LUISS

Dipartimento
di Impresa e Management

Cattedra Economia e Gestione Delle Imprese

Blockchain per Internet Of Things: *Disruptive Innovation*

Prof. Francesco Cappa
RELATORE

238341
CANDIDATO

Anno Accademico 2019/2020

Indice

Capitolo 1: Introduzione

Alla base di questo studio vi è l'analisi dell'importanza della tecnologia e delle sue dirette applicazioni. Le motivazioni che mi hanno spinto ad approfondire tale tema sono molteplici ed hanno tutte a che fare con l'attualità: si tratta di tecnologie moderne e innovative che hanno permesso la creazione di nuovi mercati. Inoltre, credo fortemente che queste, se combinate, abbiano un potenziale enorme e possano migliorare notevolmente le prestazioni aziendali. L'obiettivo di questa tesi è quello di fornire una rappresentazione di tale fenomeno mettendo in risalto l'importanza che questo può assumere nei confronti dei manager, i quali potrebbero implementare le tecnologie proposte all'interno delle proprie aziende ottenendo così degli ottimi risultati. L'elaborato, in questo modo, mira a proporre a tuti gli effetti delle nuove chiavi di lettura del fenomeno dell'evoluzione tecnologica aziendale.

Il Termine "Disruptive Innovation" nasce dal professor Clayton Christensen. Secondo il professore la "disruptive innovation" è l'effetto di una nuova tecnologia, di un nuovo modo di operare sul modello di business che porta a modificare completamente la logica fino a quel momento presente sul mercato. Può essere considerata "disruptive" nel caso in cui l'innovazione porti cambiamenti consistenti nel modello in cui è stata inserita.[1]

La blockchain può essere considerata una disrutptive innovation poiché ha cambiato fortemente il modo in cui le informazioni vengono salvate e ha rivoluzionato la logica utilizzata fino alla sua nascita per salvare le informazioni, creando così nuovi business e opportunità.

Questa tesi ha l'obiettivo di analizzare le opportunità che possono nascere dall'integrazione della blockchain nel mondo dell'IoT (internet of things). Queste due tecnologie stanno avendo un forte fermento in questi anni e hanno una moltitudine di applicazioni pratiche all'interno delle industrie. La blockchain, proprio perché è una nuova tecnologia, presenta molti buchi legislativi che analizzeremo all'interno della tesi per inquadrare gli ambiti in cui ci sarà bisogno di una maggiore regolamentazione. L'internet of things è una tecnologia che è nata prima della blockchain ma che ha avuto una forte spinta negli ultimi anni e si pensa che crescerà esponenzialmente, soprattutto se combinata con la blockchain, dato che sono due tecnologie che

si completano e spesso devono essere combinate necessariamente. Per comprendere meglio il funzionamento della blockchain, nel secondo capitolo si partirà dalla nascita e l'introduzione di alcuni concetti fondamentali fino ad arrivare al funzionamento e le opportunità che ha creato. Si continuerà spiegando in maniera approfondita gli elementi che la caratterizzano necessari al fine di questa tesi e infine verranno analizzati i vantaggi e gli svantaggi che derivano dalla blockchain per comprendere meglio come può essere utilizzata all'interno delle industrie.

La Blockchain è una tecnologia in fase di prototipazione. Può essere paragonata a internet quando era agli arbori, ovvero quando era ancora necessario scrivere su un terminale per interagirci. Il potenziale che deriva da questa tecnologia è enorme e grazie a questa tesi potremo capire meglio le possibilità che si sono create e gli ambiti di applicazione ma anche quali sono le maggiori criticità che inevitabilmente dovranno essere risolte prima che questa tecnologia farà parte della nostra quotidianità, dalla macchina alla casa.

Nel terzo capitolo verrà introdotto il concetto di Internet of Things (IoT), a partire dall'origine del termine a seguire il funzionamento dei sensori. Internet of Things è una delle tecnologie di cui si parla di più nell'ultimo decennio. Le origini di questo tipo di tecnologia prendono piede a inizio anni 90 ma negli ultimi 10 anni è entrata sempre più nella nostra vita quotidiana con i wearable devices, rivelandosi indispensabile per il funzionamento di molti oggetti che ci circondano, come ad esempio un iphone che è dotato di più sensori.

I sensori IoT lavorano in maniera coordinata al fine di raccogliere dati che verranno interpretati dal computer. Nell'ambito della gestione di questi dati parleremo dell'utilizzo della blockchain per l'IoT.

Nel capitolo 4 verranno spiegati dettagliatamente gli ambiti di applicazione e il ruolo cruciale della blockchain nel mondo IoT.

Smart City, Macchine a guida autonoma e smart home saranno solo alcuni degli argomenti che andremo a approfondire cercando di analizzare come questi fenomeni stanno cambiando il mondo e che impatto avranno sul nostro futuro. Analizzeremo tutti i possibili scenari tra cui i problemi che possono derivare dall'utilizzo di queste tecnologie. A fine capitolo verrà analizzato un caso studio riguardante un accordo tra il colosso tedesco MXC Foundation e il governo della China Shanghai Yangpu per avviare un progetto per

l’adozione dello smart city IoT Standard MXProtocol che permetterà di assicurare l’analisi sicura dei dati della città intelligente.

Una volta analizzate le caratteristiche del progetto ci concentreremo sui possibili scenari che questo potrebbe comportare sulla città di Shanghai, e più in generale come potrebbe impattare sulla nostra vita quotidiana.

Infine, nel capitolo 5 una volta finito il percorso di analisi dei vari elementi che costituiscono il mondo della Blockchain e dell’Internet Of Things, verranno tratte le conclusioni riguardo l’adozione di queste tecnologie e verranno evidenziate le motivazioni per le quali questa tesi è stata utile per approfondire il fenomeno.

Seppur innovative queste tecnologie combinate presentano molti problemi critici. Vedremo quali sono questi problemi e come potrebbero essere risolti.

Capitolo 2: Blockchain: Definizione, Nascita e caratteristiche

Satoshi Nakamoto è lo pseudonimo della persona o gruppo di persone che hanno dato vita alla blockchain. Infatti, nonostante le ricerche fatte ancora oggi non si conosce la reale identità di Nakamoto.

La blockchain è una tecnologia rivoluzionaria e tra le tante funzioni che ha crea la possibilità di trasferire asset sotto forma di informazioni, in maniera sicura, tracciabile e trasparente minimizzando i rischi di che le informazioni possano essere modificate o replicate.[2]

Proprio per queste sue caratteristiche rivoluzionarie è spesso paragonata alla nuova generazione di Internet. Come internet anche la blockchain è sottoposta a una barriera conoscitiva da parte nostra, e questo comporta un vero e proprio limite per i suoi utilizzi. Per utilizzare a pieno le funzionalità che offre blockchain è richiesto l'apprendimento di nuove conoscenze. Anche internet quando era agli arbori aveva una serie di problemi derivanti dalla difficoltà da parte del popolo di capire il suo meccanismo di funzionamento, come ad esempio quelli che derivavano dal terminale di comando il quale ostacolava l'entrata nel settore a un gran numero di utilizzatori. La blockchain, come internet nei suoi primi anni di vita, necessita di diventare più accessibile al pubblico. Questo processo richiederà il suo tempo e potrà accadere solo dopo un susseguirsi di innovazioni che definiranno e perfezioneranno l'utilizzo della tecnologia.

Per ripercorrere la storia della blockchain è importante partire dall'inizio con le tre date che hanno segnato la sua storia.[3]

Tutto inizio Il 31 ottobre 2008, quando Satoshi Nakamoto getta le prime basi teoriche pubblicando il "Bitcoin design paper" ovvero il white paper all'interno del quale spiega la sua invenzione come uno strumento utilizzabile come moneta virtuale Peer-to-peer risolvendo il problema del double spending.

Il double spending è un concetto di cui si parla molto in ambito di Bitcoin ed' è la situazione in cui il denaro digitale viene speso due volte.

Il 3 gennaio 2009, nasce il Genesis Block, ovvero il primo blocco della blockchain con la caratteristica unica che lo contraddistingue per essere l'unico blocco che non contiene nessuna informazione sui blocchi precedenti. Alla base del codice del primo blocco è stato incorporato all'interno il titolo di un articolo del

Times cifrato che parlava del piano di salvataggio delle banche del Regno Unito. La bancarotta di Lehman Brothers nel 2008 è stato un evento che ha scosso il mercato globale portandolo in recessione, in questo contesto la innovazione di Nakamoto ha proposto un exchange digitale in cui è possibile depositare valore senza l'intervento di intermediari in trasparenza, sicurezza e in maniera del tutto tracciabile e open source.
Il 4 Luglio 2014, l'Autorità Bancaria Europea rilascia "l'opinion on virtual currencies" in cui viene richiesto ai legislatori europei di applicare delle leggi antiriciclaggio e per contrastare il finanziamento del terrorismo nei mercati delle valute virtuali. [4] La legislazione in ambito di blockchain presenta numerosi buchi legislativi che devono essere colmati da parte delle autorità competenti. Solo negli ultimi anni è stato deciso di stringere le leggi in ambito di ICO (Initial Coin Offering). Fino a pochi anni fa nascevano centinaia di criptovalute ogni giorno. Venivano create in poche settimane con White Paper e business plan spesso poco accurati, redatti con l'unico scopo di raccogliere soldi dal pubblico che era incuriosito dalla forte volatilità delle criptovalute che stavano nascendo, con la conseguenza che il pubblico il più del 90% delle volte finivano per perdere i soldi che erano stati affidati a società con sede a Singapore e quindi difficilmente perseguibili legalmente a causa dei buchi legislativi che caratterizzano il settore.
Il 2015 è un anno di svolta per la blockchain. Le maggiori riviste internazionali hanno cominciato a pubblicare numerosi articoli riguardanti la distributed ledger e la blockchain diventando cosi uno dei trend tecnologici più importanti a livello internazionale. Per la prima volta si comincia a parlare non solo di Bitcoin ma anche delle caratteristiche rivoluzionarie che sono incorporate nella blockchain dando cosi il via a moltissimi ambiti di applicazione tra cui l'integrazione della blockchain nell'internet of things.
[5]

Capitolo 2.1 Blockchain elementi introduttivi

Dopo aver fatto un excursus è importante fare una breve introduzione sugli elementi che caratterizzano la blockchain che verranno ripresi più approfonditamente in seguito.

