/how-digitization-makes-the-supply-chain-more-efficient-pwc-2016.pdf

[27] Mark Deimel, Mechthild Frentrup and Ludwig Theuvsen. *Transparency in food supply chains: empirical results from German pig and dairy production.* Georg-August University Goettingen, Department of Agricultural Economics and Rural Development, 2008.
https://www.wageningenacademic.com/doi/pdf/10.3920/JCNS2008.x086

[28] Abderahman Rejeb, John G. Keogh and Horst Treiblmaier. *Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management.* MDIP, July 2019.
futureinternet-11-00161.pdf

[29] 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

[30] 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)

[31] Journal*:* Supply Chain Management: an International Journal. *Blochchain Technology: Implications for operations and supply chain management.* Emerald Publishing, Sept. 2018.
https://eprints.lancs.ac.uk/id/eprint/131605/1/PDF_Proof.pdf

[32] Youness Tribis1, Abdelali El Bouchti and Houssine Bouayad. *Supply Chain Management based on Blockchain: A Systematic Mapping Study.* MATEC Web of Conferences 200, 2018.
https://www.matecconferences.org/articles/matecconf/pdf/2018/59/matecconf_iwtsce2018_00020.pdf

[33] 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

[34] Kari Korpela, Jukka Hallikas and Tomi Dahlberg. *Digital Supply Chain Transformation toward Blockchain Integration.* Proceedings of the 50th Hawaii International Conference on System Sciences, 2017
http://128.171.57.22/bitstream/10125/41666/paper0517.pdf

[35] 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. https://arxiv.org/ftp/arxiv/papers/1608/1608.05187.pdf

[36] Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets.* White Paper. 1996. http://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf

SITOGRAFIA

[37] https://it.wikipedia.org/wiki/Innovazione_distruttiva

[38] https://www.blockchain4innovation.it/mercati/industria4-0/chi-e-satoshi-nakamoto-luomo-che-ha-inventato-il-bitcoin/

[39] https://it.wikipedia.org/wiki/Rivoluzione_digitale

[40] https://it.wikipedia.org/wiki/Catena_di_montaggio#:~:text=Una%20catena%20di%20montaggio%20%C3%A8,montaggio%20di%20un%20manufatto%20complesso.

[41] https://www.html.it/10/12/2018/la-decentralizzazione-e-il-fattore-piu-importante-del-blockchain/

[42] https://www.treccani.it/vocabolario/criptovaluta_res-016bf79f-8997-11e8-a7cb-00271042e8d9_(Neologismi)#:~:text=criptovaluta%20s.%20f.%20Strumento%20digitale%20impiegato,valuta%3B%20denaro%2C%20moneta%20virtuale.&text=La%20miniera%20d'oro%20%C3%A8,%C3%A8%20l'energia%20solare%20stessa.

[43] https://www.fastweb.it/internet/cosa-e-come-funziona-p2p/

[44] https://it.bitcoinwiki.org/wiki/Double-spending_(doppia_spesa)

[45] http://www.salvisjuribus.it/bitcoin-potenzialita-e-limiti-del-fenomeno-delle-criptovalute/

[46] https://www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-bitcoins.asp

[47] https://en.wikipedia.org/wiki/Brute-force_attack
[48] https://www.investopedia.com/terms/1/51-attack.asp

[49] https://www.blockchain4innovation.it/criptovalute/mining-di-criptovalute-cose-e-come-farlo-e-quanto-si-guadagna/

[50] https://medium.com/

[51] https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/#:~:text=Le%20principali%20caratteristiche%20delle%20tecnologie,un%20database%20in%20modo%20distribuito.

[52] https://www.blockchain4innovation.it/esperti/cosa-funzionano-le-blockchain-distributed-ledgers-technology-dlt/#:~:text=Il%20Ledger%20%C3%A8%20il%20%E2%80%9CLibro,la%20base%20fondamentale%20della%20contabilit%C3%A0.&text=In%20altre%20parole%20il%20Ledger,scambi%20che%20sono%20stati%20effettuati.

[53] www.spindox.it/it/blog/la-classificazione-delle-blockchain/

[54] https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

[55] https://www.blockchain4innovation.it/criptovalute/token-cose-come-viene-utilizzato/

[56] https://etherevolution.eu/le-tre-categorie-di-token-secondo-le-linee-guida-della-finma/

[57] https://www.fintastico.com/it/blog/criptovalute-tokens-e-coins-sono-la-stessa-cosa/

[58] https://medium.com/fraglie-digitali/la-classificazione-dei-token-f1551aed0b09

[59] https://cryptonomist.ch/2018/12/01/classificazione-token/

[60] https://www.ethereum-italia.it/community/322/

[61] https://www.pmf-research.eu/smart-contracts-e-implicazioni-blockchain/

[62] https://cointelegraph.com/ethereum-for-beginners/what-are-smart-contracts-guide-for-beginners