È possibile affermare che una blockchain (letteralmente “catena di blocchi”) è una struttura di dati condivisa e immutabile. Nonostante se la sua dimensione cresce con il passare del tempo rimane immutabile perché non è più possibile modificare il contenuto dopo averlo scritto o eliminarlo senza invalidare l’intera struttura. Possiamo definire la blockchain quindi come un registro digitale in cui gli agenti identificati come nodi (o minatori o detentori del registro), a turno, registrano informazioni in sequenza in strutture di dati note come blocchi. Questi dati potrebbero comprendere ad esempio cronologie di pagamenti. Fondamentalmente è concepibile utilizzare una blockchain in qualsiasi ambito in cui è importante registrare dati. Il registro comprende un albero di blocchi che contiene tutti i dati registrati dai minatori a partire dal primo blocco, noto come blocco iniziale. Ogni parte dell’albero si riferisce a una catena che riconduce al blocco della genesi. Alcune delle azioni che i clienti e i tutori del registro acconsentono a perseguire sono effettuate implicitamente nell’ambito della blockchain. Le linee guida sono espresse tramite un codice scritto dagli ingegneri della blockchain, e includono (ma non si limitano a) gli standard crittografici che devono essere eseguiti durante la registrazione delle informazioni, i tipi di informazioni che possono essere registrate in un blocco e il compenso dei minatori. Le regole seguite dai nodi devono costituire un algoritmo di consenso. L’algoritmo di consenso deve coordinare i nodi anche quando la rete ha una certa latenza e non tutti i nodi ricevono i messaggi allo stesso ordine. La comunità gestisce la catena di blocchi. In generale, la blockchain è un nuovo meccanismo attraverso il quale i dati sono condivisi in maniera trasparente e sicura. Le grandi imprese focalizzate sull’innovazione stanno gareggiando per trovare un modo per utilizzare la tecnologia del registro decentralizzato dalla blockchain con il fine di risparmiare tempo e costi di organizzazione.
La blockchain ci ha fornito un metodo innovativo e funzionale per la registrazione dei dati. Probabilmente in termini di innovazione, può essere paragonata alla creazione della partita doppia nell’Italia del XIV secolo. Karim Lakhani, uno specialista della NASA Tournament Lab presso l’Harvard Institute for Quantitative social Science sostiene:
“Dal punto di vista concettuale, la blockchain è il TCP / IP applicato al mondo degli affari e delle transazioni. Negli anni Settanta e ottanta dal ventesimo secolo non si pensava che il protocollo TCP / IP

sarebbe stato così robusto e scalabile come si è dimostrato nel corso dei decenni. La blockchain ha lo stesso potenziale."

Possiamo affermare che la blockchain è un derivato di tecnologie in cui il registro è formato da una catena di blocchi (da li prende il nome blockchain) che contengono tutti i dati sulle transazioni e la validazione, per controllare con lo scopo di controllare che non siano state modificate e affidate a un meccanismo di consenso, che viene distribuito sulla totalità dei nodi che formano la rete, o meglio ancora su tutti i nodi della rete che vengono autorizzati a far parte del processo che si occupa di convalidare le transazioni da includere nel registro.

Le caratteristiche principali e fondamentali che rendono la blockchain una tecnologia unica e affidabile sono l'immutabilità del registro che contiene i dati, la tracciabilità delle transazioni fatte all'interno della rete e la sicurezza della crittografia. Per capire meglio la blockchain si può fare affidamento sulle definizioni proposte. Molti considerano la blockchain la nuova generazione di internet, ma meglio ancora possiamo vederlo come un internet per effettuare transazioni.

Sei componenti chiave rendono la blockchain una tecnologia unica:

- Decentrata: è l'elemento fondamentale della blockchain, implica che la blockchain non deve più dipendere dai nodi, le informazioni possono essere registrate, archiviate e aggiornate.
- Trasparente: possiamo affermare che la blockchain è trasparente in quanto il contenuto del registro è possibile visualizzarlo e consultarlo liberamente.
- Open Source: la maggior parte del framework blockchain è disponibile per tutti, il registro può essere controllato liberamente e anche gli utenti possono utilizzare la blockchain per realizzare qualsiasi applicazione di cui hanno bisogno.
- Autonomia: non è necessario comprovare la propria identità anagrafica per utilizzare la blockchain. Infatti, è possibile fare transazioni nascondendosi dietro a delle chiavi pubbliche. [6]

Come suggeriscono queste caratteristiche sopra citate, riflettendoci possiamo dedurre che la blockchain è la versione digitalizzata di un nuovo modo di fidarsi.

Per secoli persone, aziende e in alcuni casi interi settori economici hanno fatto affidamento sul semplice principio di fiducia tra le varie parti.
Questa modalità è diventata così radicata da diventare un'impresa in sé, basata sulla moltiplicazione dei ruoli intermedi lungo le catene di fornitura di servizi e prodotti.
Per questi motivi, molti ritengono che la blockchain possa anche assumere un valore "politico". Infatti, per alcuni aspetti, potrebbe essere vista come una piattaforma che permette lo sviluppo e la realizzazione di una nuova forma di democrazia completamente nuova, realmente distribuita e in grado di garantire a tutti la possibilità di verificare, per "controllare", al fine di massimizzare la trasparenza su atti e decisioni, che possono essere registrate in archivi immutabili e condivisi che si caratterizzano per essere immutabili, inalterabili e quindi immuni alla corruzione. [7]

Capitolo 2.2 Tipi di Blockchain

La blockchain non dovrebbe essere considerata come una singola entità, ma invece come un sistema variegato, che presenta molte sfaccettature. In particolare, è possibile distinguere tre tipi principali di blockchain. Ma prima di addentrarci nelle tipologie di blockchain è fondamentale introdurre il concetto di Distributed Ledger Technology (DLT).
Per DLT si intende un database che è situato all'interno di una serie di computer che sono sincronizzati tra di loro dove all'interno viene salvata una copia identica di una serie di documenti rendendo permettendo cosi di essere più facilmente reperibili agli utenti, in modo tale che hanno modo di reperirli in un maggior numero di server. Cosi facendo aumenta anche l'immutabilità infatti una delle caratteristiche del DLT è che le informazioni sono identiche in ogni computer. [2] Tornando a quanto esposto nelle righe precedenti, è dunque importante distinguere tre principali tipi di blockchain che possono essere analizzate.
La blockchain privata (permissioned): è controllata da una più autorità centrali che decidono chi può accedere. Inoltre, definisce chi può far parte della rete e il ruolo che un utente può ricoprire all'interno della

stessa. Quindi anziché consentire a chiunque di partecipare al processo di verifica delle transazioni, il compito viene affidato ad alcuni nodi selezionati. Questo tipo di blockchain è adatta a realtà industriali, questo perché sacrifica una totale decentralizzazione per avere in cambio migliori performance.

La blockchain pubblica (permissionless): è quella che viene utilizzata per esempio su Bitcoin ed è un sistema con un'autorità decentralizzata, architettura decentralizzata e logica centralizzata. Si caratterizza per il fatto che appartiene a tutti, quindi chiunque lo vuole può accedervi e inoltre non è controllata da un'entità centrale.

Viene considerata come una rete pubblica in quanto i dati vengono condivisi con tutti e nessun può essere escluso dalla rete grazie al sistema di consenso distribuito. In genere una blockchain aperta è anche open source rendendo cosi pubblico il codice che ne regola il funzionamento. Questo tipo di database è utile per tutti quei dati che devono rimanere immutati nel tempo. Questo tipo di blockchain è utilizzata per le criptovalute proprio per le sue caratteristiche uniche. Ma potrebbe essere utilizzata in molti altri ambiti come per maneggiare informazioni di utenti che non vogliono mettere in mano a un'entità centrale. Se Facebook adottasse questo tipo di soluzione non sarebbe sotto tutti i riflettori per la questione privacy, però perderebbe il suo maggiore asset, ovvero il database che raccoglie tutte le informazioni private degli utenti (a cosa mettono like, le interazioni etc)

Consorzi Blockchain/Hybrid: si caratterizza per il fatto che il processo di autorizzazione è affidato a un gruppo preselezionato. La possibilità di aderire e di operare è in funzione del fatto che sia pubblica o limitata ai soli partecipanti. Anche questo modello viene utilizzato molto nel mondo del business in quanto è un ibrido tra i due modelli precedenti.[6]

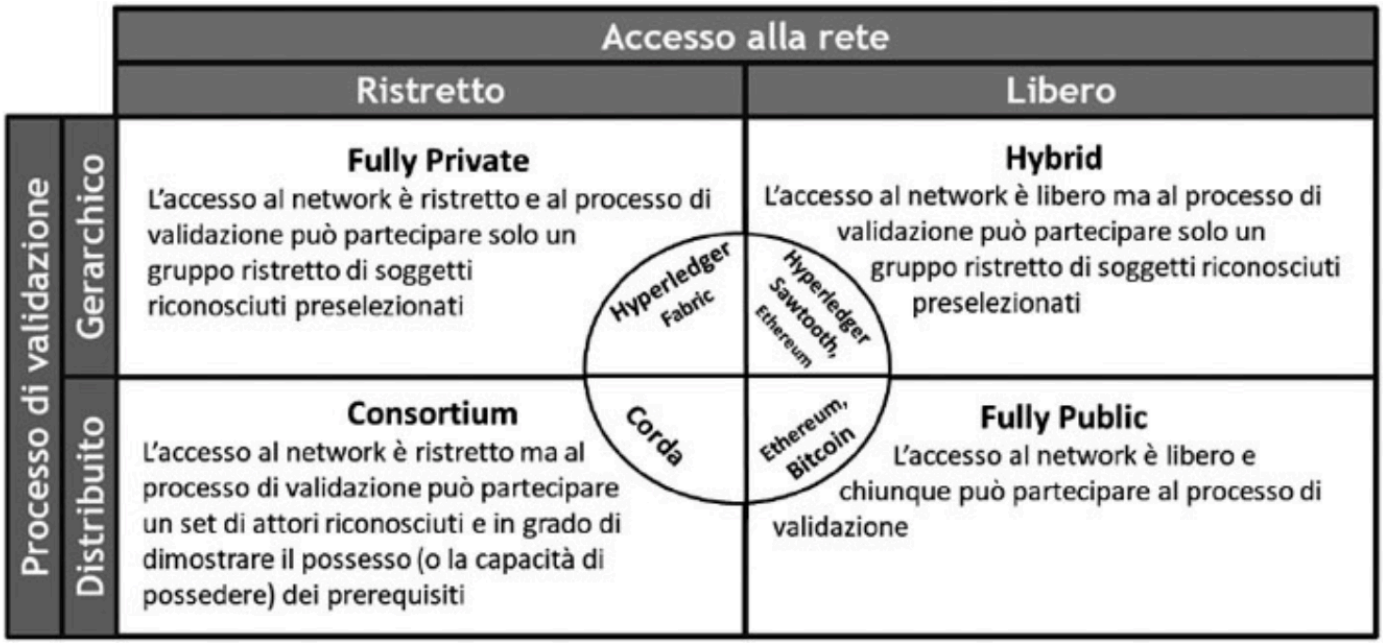

Figura 1. (immagine presa da Garavaglia, R. (2018). Tutto su Blockchain: Capire la tecnologia e le nuove opportunità. Hoepli. p.29)

Capitolo 2.3 Ledger

La blockchain funziona tramite la registrazione di informazioni all'interno di un Ledger.

Per rendere l'idea di cosa sia un Ledger, possiamo paragonarlo a un libro mastro, ma con la caratteristica che al suo interno possono essere registrate transazioni di ogni tipo.

Utilizziamo i Ledger da centinaia di anni, si sono evoluti dalla forma cartacea che hanno una logica centralizzata a quella digitale in cui è possibile integrare il concetto di decentralizzazione.

Il Ledger che utilizziamo nella blockchain è chiaramente di tipo digitale.

La differenza principale è data dal fatto che al suo interno non è possibile maneggiare dati eliminandoli o modificandoli. Infatti, è possibile maneggiare dati eliminandoli o modificandoli, all'interno del Ledger della blockchain non è possibile farlo. Infatti, è possibile la sola aggiunta di dati, questo grazie alle caratteristiche che compongono la blockchain come la crittografia e la decentralizzazione che vedremo più avanti.

Riassumendo quindi, un Ledger è un database con cui è possibile interagire solo tramite l'aggiunta di dati. L'applicazione della blockchain possiamo affermare che è utile in situazioni in cui è richiesta la sicurezza, l'immutabilità e fiducia dei dati. [3]

Permisionless ledger: è quella utilizzata da Bitcoin e ethereum e più in generale su tutte le criptovalute che impiegano il consenso distribuito Proof of Work o Proof of stake. Si caratterizza per un accesso non condizionato alla blockchain l'assenza di una terza parte e anonimato per i soggetti che effettuano transazioni.

Permisioned ledger: si caratterizzano per la presenza di una o più parti trusted e sono quelle che si basano su un protocollo per il consenso distribuito che adotta una sistema Byzantine Fault Tollerance. [2]

Citando la definizione di Wikipedia del problema dei generali bizantini "Informalmente il problema è esemplificato dalla situazione in cui tre o più generali bizantini debbano decidere se attaccare o ritirarsi dato un ordine da un comandante superiore. Uno o più dei generali potrebbero essere dei traditori con l'intenzione di confondere gli altri, quindi potrebbe verificarsi il caso in cui il comandante dia ordini discordanti ai generali oppure il caso in cui uno dei generali comunichi ai propri colleghi un ordine differente da quello impartito dal comandante. La soluzione al problema permette ai generali leali di evitare queste trappole." [8]

Nel mondo informatico possono verificarsi situazioni in cui ci si riscontrano informazioni dissonanti e che presentano degli errori, il problema si risolve se i vari componenti trovano un accordo attraverso la comunicazione tramite messaggi. L'esempio citato può essere esplicativo per quanto riguarda il modo in cui opera una blockchain. I generali possiamo paragonarli ai nodi, invece i traditori ai nodi maligni e infine i messaggeri possono essere il canale di comunicazione tra i nodi.

La blockchain deve necessariamente raggiungere un consenso distribuito anche in uno scenario come quello sopracitato, deve essere appunto Byzantine fault tolerant.

Per risolvere questo problema sono stati creati una serie di algoritmi. Quelli più famosi per quanto riguarda la blockchain sono il Proof Of Work e il Proof Of Stake. I nodi che fanno parte del processo di consenso sono detti miners e il lavoro che fanno viene detto mining. Approfondiremo questa tematica più avanti nell'ambito del mining.

Capitolo 2.4 Reti decentralizzate e centralizzate e Distributed systems

Nei sistemi centralizzati le decisioni del sistema vengono prese da un meccanismo centrale e vengono poi trasferite alle persone o ai componenti esecutivi. Viene tutto fatto in un singolo nodo. Possiamo paragonare un sistema centralizzato a un CEO che governa un'intera azienda.

Un sistema decentralizzato invece funziona con il P2P, ovvero nessuna entità ha il controllo dell'intero processo. Questo implica che le informazioni sono distribuite in varie parti eliminando così i rischi collegati allo storage di dati in un unico luogo. Il punto chiave della decentralizzazione è che non c'è un punto centrale di controllo, nessuna entità controlla l'altra.

Quando si parla di decentralizzazione è di fondamentale importanza introdurre il concetto di immutabilità, ossia che all'interno della blockchain le informazioni vengono salvate in maniera permanente e immutabile. Quindi se un blocco passato venisse modificato provocherebbe la modifica anche di tutti i blocchi successivi modificando cosi la blockchain con il risultato di essere rifiutata dalla rete. Grazie alla funzione hash i nodi sono in grado di capire se l'integrità della blockchain è rimasta immutata nel tempo.

È importante però specificare che l'hashing non garantisce l'immutabilità della rete, ma invece rende evidente ogni modificazione della blockchain. Di conseguenza chiunque provi a modificare la sua copia della blockchain avrebbe difficoltà invece a convincere il network che la sua copia manomessa sia corretta.

Per ridurre il rischio di attacchi ai server le aziende come Google, Facebook hanno una rigida politica di controllo sugli accessi per ridurre i rischi. Questo perché sono basate su un sistema centralizzato di storage di informazioni che l'azienda detiene tramite dei server. Nelle blockchain pubbliche questo non è possibile in quanto tutto è aperto al pubblico, si parla un sistema che detiene miliardi di dollari in indirizzi pubblici costantemente sotto attacco. Il sistema è sicuro grazie alla natura distribuita e decentralizzata che insieme ai protocolli di crittografia rendono quasi impossibile rubare i soldi detenuti nei wallet proprio perché non c'è un punto centrale di attacco. [3]

Nei Distributed Systems una serie di componenti che comunicano tra di loro al fine di raggiungere lo stesso obiettivo. Questi componenti non sono localizzati in un punto specifico ma sono localizzati nei vari

computer che sono connessi tra di loro tramite rete (riportato in figura 2). Ma questo non vuol dire che un Distributed Systems sia necessariamente sotto il controllo di un'entità centrale. Infatti, un sistema decentralizzato è anche distribuito, ma un sistema distribuito non è necessariamente decentralizzato. [9]

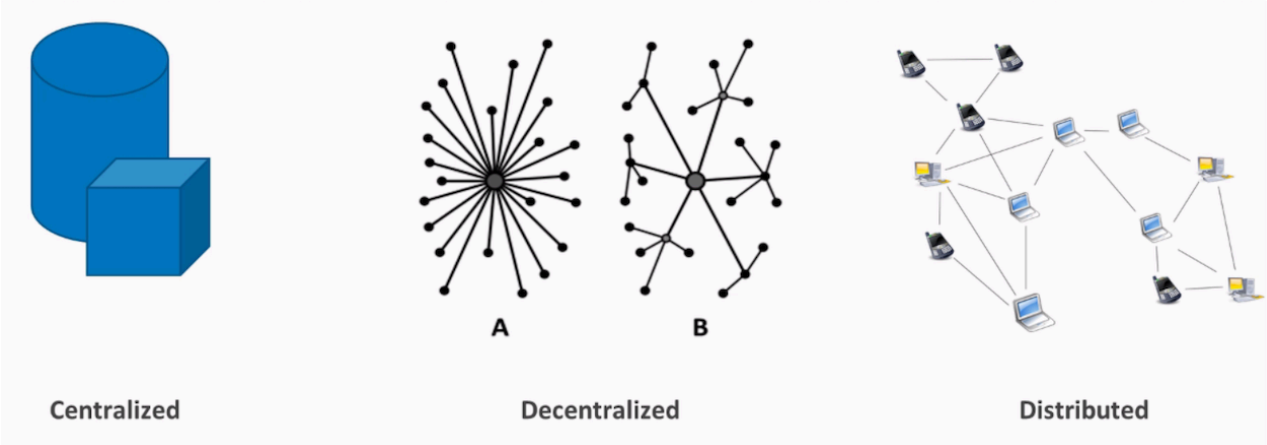

Figura 2.(immagine presa da Chiap, G., Ranalli, J. and Bianchi, R. (2019). Blockchain. Tecnologia e applicazioni per il business: Tutto ciò che serve per entrare nella nuova rivoluzione digitale)

Capitolo 2.5 Nodi

Qualsiasi computer che è collegato alla blockchain può essere definito un nodo. Dobbiamo però distinguere due tipologie di nodi:

Nodo Completo: ha la funzione di scaricare e archiviare localmente una copia della blockchain e si occupa di controllare che ogni transazione e blocco seguano le regole del sistema.

Nel caso in cui ci fosse un'anomalia, il blocco (ovvero la transazione) verrebbe rifiutato, anche se gli altri nodi della rete lo considerassero valido. Un full node quindi non necessita della fiducia degli altri nodi e segue le regole indipendentemente da tutto. Possiamo quindi affermare che utilizzare un full node è il modo più sicuro per utilizzare la blockchain. Per utilizzarlo è richiesto però scaricare l'intera blockhain sul computer ma non è particolarmente pesante, ad esempio nel caso di Bitcoin pesava 180GB nel 2018.

Nodo Light: a differenza del nodo completo non è necessario scaricare l'intera blockchain ma riceve solo i dati necessari da un nodo fidato (il full-node). Questa tipologia di nodo è quella più utilizzata. Un esempio di light node può essere quello di un wallet per ricevere e inviare criptovalute su un dispositivo mobile.
Una delle ragioni che ha portato alla nascita della blockchain è la ricerca di una piattaforma che potesse essere indipendente dall'errore umano (infatti nel 2009 quando Satoshi Nakamoto creò il primo blocco all'interno c'era un chiaro messaggio che faceva riferimento agli avvenimenti che causarono la crisi del 2008). Dato che il Full Node segue le regole imposte dal sistema, ne consegue che è un sistema libero dai problemi che hanno fatto emergere che le istituzioni centralizzate non funzionano come la corruzione. [3]

Capitolo 2.6 Crittografia

La crittografia è un insieme di tecniche che permettono di comunicare in maniera sicura su internet. Nella blockchain viene utilizzata molto la crittografia a chiave pubblica, una tecnica molto utilizzata in internet. Con questo sistema gli indirizzi sulla blockchain sono generati tramite un sistema crittografico e le transazioni vengono autenticate con firme digitali, spiegheremo questo concetto più approfonditamente a breve ma prima è necessario capire il funzionamento delle chiavi crittografiche.
Le chiavi crittografiche possono essere racchiuse in due tipologie:
La chiave pubblica: questa chiave deriva matematicamente dalla chiave privata non è segreta. Anche se la chiave pubblica deriva dalla chiave privata non è possibile in alcun modo derivare la chiave privata tramite la pubblica.
La chiave privata: generata in maniera casuale e deve restare segreta.
Le chiavi sono composte da numeri e lettere.
Generare una chiave pubblica da una chiave privata è un procedimento facile da fare utilizzando programmi appositi, ma invertire l'operazione è quasi impossibile, per rendere meglio l'idea anche con i super computer

più moderni ci vorrebbero milioni di anni. Questo è uno dei motivi per il quale è impossibile hackerare le chiavi crittografiche.

La criptazione è il processo attraverso il quale un'informazione, viene codificata in modo tale che solo chi viene autorizzato possa accedere alle informazioni inviate. Quindi una volta criptata un'informazione può navigare su internet in maniera sicura.