[63] https://blockgeeks.com/guides/ethereum-gas/

[64] https://nirolution.com/decentralized-autonomous-organization/

[65] https://blockchainhub.net/dao-decentralized-autonomous-organization/

[66] https://www.multichain.com/blog/2016/06/smart-contracts-the-dao-implosion/

[67] https://www.solofinanza.it/15042019/che-cose-la-tokenizzazione/16387

[68] https://medium.com/@coinsociety/la-nascita-di-bitcoin-4c0b2e4213ce

[69] https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni

[70] https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/

[71] https://academy.binance.com/it/articles/difference-between-blockchain-and-bitcoin?fbclid=IwAR0yV9C9LB-vPC3fXUHLaLzX-hKYpQd0dNmSl09i0e6NJeJZQkKfgeC_iRk

[72] https://www.money.it/Ethereum-cos-e-come-funziona

[73] https://www.preethikasireddy.com/post/how-does-ethereum-work-anyway

[74] https://medium.com/@micheledaliessi/how-does-ethereum-work-8244b6f55297

[75] https://etherevolution.eu/consenso-blockchain/

[76] https://aithority.com/technology/cryptocurrency/announcing-oxygen-the-first-crypto-repo-trading-platform/

[77] https://www.assinews.it/01/2020/tecnologia-blockchain-migliora-la-customer-le-assicurazioni-riducono-costi/660070779/

[78] https://medium.com/@cryptoresearch/aigang-aix-the-autonomous-insurance-network-fully-automated-insurance-for-iot-devices-and-a-6ea7f08aa6e6

[79] https://insights.digitalmediasolutions.com/articles/digital-spending-2020

[80] https://www.agendadigitale.eu/sicurezza/blockchain-e-digital-advertising-ecco-come-tutelare-i-dati-dei-consumatori/

[81] https://blog.osservatori.net/it_it/blockchain-advertising-nuovi-media

[82] https://it.pearson.com/aree-disciplinari/italiano/didattica-digitale/copyright-nel-mondo-digitale.html

[83] https://www.blockchain4innovation.it/mercati/energy/energia-e-blockchain-come-cresce-il-mercato-e-in-quali-ambiti-applicativi/

[84] https://musicoin.org/

[85] https://coinswitch.co/info/musicoin/what-is-musicoin

[86] https://www.forbes.com/sites/ciocentral/2018/08/05/will-blockchain-transform-healthcare/#2e63a56c553d

[87] https://www.agendadigitale.eu/sanita/blockchain-per-il-settore-sanitario-casi-duso-e-trend-futuri/

[88] https://lina.network/how-has-estonia-applied-blockchain-technology-to-the-e-government-system/

[89] https://guardtime.com/

[90] https://www.cbinsights.com/research/report/blockchain-election-security/

[91] https://www.agendadigitale.eu/documenti/e-voting-e-blockchain-si-o-no-i-casi-internazionali/

[92] https://www.fintricity.com/blockchain-tax-fraud/

[93] https://it.pearson.com/aree-disciplinari/italiano/didattica-digitale/copyright-nel-mondo-digitale.html

[94] https://cryptoinsider.media/musicoin-music-industry-artists-listeners-rewarded/

[95] https://it.pearson.com/aree-disciplinari/italiano/didattica-digitale/copyright-nel-mondo-digitale.html

[96] https://coinswitch.co/info/musicoin/what-is-musicoin

[97] https://www.digital4.biz/supply-chain/supply-chain-trends/supply-chain-management-cose-e-perche-e-importante-per-le-aziende/

[98] https://applicature.com/blog/blockchain-technology/blockchain-scalability

[99] https://it.wikipedia.org/wiki/Agente_intelligente

[100] https://it.wikipedia.org/wiki/Cypherpunk#:~:text=Nel%20Manifesto%20Cypherpunk%20di%20Eric,privacy%20se%20ci%20aspettiamo%20qualcosa.

[101] https://medium.com/@AndreaFerraresso/bitcoin-come-funziona-il-sistema-1c970c3cad6b

RINGRAZIAMENTI

Vorrei dedicare qualche riga di questa tesi per tutte le persone che mi hanno accompagnato durante il percorso universitario, dandomi la forza per arrivare fin qui e che sicuramente non mancheranno nell'accompagnarmi nelle sfide di domani.

Innanzitutto vorrei ringraziare il mio relatore il Professor Piglione, che in questi mesi di lavoro ha saputo guidarmi e supportarmi, con numerosi suggerimenti pratici per la stesura di questo elaborato.

In particolar modo vorrei ringraziare i miei genitori per tutto il loro amore, grazie al quale hanno saputo sopportare tutte le ansie e preoccupazioni di questi anni di studio e non solo. Spero che questo piccolo traguardo possa ripagare in parte la pazienza spesa.

Un altro ringraziamento speciale va ai miei fratelli Niccolò, Jacopo e Gian Maria che da sempre sono il mio punto di riferimento ed hanno saputo darmi il supporto emotivo, che mi ha permesso di percorrere e concludere questo cammino.

Vorrei ringraziare anche i miei più cari amici. In particolar modo quelli che mi sono stati vicini durante gli alti e bassi della vita e con cui so che condividerò il raggiungimento di ancor più grandi traguardi.

Infine, vorrei ringraziare anche i miei compagni di studi oltre alle persone che ho avuto modo di conoscere durante questo percorso universitario.