Per criptare un messaggio è necessario utilizzare la chiave pubblica del destinatario per criptare il messaggio. Solo il possessore della chiave privata collegata alla chiave pubblica potrà decriptare il messaggio.

Un messaggio criptato però è comunque possibile da modificare, per risolvere questo problema si usa integrare altre tecniche alla criptazione come l'hashing.

Le firme digitali sono un metodo per garantire la presenza di qualcuno all'interno di una transazione senza la presenza fisica. "Le firme digitali sono create con una combinazione di hashing e crittografia a chiave pubblica". [3]

Capitolo 2.7 Transazioni

Come abbiamo visto precedentemente una transazione causa un nuovo stato nella blockchain.

Le transazioni sono di tipo monetario (ad esempio l'invio di Bitcoin), ma possono avere anche a oggetto asset digitali (stock, certificati di proprietà etc.).

Una transazione può essere ritenuta valida solo se viene approvata dal consenso del network. Non essendoci un'autorità centrale il consenso decide quali transazioni sono avvenute e la cronologia delle stesse. Quindi se non è avvenuto il consenso del network non è considerata valida.

Le transazioni possono o cambiare lo stato della blockchain se considerate valide oppure lasciare la blockchain nel suo stato se considerate non valide, ma non possono generare in alcun modo stati intermedi ed è per questo che vengono definite operazioni atomiche.

Quindi se creiamo una transazione, una volta validata non c'è modo per annullarla o modificarla, proprio per il principio di immutabilità che caratterizza la blockchain.

Però è possibile creare delle condizioni tramite gli smart contract. Possiamo per esempio subordinare la conferma di un pagamento al raggiungimento di vincoli specifici.

Per effettuare una transazione è semplice, come prima cosa è necessario possedere la chiave privata di un indirizzo a cui è associato l'asset che vogliamo inviare. Una volta inviato, la chiave privata firmerà digitalmente la transazione, che in seguito verrà validata dai nodi e infine sarà disponibile reperirla sull'indirizzo del destinatario.

La firma digitale certifica che la transazione non è stata modificata in seguito alla firma e infine che l'indirizzo da cui proviene la transazione proviene dall'utente di origine il quale non potrà ripudiare.

La transazione che viene considerata valida viene quindi inviata ai nodi del network i quali hanno dovranno verificare la validità della transazione e se continuare a propagarla o meno, ma non è ancora registrata in modo immutabile.

Per comprendere meglio il funzionamento delle transazioni è utile introdurre il concetto di conferma di una transazione.

Le transazioni devono superare una verifica prima di essere inserite nel blocco, ma prima di essere aggiunta la transazione è definita "senza conferme". Una volta inclusa in un blocco ha 1 conferma, quando viene aggiunta al blocco successivo avrà 2 conferme etc. Prima che la transazione venga considerata immutabile la transazione dovrà essere inserita in una serie di blocchi, nel caso di Bitcoin 6 sono sufficienti.

Ogni transazione ha un costo che viene utilizzato per ricompensare i miners (spiegheremo il loro ruolo più avanti). [3]

Capitolo 2.8 Hash

Con il termine hash si intende una stringa di lettere e cifre che permette di effettuare una conversione di un messaggio contenente un numero variabile di caratteri in un codice alfanumerico di lunghezza fissa chiamato digest o impronta digitale. [2]

Quindi l'input di un hash può contenere da un file mp3 a un'intera blokchain, invece l'output sarà composto sempre da un numero predefinito di caratteri. L'hash ha diverse funzioni fondamentali.

Una funzione deterministica ovvero lo stesso input produrrà sempre l'output corrispondente. Infatti, la modificazione seppur minima del messaggio potrebbe generare un Hash completamente diverso. Rendendo impossibile modificare il contenuto senza lasciarne traccia. Nel caso in cui ci sono due file apparentemente uguali sarà sufficiente confrontare l'hash per capire se i file sono anche minimamente diversi. Quindi possiamo vedere l'hash come una impronta digitale di un file.

Unidirezionale in quanto è impossibile dall'output risalire all'input. Quindi se un malintenzionato provasse a decifrarlo con tecniche brute-force (ovvero provare tutte le possibili combinazioni) e super computer di ultima generazione non riuscirebbe comunque a risalire all'input (riportato in figura 3).

All'interno della blockchain, una delle funzioni più importanti dell'hash è quella di esprimere l'intero stato della blockchain tramite una stringa di lunghezza definita. Nei nuovi blocchi generati infatti l'hash corrispondente al vecchio blocco viene inserito nell'input del nuovo blocco.

Questa funzione è quella che rende la blockchain immutabile in quanto se qualcuno provasse a modificare, cancellare, aggiungere informazioni contenenti in un blocco passato andrebbe a cambiare la conformazione del hash del blocco e di conseguenza anche l'hash tutti i blocchi successivi. Attualmente la blockchain è di 290 GB, per valutare lo stato corrente sarà sufficiente guarda l'hash dell'ultimo blocco.

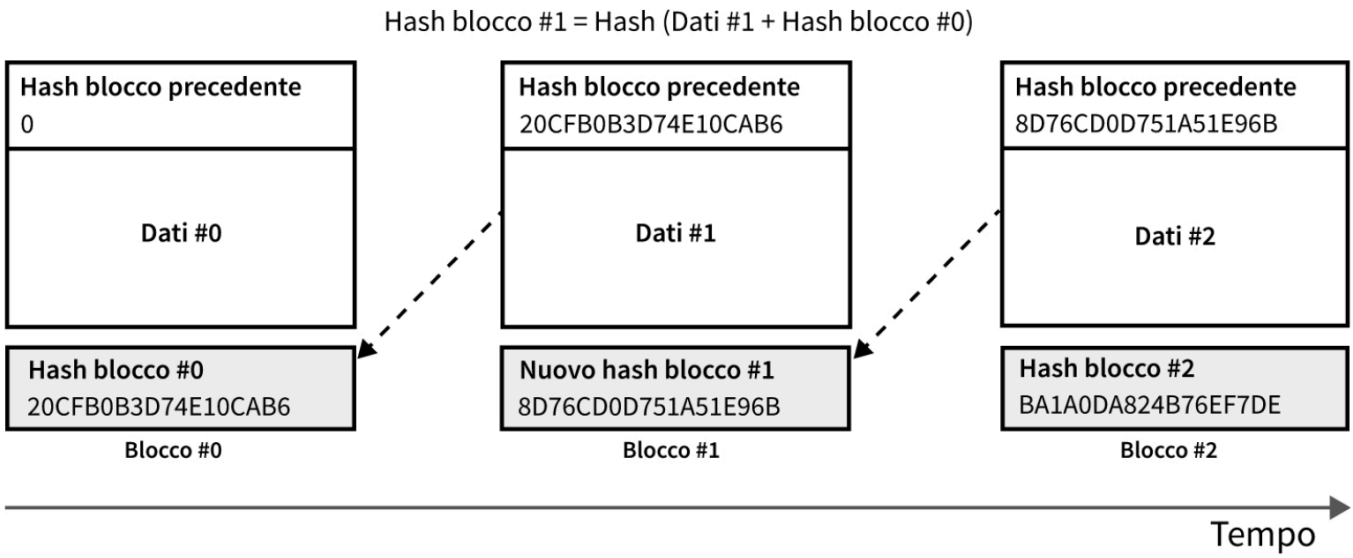

Figura 3. (immagine presa da Chiap, G., Ranalli, J. and Bianchi, R. (2019). Blockchain. Tecnologia e applicazioni per il business: Tutto ciò che serve per entrare nella nuova rivoluzione digitale)

L'hashing è un metodo di verifica delle informazioni utilizzato come garanzia che le informazioni non sono state manomesse prima di essere viste dal beneficiario proposto. In questo modo, ad esempio, nel caso in cui l'utente scarichi un registro contenente dati delicati, potrebbe eseguirlo attraverso un calcolo dei hash, quindi dovrebbe calcolare l'hash del registro e paragonarlo con quello del mittente. Nel caso in cui gli hash non corrispondono, può essere sicuro che il registro è stato modificato prima di ottenerlo.
Nella blockchain, gli hash vengono utilizzati per descriverne lo stato attuale. Di conseguenza, l'hash racconta tutto ciò che è accaduto sulla blockchain, quindi ogni transazione fino a quel momento. Ciò significa che l'hash di una blockchain, è plasmato da tutti gli scambi passati avvenuti su una blockchain. Quindi anche il cambiamento più piccolo in qualsiasi parte dei blocchi passati si traduce in un enorme cambiamento nell'hash finale; questa è la dimostrazione dell'innegabile sicurezza dell'innovazione blockchain. La modifica di qualsiasi blocco che si è verificato recentemente su una blockchain cambierebbe tutti gli hash. Il primo blocco di una blockchain, noto come blocco iniziale, contiene i suoi scambi che, una volta consolidati e approvati, producono un hash speciale. Questo hash e tutti i nuovi scambi vengono quindi utilizzati per creare un nuovo hash che viene utilizzato nel blocco successivo della catena.

Ciò implica che ogni blocco si ricolleghi al blocco precedente attraverso il suo hash, creando cosi una catena fino al blocco iniziale, da questo concetto prende il nome la blockchain ovvero catena di blocchi. Pertanto, gli scambi possono essere effettuati in modo sicuro purché i nodi sul sistema siano in accordo su ciò che dovrebbe essere l'hash.

Quando i nodi verificano il nodo validato propagato nel network viene espresso il loro consenso e quindi l'accettazione del nuovo blocco. Una volta accettato viene inserito nella catena e comincia il processo di creazione del blocco successivo utilizzando l'hash del blocco utilizzato precedentemente. [3]

Capitolo 2.9 Mining

Anche se il mining molte volte viene associato al Bitcoin, viene utilizzato su tutte le blockchain.

Il mining è un processo attraverso il quale il network della blockchain può validare le transazioni, raggrupparle e aggiungerle alla blockchain.

Questo meccanismo consente di ottenere il consenso distribuito e quindi rendere il network sicuro.

Tutti i nodi che partecipano a questo processo di consenso sono detti miner e il processo che svolgono è detto mining.

Oltre quelle sopracitate le responsabilità di un miner sono quelle di:

Assicurarsi che le transazioni siano valide e nel caso lo siano hanno il compito di propagarli per il network.

Controllare che i blocchi siano validi e in caso positivo propagarli per il network

Inoltre, hanno il compito di scegliere le transazioni per poi ordinarle e aggiungerle al blocco.

Invece un full node ha il compito di validare le transazioni e i nuovi blocchi e propagarle al resto della rete ma solo se sono valide.

Il ruolo di un full-node all'interno della blockchain è quello di renderla sicura e lo fa analizzando la validità delle transazioni di ogni blocco, assicurandosi cosi che i miner non possono imbrogliare.

Per questo motivo full-node può essere considerato il metodo più sicuro e efficace per utilizzare la blockchain proprio perché un full node non accetta in nessun caso una transazione oppure un blocco che non è conforme alle regole.

Nel caso in cui un miner crei un blocco che non è valido, tutti gli altri nodi non lo accetteranno. Nel caso in cui il blocco del miner venisse accettato e quindi aggiunto alla blockchain allora potrà essere ricompensato secondo le regole che caratterizzano la blockchain su cui opera. La ricompensa potrebbe consistere in commissioni di transazione del blocco e in alcuni casi può prevedere delle criptovalute che sono generate grazie all'aggiunta del nuovo blocco. [3]

Capitolo 2.10 Proof of Work

Come precedentemente accennato quando si parlava di algoritmi Byzantine fault tolerant, il Proof of Work che può essere tradotto letteralmente prova del lavoro è utilizzato al fine di raggiungere il consenso distribuito. Prima di spiegare In linea generale il funzionamento del Proof of Work è necessario spiegare che Proof of Work indica sia l'algoritmo Proof of Work che la soluzione del problema da risolvere. Per questo motivo quando scriverò PoW mi riferirò alla soluzione del problema, invece quando scriverò Proof of Work mi riferirò all'algoritmo.

Il Proof of Work è basato sulla ricerca di un numero difficile computazionalmente da trovare, una volta trovato diventa facile per tutti gli altri nodi verificare la correttezza.

Nei sistemi che utilizzano il PoW, i blocchi vengono considerati validi solo se contengono la soluzione valida al PoW.

Il valore che cerca il PoW apparentemente ha gran parte delle caratteristiche di un hash, difatti il PoW è basato sugli algoritmi dell'hash. Da ricordarsi che l'hash ha la funzione di trasformare un input di qualsiasi tipo in un output di lunghezza definita in una funzione non invertibile. [3]

Capitolo 2.10.11 PoW Mining

Per quanto riguarda il PoW-mining, i nodi del network concorrono al fine di risolvere problemi matematici complessi. Per risolvere il suddetto problema è necessario provare tutte le combinazioni finche non si trova la risposta giusta. Questo sistema è del tutto casuale e con probabilità basse di trovare la combinazione giusta.

Il primo miner che riesce a risolvere il problema potrà creare il successivo blocco e ricevere una ricompensa per il lavoro svolto. Quando il nuovo blocco viene creato potrà essere trasmesso alla rete, nel frattempo gli altri nodi del network ne dovranno verificare la validità. Nel caso in cui il blocco sia valido può essere inoltrato ai nodi vicini nel caso contrario viene ignorato.

In un sistema basato sul PoW il mining ha le seguenti caratteristiche:

- Le transazioni una volta create vengono trasmesse alla rete di nodi.
- Sono i miners a scegliere quali transazioni vogliono (ovvero quelle con commissioni maggiori). Queste transazioni vengono raccolte in un blocco detto blocco candidato, in quanto non ancora valido non avendo una soluzione valida al PoW.
- Il miner inizia eseguendo calcoli al fine di trovare la soluzione al problema matematico e generare una valida PoW per il blocco da lui costruito. Per ogni soluzione non validata il miner cambia il valore di un numero, che è detto nonce, e viene aggiunto all'input del PoW per cambiare il valore finale della soluzione.
- Appena il miner genera un PoW valido per il blocco nuovo, trasmette il blocco all'intera rete
- I nodi della rete si occupano di verificare la validità del nuovo blocco.
- Nel caso in cui il blocco sia validato, il miner può aggiudicarsi le commissioni delle transazioni. In seguito, il nodo potrà essere aggiunto dalla rete nella blockchain.

Nell'ambito del PoW la potenza di calcolo può essere misurata con l'hashrate, questo perché il problema che deve essere risolto è un hash inverso con alcuni vincoli.

Tramite l'hashrate possiamo sapere il numero di hash calcolati al secondo.

Una PoW come abbiamo accennato precedentemente deve soddisfare un vincolo detto difficoltà.
La difficoltà indica quanto è difficile trovare la PoW valida.
Si può fissate il target di difficoltà impostando che l'hash da trovare deve iniziare per esempio con 9 zeri.
Questo vuol dire che i primi 9 valori saranno tutti 0 per soddisfare il target impostato. [3]

Capitolo 2.10.2 Proof of work pro e contro

Il Proof of Work viene scelto all'interno delle blockchain soprattutto perché si caratterizza per una sicurezza dell'immutabilità della catena.
Questa sicurezza è data dal fatto che una volta che le transazioni raggiungono un numero sufficiente di conferme sono estremamente difficili da modificare, più blocchi vengono aggiunti (quindi quante più transazioni vengono confermate) e sempre più difficile sarà modificarle.
Il problema principale del Proof of Work è l'elevato consumo di energia richiesto per la potenza di calcolo.
Per dare un'idea della quantità di energia richiesta, il PoW attualmente consuma lo 0.3% dell'elettricità mondiale ovvero più di 1 000 000 $ al giorno di elettricità. Proprio questo suo difetto però la rende impossibile da attaccare, per la enorme potenza di calcolo necessaria a validare le transazioni.
Ma l'elevato consumo di corrente non è l'unico problema infatti non è facilmente scalabile e infine c'è discriminazione geografica, economie di scala e centralizzazione. I miners sono in aree geografiche in cui il costo della corrente e le temperature sono basse. Un posto caldo implicherebbe un maggior numero di ventole di raffreddamento per i computer e quindi un maggior consumo di elettricità e costi fissi maggiori.
Oltretutto vengono applicate economie di scala per ottenere elettricità e i macchinari necessari per attuare il mining. [3]

Capitolo 2.11 Proof of Stake

Il Proof of Stake è il protocollo più famoso della blockchain insieme al Proof of work.
Lo scopo è lo stesso per entrambe ma cambia il processo per raggiungerlo. Nel Proof of Stake non esiste la figura del miner, infatti in questo tipo di protocollo vengono premiati i validatori che sono l'equivalente del miner. Vengono scelti in base alla quantità di criptovalute (detta anche stake) che detengono all'interno della blockchain in cui opera il protocollo.

Capitolo 2.11.1 Proof of stake mining

Nel caso del Proof of Stake invece che la potenza di calcola in possesso, vengono utilizzati i token in possesso. Gli utenti bloccano temporaneamente i propri token fino a quanto il processo di **staking** si conclude ottenendo in cambio il diritto di conferma delle transazioni di un blocco e una volta validato ottenere in cambio una ricompensa.
Il creatore del nuovo blocco a differenza del PoW viene scelto in anticipo se soddisferà determinati parametri, che cambiano in base all'algoritmo utilizzato. Possono cambiare ad esempio in base al numero di token, o anche il tempo in cui il validatore detiene i token.
Il protocollo Pos è equo verso i validatori. Infatti, un validatore che detiene il 10% del totale dei token, ha il 10% di probabilità di ottenere il diritto a creare il nuovo blocco.
Per rendere meglio l'idea di come funziona, facciamo un esempio pratico su 3 personaggi immaginari (validatori).

- Francesco detiene 500 Ethereum
- Giulia detiene 300 Ethereum
- Marco detiene 200 Ethereum

Lo stake totale della rete totale del network è composto quindi da 1000 Ethereum. Secondo la logica del PoS Francesco verrà scelto il 50% delle volte, Giulia il 30% delle volte e Marco il 20% delle volte.

Se paragoniamo il PoW al Proof of Stake il Proof of stake in termini di efficienza è il migliore.

Il PoS è dotato di caratteristiche uniche che lo contraddistinguono dal PoW.

Gli attacchi sono più onerosi. Come per il PoW anche nel caso del Proof of Stake se un miner (o validatore nel caso del PoS) malintenzionato riuscisse ad acquisire il 51% della potenza di calcolo del network potrebbe creare blocchi più velocemente rispetto a tutti gli altri miners insieme. Il miner quindi potrebbe invertire o anche modificare le proprie transazioni e potrebbe essere in grado di bloccare la conferma delle nuove transazioni. Nel caso del PoS se qualcuno provasse a fare questo tipo di attacco dovrebbe acquistare il 51% dei token totali anziché il 51% del hashrate come nel caso del PoW. Chiaramente una crescita della domanda di queste proporzioni porterebbe a un aumento del prezzo dei token in maniera esponenziale. Un attacco di questo genere oltre a essere molto costoso, non porterebbe nessun tipo di guadagno per il malintenzionato, perché con un attacco di questo genere distruggerebbe la fiducia di quella blockchain e quindi inevitabilmente crollerebbe il valore del token.

Si può affermare che è molto più economico perché è un protocollo che non prevede costi di elettricità e di hardware per il mining.

Il PoS prevede penitenze, infatti da la possibilità di disincentivare economicamente validatori malevoli, distruggendo il loro stake in caso di condotte malevole.

Infine, l'ultima caratteristica è la lealtà questo perché i validatori sono incentivati a restare nella stessa blockchain. Se avessero intenzione di partecipare al PoS su un'altra blockchain, dovrebbero necessariamente sostituire i loro token. A differenza del PoS nel PoW si può cambiare blockchain ogni qualvolta la moneta che si sta minando non è più redditizia. [3]

Capitolo 2.12 Smart Contract

Nick Szabo nel 1994 ha definito lo smart contract come un “protocollo di transazione digitale che esegue i termini di un contratto”.

Lo Smart Contract è nato con l’obiettivo di soddisfare le condizioni che compongono un contratto in modo autonomo in modo tale di diminuire le probabilità che vengono intraprese azioni malevole e la necessità della fiducia verso gli intermediari. Gli intermediari tendono a essere non efficienti, lenti e onerosi.

I contratti sono dei documenti essenziali per rafforzare la fiducia tra le controparti che costituiscono una determinata transazione, sono la base di ogni attività di business.

Lo smart contract la maggior parte delle volte necessita di criptovalute come mezzo di scambio, ma non solo infatti può essere applicato al concetto di proprietà di beni fisici ovvero le smart property o nell’ambito dell’identità anche detta smart identity.

L’idea di smart contract si integra perfettamente nella logica che caratterizza la blockchain creando una formula vincente. All’interno di una blockchain uno smart contract è un programma che ha la stessa funzione di un contratto cartaceo, ma che viene eseguito su una blockchain.

Il contratto non è caratterizzato da vincoli legali, ma è un accordo che viene eseguito tramite il consenso del network. Questo lo rende applicabile in più nazioni con legislazioni differenti.

Infatti, gli smart contract si occupano di definire le regole che di conseguenza le controparti dovranno rispettare, tutto questo in modo decentralizzato.

Una volta che le regole preimpostate vengono soddisfatte, lo smart contract si occupa di eseguire in maniera autonoma delle azioni specifiche.

All’interno dello smart contract vige la regola del IFTT (if this then that). Quindi finche tutte le condizioni non vengono soddisfatte lo smart contract non eseguirà determinate azioni, il più delle volte sotto forma di transazioni.

Per comprendere meglio la logica con cui operano gli smart contract illustrerò degli esempi pratici che possono essere applicati a contratti che compongono la nostra vita quotidiana.

Potrebbe essere applicato per esempio all'interno di siti che si occupano di consegna a domicilio. Potrebbe essere possibile creare uno smart contract che applica uno sconto sul prezzo dell'ordine in base al tempo di consegna.

Se la consegna richiede meno di 20 minuti non viene applicato nessuno sconto. Se il tempo di consegna è tra i 20 e i 50 minuti viene applicato uno sconto del 40%. Se l'ordine arriva dopo 50 minuti lo sconto è del 50%

Queste sono le condizioni che caratterizzano lo smart contract. Nel momento in cui il cliente fa l'ordinazione viene richiesto al cliente di versare l'intero importo a un indirizzo, automaticamente verrà bloccato all'interno dello smart contract e solo una volta che l'ordine è arrivato a destinazione viene stabilito il prezzo effettivo da pagare sulla base del tempo di consegna. Tutto eseguito in maniera autonoma, trasparente e senza l'uso di intermediari.

Un altro esempio potrebbe essere applicato nel mondo del crowdfunding.

Immaginiamoci di creare un sito web che si occupa di raccogliere denaro per start up in fase di pre seed. Esattamente allo stesso modo di piattaforme come Kickstarter o MamaCrowd.

Un utente pubblica quindi un progetto, e stabilisce le regole dello smart contract, ovvero la quantità di denaro che vuole raccogliere da impiegare nella start up e il periodo di tempo entro il quale vuole raccogliere il denaro. Gli utenti investitori hanno la possibilità di partecipare al progetto inviando le criptovalute allo smart contract, che si occuperà di bloccarle fino a quando non verranno soddisfatte le regole impostate all'interno dello smart contract. Quindi il creatore del progetto non potrà raccogliere i fondi raccolti durante la campagna fino a quando l'obiettivo iniziale non viene raggiunto entro il tempo limite stabilito.

Una volta soddisfatte le condizioni lo smart contract sblocca i fondi automaticamente e li trasferisce al creatore del progetto. Nel caso in cui una o entrambe le condizioni non vengono soddisfatte i soldi raccolti vengono restituiti ai donatori.

Anche in questo caso non c'è bisogno di un intermediario e quindi vengono abbattuti dei costi di gestione grazie allo smart contract. [3]

Il concetto di smart contract è fondamentale al fine di contestualizzare questa tesi. Immaginiamoci la molteplicità di applicazioni possibili che potrebbero nascere dalla combinazione dello smart contract insieme all'internet of things.

In un futuro non molto lontano sarà possibile combinare queste due innovazioni nella vita di tutti i giorni. Immaginiamoci quando le macchine a guida autonoma potranno muoversi senza conducente all'interno della città, oppure una situazione in cui i sensori presenti in una macchina (Iot) individuano una ruota sgonfia, la macchina dotata di un wallet con criptovalute, potrebbe andare autonomamente dal meccanico per farla rigonfiare. In questo caso la condizione dello smart contract è che la ruota sgonfia deve ritornare ai livelli di pressione standard, una volta che il sensore di pressione delle gomme stabilisce che la gomma è stata gonfiata lo smart contract sblocca i soldi che vengono rilasciati sul wallet del gommista. In questo caso lo smart contract è indispensabile perché è un contratto che può essere redatto da una macchina, si parla della prima tipologia di contratti che può essere creato per accordare una macchina con una macchina. Al momento sembra fantascienza, ma si parla di tecnologie già presenti sul mercato, (Autopilot Tesla e smart contract) e devono solo essere perfezionate e applicate alla nostra quotidianità. L'autovettura inoltre potrebbe pagare l'assicurazione autonomamente e l'assicurazione potrebbe monitorare grazie ai sensori della macchina la condotta del conducente in caso di incidente.

Ho fatto solo un breve accenno delle funzionalità che nascono dalla combinazione dell'internet of things e dello smart contract per ricalcare fin da subito l'importanza dello smart contract all'interno della blockchain. La blockchain e più nello specifico gli smart contract potrebbero rivoluzionare anche il mondo del trading. Uno dei problemi principali è la liquidazione dei titoli azionari che ha un processo di verifiche molto lungo e la burocrazia può richiedere numerosi giorni a causa della regolamentazione e degli intermediari coinvolti. La blockchain potrebbe rendere queste operazioni più veloci rafforzandone la sicurezza e rendendole meno costose eliminando i numerosi intermediari.

Johan Toll, Nasdaq, Head of Blockchain Product Management, afferma che:

"C'è una possibilità molto concreta che tutte le transazioni societarie verranno spostate su blockchain."

Nasdaq è il secondo stock exchange al mondo per market cap, sta cercando ambiti di applicazione della blockchain in ambito di servizi finanziari. L'immutabilità delle transazioni potrebbe incrementare l'efficienza del sistema per la liquidazione di asset, trasferimenti in denaro, ma anche per la gestione dei collaterali.
Link è una piattaforma sperimentale che ha creato Nasdaq per testare la gestione di quote societarie di compagnie private all'interno del Nasdaq private Market. [3]

Capitolo 2.13 Vantaggi della Blockchain in ambiti cross-industry

Una piattaforma DLT (Distributed Ledger Technology) offre numerosi vantaggi alle imprese. Riassumendo le principali peculiarità che caratterizzano la blockchain poi potremmo vedere in che modo possono essere applicate nell'ambito cross-industry:

- Sicurezza dovuta dall'utilizzo di tecniche criptografiche. La crittografia utilizzata all'interno della blockchain è di tipo avanzato e permette di incrementare la sicurezza e l'integrità dei dati.
- Immutabilità.
- Nessun tipo di intermediario.
- Programmabilità della criptovaluta .
- Utilizzo di smart contract. Grazie a questo tipo di contratto è possibile eliminare la figura dell'intermediario in determinate transazioni e si crea la possibilità di creare un contratto che interagisce con il mondo esterno tramite l'IoT senza la necessità dell'intervento umano.
- Interazione tra blockchain e mondo esterno. Ovvero l'utilizzo di sensori e di software che si occupano di processare le condizioni degli smart contract per verificare il rispetto delle condizioni (detti oracoli).
- Automazione di interi processi.

- Governance decentralizzata e distribuita. L'affidabilità del sistema è garantita dalla cooperazione tra macchine e essere umani che interagiscono tra di loro al fine di rispettare le regole. L'intero processo è gestito da un algoritmo open source, ottenendo cosi trasparenza.
- Riduzione dei tempi per le procedure burocratiche.

Questo insieme di caratteristiche uniche che caratterizzano la blockchain si traducono in termini di vantaggi per l'impresa. Il più rilevante è l'ottimizzazione operativa. Infatti, diminuisce l'intervento manuale e vengono automatizzati maggiormente determinate azioni, riducendo il rischio di incombere nell'errore umano.

Si ottengono vantaggi in termini di gestione organizzativa. La blockchain snellirebbe le procedure burocratiche diminuendo cosi i tempi correlati. Potrebbe inoltre risolvere il problema della corruzione e restituirebbe il potere alla comunità.

Una maggiore trasparenza e quindi come conseguenza una diminuzione di frodi e contraffazioni. Le autorità possono vigilare più efficientemente sui processi.

Ultimo vantaggio è la riduzione di affidamento alla controparte, questo perché non è più necessaria la fiducia verso la controparte per l'adempimento di obblighi, grazie alla figura dello smart contract che permette di creare accordi in un ambiente condiviso e trasparente.

La blockchain può essere applicata in svariate industrie. Partendo dall'Agrifood, infatti molte catene di supermercati stanno adottando la blockchain per consentire una maggiore tracciabilità dei prodotti. Assicurazioni, pensiamo all'esempio della macchina che può pagarsi l'assicurazione da sola. Banking e Finance e nelle sharing economy. Ma anche in ambito pubblico molte nazioni stanno adottando la blockchain per il Welfare oppure per l'Identità digitale. Viene adottata anche per il Turismo, Trasporti e Utilities, per le Donazioni e Digital Marketing. [3]

Capitolo 2.14 Rischi e svantaggi della Blockchain

Il primo rischio connesso alla blockchain è dovuto alla privacy in quanto ogni transazione è visibile da tutti, anche se sono visibili solo chiavi pubbliche degli indirizzi su cui vengono effettuate le transazioni rimane comunque visibile l'importo della transazione, si sta quindi pensando di crittografare i dati delle transazioni. Crittografare i dati potrebbe però portare a un degrado delle performance e anche il problema dovuto dal totale anonimato delle transazioni.

Il Proof of Work ha un modello d'incentivazione che premia il miner solo quando il compito è svolto correttamente (ovvero approvato dagli altri nodi) cosi facendo sarebbe antieconomico per il miner modificare i blocchi validati precedentemente. Ma oltre a questo sul PoW esiste anche un altro tipo di modello di retribuzione che si basa sulle commissioni, che permette al miner di essere ulteriormente ricompensato se presenta per primo la PoW.

I nodi validatori tenderanno sempre a scegliere i blocchi che contengono retribuzioni maggiori, creando cosi una disparità di trattamento per gli utenti che spenderanno meno sulle commissioni, che saranno costretti ad attendere anche per ore per far confermare le loro transazioni. Specialmente in periodi in cui il network è congestionato i miners decideranno di inserire nei loro blocchi le transazioni che prevedono commissioni più alte. [2]

Immaginiamoci se nelle case le serrature fossero connesse alla blockchain. Nel caso in cui la casa fosse in affitto si potrebbe creare uno smart contract (teoricamente) in cui qualora non fosse pagato l'affitto le serrature si bloccano. Oppure si potrebbe pensare al fatto che se le automobili superassero il limite di velocità potrebbero essere multate istantaneamente. Oppure un computer domestico che si occupa di pagare bollette, spese condominiali etc. Vorremo veramente tutto questo controllo sui nostri pagamenti? Cosi facendo ci troveremo obbligati a rispettare le regole della società perché saremmo costantemente monitorati da sensori e software collegati a smart contract che ci penalizzerebbero istantaneamente nel caso di condotte non conforme alle regole. Vivere in un mondo regolato da contratti digitali sicuramente sarebbe un bene per la collettività ma questo ci farebbe sentire meno liberi o più sicuri?

Gli smart contract baseranno le loro scelte in base alle regole che sono state inserite all'interno dal creatore del contratto. Quindi al versificarsi di determinate condizioni risponderanno sempre allo stesso modo. L'umano invece può reagire in maniera completamente differente in situazioni apparentemente uguali. Questo però non è necessariamente un errore, pensiamo al caso in cui dobbiamo scegliere tra due candidati per un posto lavorativo, un computer sceglierebbe quello che soddisfa maggiormente i criteri di ricerca impostati dall'azienda, un recruiter invece potrebbe scegliere un candidato meno conforme ai parametri di ricerca per quel posto di lavoro ma con altre doti che solo un umano potrebbe percepire. L'umano si basa sul buon senso e l'esperienza, un software non ha modo di giudicare le situazioni con parametri differenti da quelli impostati nello smart contract.

Oppure, per quale ragione l'inquilino non ha pagato l'affitto? Un umano può sentire le motivazioni e in base alle risposte decidere se sfrattare o meno l'inquilino, (anche se non è molto facile, il mio è solo un esempio teorico) il software no. Per lo smart contract non fa differenza il motivo per cui non si paga l'affitto quindi in un periodo come quello che abbiamo appena attraversato per il covid 19 quanta gente si sarebbe trovata senza una casa a causa della disoccupazione. Ricordiamo che gli smart contract sono immutabili e decentralizzati, questo vuol dire che non possono essere modificati in nessun modo e i nodi della rete verificheranno che le condizioni non vengono modificate.

Decidendo di attribuire responsabilità a un codice informatico sacrifichiamo la nostra facoltà e capacità di dare un giudizio su situazioni che apparentemente potrebbero sembrare uguali. Eliminando la figura dell'intermediario e affidandoci ai benefici dell'automazione si crea un altro problema; come fare se il software presenta dei bug? Prima che l'errore viene rilevato potrebbero esserci diversi danni. Le vittime a chi dovrebbero rivolgersi per il risarcimento?

La blockchain è veramente inattaccabile? Dipende da quanti partecipanti ci sono nella rete. Se è distribuita tra decine di migliaia di partecipanti allora sarà quasi impossibile modificarla perché come abbiamo visto nel capitolo sul PoW e PoS, in quanto sarebbe necessario il 51% dell'hashrate (di criptovalute di quella determinata blockchain nel caso di PoS) per modificare le informazioni.

In caso di blockchain private il discorso cambia in quanto il registro viene conservato su pochi supercomputer e solo poche persone possono accedere, il rischio di manomissione dei dati in questo caso cresce in maniera esponenziale.

Per concludere il capitolo prendiamo in esame la trasparenza e la sicurezza della blockchain. Il registro è effettivamente visibile a tutti quelli che vogliono partecipare alla blockchain ed è anche immutabile.

Ma c'è un problema che neanche la blockchain può risolvere ovvero gli imbrogli.

Molte catene di supermercati stanno introducendo il registro distribuito all'interno dell'azienda al fine di rendere più tracciabili i loro prodotti consentendo al cliente di avere accesso a un maggior numero di informazioni riguardo la provenienza del prodotto e degli ingredienti che sono stati utilizzati qualora provengono da società terze. Come ha scritto Kai Stinchconbe in un articolo che è stato pubblicato su Medium ha affermato che:

"I sistemi legati alla blockchain non rendono magicamente accurati i dati contenuti o affidabili le persone che li inseriscono. Semplicemente, ti permettono di controllare se qualcosa è stato manomesso. Una persona che spruzza pesticidi su un mango può comunque inserire nella blockchain dei dati che invece mostrano come il suo mango sia biologico. Un governo corrotto può comunque creare un sistema di blockchain per il voto digitale e inserire milioni di voti falsi".

Se la blockchain è decentralizzata sufficientemente i dati non possono essere manomessi, ma ciò non garantisce che i dati inseriti sono veritieri. [10]

Capitolo 3 Iot: Definizione, Nascita e caratteristiche

L'internet of things (IoT) possiamo vederla come una rete di oggetti interconnessi tra di loro, che possono raccogliere e scambiare informazioni attraverso l'utilizzo di internet in maniera del tutto autonoma.
Negli ultimi anni è un fenomeno di cui si parla molto e si sta cominciando a apprezzare sempre di più grazie alle diverse innovazioni tecnologiche fatte in diversi ambiti.
L'idea di connettere oggetti diversi da computer a internet nasce nel1982 quando un distributore di Coca Cola situato nella Carnagie Mellon University poteva inviare informazione riguardanti la temperatura delle bibite all'interno e sulle quantità rimanenti. Nel 1990 fu inventato un tostapane da John Romkey e Simon Hackett che comunicava con gli utenti tramite internet, gli utenti potevano scegliere la temperatura grazie a un'applicazione. L'anno successivo perfezionarono la loro invenzione automatizzando l'inserimento del pane tramite un comando apposito sull'applicazione.
Fu il primo oggetto in commercio dotato di questo tipo di tecnologia.
Il maggior contributo nel mondo dell'IoT va attribuito all'utilizzo dei sensori RFID (Radio-Frequency IDentification) che permettono di collegare le informazioni raccolte dai sensori a internet, insieme alla diffusione esponenziale di internet grazie al World Wide Web in cui nacque il protocollo http, il linguaggio HTML e la realizzazione dei primi browser. Gli utenti passano da 40 milioni nel 1995 a più di 400 milioni nel 2000.
Pare che Kevin Ashton abbia coniato il termine "internet of things" nel 1999 durante una presentazione a Procter & Gamble, stava presentando l'idea di utilizzare i sensori RFID per collezionare dati tramite internet al fine di incrementare l'efficienza della catena di gestione di approvvigionamenti. [11]
In un articolo dell'RFID Journal Kevin Ashton scrive "Se avessimo computer in grado di conoscere tutto ciò che c'è da sapere sulle cose, utilizzando dati raccolti senza alcun aiuto da parte nostra, saremmo in grado di monitorare e conteggiare ogni cosa e di ridurre notevolmente sprechi, perdite e costi. Potremmo sapere quando le cose devono essere sostituite, riparate o richiamate, e se sono fresche o hanno superato il loro momento migliore. Abbiamo bisogno di potenziare i computer in modo che siano in grado di raccogliere

informazioni autonomamente, in modo che possano vedere, ascoltare e annusare il mondo. La tecnologia RFID e altre tipologie di sensori consentono ai computer di osservare, identificare e comprendere il mondo, superando il vincolo dell'inserimento delle informazioni da parte dell'uomo". [12]

Capitolo 3.1 Sensori

Il computer nell'immaginazione collettiva rappresenta un'estensione del cervello umano, che può svolgere funzioni dettate da precisi comandi impartiti dall'uomo. Internet ha dato la possibilità di creare un ecosistema all'interno del quale è possibile scambiare informazioni e incrementare la capacità di analisi. IoT attribuisce al "cervello digitale" dei veri e propri sensi ovvero dei sensori che sono in grado di collezionare informazioni nell'ambiente che lo circondano.

I sensori e l'RFID e tutti gli altri dispositivi che permettono di codificare dati sull'ambiente che li circonda sono ciò che da la possibilità ai computer di analizzare l'ambiente e di eseguire funzioni tramite gli input esterni.

Il primo RFID ovvero identificazione a radiofrequenza è stato brevettato da Charles Walton nel 1983. RFID è un tipo di tecnologia che permette di identificare e memorizzare automaticamente le informazioni che riguardano oggetti o soggetti. I dati vengono salvati tramite dei tag che possono essere attivi o passivi e vengono comunicati tramite onde radio e ricevuti da apparecchi fissi o portatiti detti reader.

I tag attivi sono dotati di batteria e possono inviare e ricevere risposte in un raggio d'azione non maggiore a 200 metri. I tag passivi invece sono privi di batteria, in questo caso comunica tramite onde radio in una distanza nettamente minore (un esempio può essere quello del sensore antitaccheggio oppure il passaporto italiano che all'interno contiene un tag passivo).

Ultimamente si è diffusa una tipologia di RFID detta NFC ovvero comunicazione in prossimità. Sostanzialmente è un'evoluzione della tecnologia RFID che consente una comunicazione bidirezionale a

raggio ridotto. Questo tipo di tecnologia la ritroviamo nelle carte contactless e nella maggior parte degli smartphone.

I sensori e i trasduttori riescono a misurare alcuni parametri di grandezza in prossimità (ad esempio la temperatura, battiti cardiaci, luminosità etc). Questo tipo di sensori negli ultimi anni sono stati utilizzati sempre di più anche in ambito privato all'interno delle case come vedremo più avanti nell'ambito delle smart home. Infatti, in ambito privato vengono utilizzati spesso per rilevare incendi e misurare l'umidità. Vengono utilizzati anche i wearable devices che sono oggetti sempre più presenti nella nostra vita che permettono di rilevare parametri biofisici.

I sensori al di fuori dell'ambito privato vengono utilizzati anche nelle industrie per monitorare parametri come la misurazione della qualità dell'aria, monitoraggio ambientale, rilevamento di temperature etc.

Per concludere, le Webcam e le IP camera sono dispositivi che possono attribuire un maggior grado di precisione ai dati raccolti. Con questi dispositivi è possibile rilevare movimenti fino ad arrivare al riconoscimento facciale.

Queste sono le principali categorie di sensori che raccolgono informazioni sugli oggetti e soggetti che li circondano. Se pensiamo a uno smartphone è dotato di NFC, bluethoot, WIFI,4G e riconoscimento facciale o di impronte digitali, è come se il telefono fosse dotato di sensi che gli consentono di percepire l'ambiente esterno, con chi sta comunicando e dove si trova.

Ma ogni telefono non è solo infatti fa parte di una community di telefoni che interagiscono tra di loro per diversi scopi. Uno di questi è l'algoritmo di Google che consente di raccogliere informazioni precise in tempo reale sul traffico dagli utenti che stanno utilizzando Google Maps. Processando le informazioni relative alla velocità dei diversi veicoli e il numero di veicoli presenti, Google può fornire informazioni accurate sul traffico. In questo caso è l'uomo a riceve i dati presentati da Google e sarà il guidatore a decidere se cambiare percorso. In questo caso il flusso informativo è detto Machine-to-People o "M2P". I dati vengono quindi raccolti da dispositivi e successivamente elaborati da umani.

Possiamo individuarne altri due tipi: P2P (people to people) e M2M (machine to machine). [11]

Capitolo 3.2 Cloud computing, Big Data, Machine learning

Il cloud computing è il termine con cui si indicano le tecnologie che si occupano di processare, archiviare e salvare dati grazie a hardware e software distribuiti all'interno della rete.
Un servizio cloud può essere utilizzato nel caso in cui tramite i dispositivi si utilizzano risorse o servizi attraverso la rete.
I servizi cloud ci permettono di avere un computer virtuale con una potenza, memoria variabile in base alle proprie preferenze. Generalmente viene utilizzato come servizio e molto spesso comporta un costo che varia in base alle specifiche richieste. Alcuni esempi possono essere i servizi icloud di Apple o Google drive.
Ci sono tre tipi di categorie di servizi cloud.
La prima categoria riguarda l'utilizzo di software che vengono utilizzati come utente finale, ad esempio la posta elettronica via web.
La seconda prevede l'utilizzo di software in cui è possibile amministrarne la configurazione. Un esempio sono le aziende che acquistano un servizio di posta da un provider e configura la piattaforma creando le caselle per i suoi dipendenti.
La terza categoria è rappresentata in cui il servizio è un server virtuale in cui è possibile installare il software di sistema. In questo caso il servizio sarà un sistema hardware virtuale il cui costo varia in base alla configurazione.
Il cloud computing è un concetto fondamentale ai fini di questa tesi in quanto è una tecnologia che la blockchain sta rivoluzionando. Questo perché tramite le caratteristiche uniche della blockchain come la crittografia e la decentralizzazione è possibile salvare le informazioni in cloud in maniera molto più sicura. Infatti, uno dei problemi principali di salvare dati in cloud centralizzati è che possono essere facilmente hackerati.
Big Data: la digitalizzazione dei servizi e dei processi che si sono sviluppati anche grazie al cloud computing, ma anche la crescita continua del network dei social media e social network e anche la enorme crescita dell'IoT, generano un enorme quantità di informazioni digitali.

Per far fronte a questo flusso enorme di dati è nato il big data che è caratterizzato dalle "4V" ovvero velocità, volume, varietà e veridicità. Andando su Webfx.com è possibile vedere in tempo reale quanti dati vengono caricati in internet. Per dare un'idea del volume e della velocità con cui vengono caricati i dati, in un secondo vengono caricati 24 mila gigabyte, in un mese 1 miliardo di gigabyte.
I diversi tipi di informazioni si muovono in volumi enormi e ad una velocità impressionante.
La varietà caratterizza i big data in quanto i dati vengono da una moltitudine di sorgenti diverse.
La veridicità è una caratteristica che non si può dare per certa in quanto è importante selezionare con accuratezza la fonte da cui l'algoritmo raccoglie i dati.
Il machine learning è un ramo dell'informatica che si colloca nel campo di studi dell'intelligenza artificiale in cui gli algoritmi dettano regole nel modo in cui devono essere letti e interpretati i dati al fine di trovare soluzioni a problemi connessi ai dati da analizzare. Grazie alla grande quantità di dati immagazzinati negli ultimi anni il machine learning sta riscontrando molto successo. Le applicazioni machine learning raccolgono i dati e li utilizzano per perfezionare i dati generati negli scenari successivi, per questo motivo il machine learning è strettamente collegato con il big data e il cloud computing. [11]

Capitolo 3.3 Funzionamento e impiego

L'IoT è una rete di dispositivi online che hanno lo scopo di immagazzinare e scambiare dati tramite l'utilizzo di sensori e altre tecnologie. L'unico requisito per entrare a far parte dell'IoT è che l'oggetto sia dotato di un circuito elettrico che può essere collegato in rete. Quindi ad uso privato può essere ad esempio un'automobile, un frigorifero, una televisione e qualunque tipologia di dispositivo che sia in grado di comunicare con la rete. Per quanto riguarda le industrie può essere usato per macchinari, impianti, l'automazione di un processo e molto altro. Nel settore pubblico l'IoT viene utilizzato in progetti collegati al concetto di smart city ma anche nei trasporti, rilevare le informazioni riguardanti il traffico, l'aria etc.

Questi dispositivi che raccolgono costantemente dati, devono trasmetterli alla rete per poi essere memorizzati il più delle volte in cloud. I dati vengono utilizzati da algoritmi come ad esempio quelli del machine learning con lo scopo di elaborare soluzioni sempre più efficaci.

Questi dati e le soluzioni riportate possono essere usate dall'umano come supporto ai propri processi decisionali (machine-to-people) o da altri dispositivi (machine-to-machine). Gartner sostiene che a fine 2017 erano 8,4 miliardi i dispositivi IoT connessi a internet, con una crescita di 2 miliardi in più rispetto all'anno precedente. [11] Nel 2020 ci sono oltre 9.9 miliardi di dispositivi connessi con IoT e si prevede che i dispositivi connessi con IoT salgono a 21.5 miliardi. [13]

Secondo un report di GrowthEnabler i settori in cui si adotta l'IoT si possono dividere in due macro-aree: Quella legata alle persone e quella collegata alle imprese.

Per quanto riguarda l'area collegata alle persone viene utilizzata prevalentemente per soluzioni riguardanti la smart home. Quindi tutti i dispositivi presenti nella casa che sono collegati a un WI Fi con cui è possibile interagire tramite un'app sullo smartphone. Ma di recente si stanno diffondendo molto anche i wearable device che fanno parte anche essi di questa categoria. I wearable devices sono pensati per monitorare le attività svolte dalla persona che li indossa al fine di offrire soluzioni per migliorare le proprie abitudini.

In conclusione, della prima macro-area ci sono i sistemi a guida autonoma o assistita.

La macro-area collegata alle industrie è principalmente collegata a fini commerciali come la pubblicità che si basa sulla prossimità, il monitoraggio del comportamento d'acquisto da parte dei consumatori all'interno dei negozi. L'IoT può essere utilizzato anche per incrementare la sostenibilità dell'azienda migliorando l'efficienza e la gestione energetica della stessa. I sensori vengono utilizzati per monitorare i macchinari al fine di prevedere eventuali guasti e quindi procedere subito alla manutenzione.

La smart city è un settore che è in rapida espansione. Grazie all'utilizzo di dispositivi IoT e i big data si è creata la possibilità di rivoluzionare i servizi pubblici come la gestione del traffico, la ripartizione dell'acqua, il monitoraggio ambientale ma anche per aumentare la sicurezza dei cittadini da furti. [11]

Le due macro aree in cui è possibile raggruppare le soluzioni IoT	
Consumer segment	**Business segment**
Smart home e domotica Wearable device Dispositivi sanitari Guida autonoma o assistita (Automotive)	Smart city Smart utilities & Energy Sanità IoT industriale Proximity-based advertising

Figura 4. (immagine presa da Za, S. (2018). Internet of Things: Persone, organizzazioni e società 4.0. [ebook] LUISS University Press)

Capitolo 4: Blockchain per l'IoT

Come abbiamo visto nel capitolo precedente l'IoT richiede che una serie di dispositivi tra loro collegati, i quali raccolgono dati che vengono salvati in cloud e grazie all'utilizzo dei big data possono essere utilizzati per trovare soluzioni intelligenti grazie al machine learning.

La blockchain invece come abbiamo visto nel secondo capitolo è decentrata, trasparente, immutabile, open source, autonoma, anonima. In poco tempo si è capito dell'enorme potenziale che poteva derivare dalla combinazione di queste due tecnologie rivoluzionarie.

La caratteristica principale alla base dell'IoT è la gestione di un enorme flusso di dati che viaggia a altissima velocità. Trasportando informazioni riguardanti la salute delle persone, dati finanziari, informazioni confidenziali per industrie, governi e persone.

Proprio per la sensibilità dei dati trasportati è nata l'idea di far viaggiare questi dati nel cloud della blockchain in modalità peer-to-peer minimizzando cosi i rischi di attacchi da hacker ma aumentando anche la velocità e connettività. Molte aziende leader nel campo tecnologico IoT hanno già adottato questa tecnologia tra cui Samsung e IBM che hanno annunciato la loro piattaforma IoT Blockchain based, ADEPT.

Bisogna sottolineare che questa non è l'unica svolta che può nascere dalla combinazione dell'IoT con la blockchain. Se si attribuisse a questi oggetti un wallet virtuale con all'interno criptovalute, e se attribuissimo a questi oggetti la capacità di fare acquisti per conto nostro che impatto avrebbe sulle nostre vite in termini di efficienza e di tempo? Questo tipo di automazione indubbiamente ci permetterebbe di risparmiare molto tempo in task quotidiane noiose regalandoci così più tempo da impiegare per svolgere le azioni che vogliamo veramente portare a termine. IBM e Samsung hanno descritto come una blockchain potrebbe permettere alla lavatrice di essere semi-indipendente, in grado di autogestire la fornitura di detersivo, ammorbidente ma anche l'avvio e lo spegnimento di programmi e la manutenzione, interagendo con gli altri dispositivi della smart home. Questo meccanismo potrebbe essere applicato anche in un impianto petrolifero per regolare le funzionalità dell'impianto in base alle condizioni metereologiche [14]. Il mondo si sta spingendo ogni giorno di più in questa direzione, ma come ogni rivoluzione, il processo non accade in un

giorno. Solo con il tempo riusciremo a fidarci delle macchine a tal punto da concedergli una gestione così totalitaria e" autonoma".

In questo capitolo analizzeremo i settori di impiego più rilevanti della blockchain e IoT e verranno analizzate le opportunità e gli scenari futuri, ma anche le maggiori criticità che derivano da queste tecnologie su cui bisognerà implementare delle soluzioni valide. A fine capitolo sarà preso a oggetto un caso studio su l'accordo tra la tedesca MXC Foundation e il governo della China Shanghai Yangpu per l'adozione dello smart city IoT standard MXProtocol che permette una gestione sicura dei dati delle città intelligenti, considerando tutti i pro e contro che potrebbero derivare dall'implementazione di questa tecnologia nella città di Shanghai.

Capitolo 4.1 Smart City

Come abbiamo visto precedentemente nel settore pubblico il concetto di smart city è il concetto più rilevante. Smart city è la definizione di una città che tramite l'utilizzo di sensori e dispositivi si pone il fine di raccogliere dati da impiegare per una gestione più efficiente delle risorse. Per esempio, queste informazioni possono essere utilizzate per gestire il traffico, centrali elettriche, reti idriche, le scuole, gli ospedali, gestione dei rifiuti, e molte altre attività con la finalità di aumentare la qualità dei servizi percepiti dai cittadini, innalzando cosi il livello generale di benessere.

Nel Queensland per esempio per migliorare il transito di mezzi di emergenza (ambulanze, polizia etc) se coinvolti in operazioni di soccorso avranno sempre la luce verde a tutti i semafori che troveranno lungo il tragitto. Questo sistema è detto "Emergency Vehicle Piority".

Un'altra soluzione intelligente è stata adottata a Barcellona. Il 40% del traffico nel centro della città era causato da persone che cercavano parcheggio. Questa ricerca causava rumore, congestione e inquinamento.

Per risolvere il problema sono stati installati dei sensori nelle aree di sosta con la finalità di indicare i parcheggi disponibili, inoltre è anche possibile pagare il parcheggio qualora sia a pagamento. Questo tipo di soluzione ha portato a una riduzione di emissioni di anidride carbonica, inquinamento acustico e ambientale.
Il car sharing è un'altra iniziativa valida in ambito di smart city che si è diffusa molto rapidamente. La possibilità di utilizzare un veicolo in condivisione sbloccabile tramite un'app, affiancato alla rapida diffusione di mezzi elettrici porta a una diminuzione di mezzi in circolazione, riducendo cosi le emissioni e il traffico. Si stima che in 20 anni i mezzi di trasporto pubblici saranno completamente elettrici e in condivisione ma anche a guida autonoma.
In ambito medico l'IoT viene utilizzato per diversi obiettivi come ridurre gli errori, ma anche per gestire efficientemente il paziente e migliorare la gestione delle risorse.
Al fine di ridurre gli errori, il Singeland Hospital in Olanda utilizza una serie di sensori per monitorare la salute dei pazienti, permettendo così da ridurre i tempi per le diagnosi e di prescrizione per i farmaci adatti. Il monitoraggio dei pazienti che viene fatto in tempo reale limita la necessita di interventi da parte dei medici riducendo così i costi collegati alle visite a domicilio.
Ma l'IoT può essere utilizzato anche per monitorare la fornitura degli armadi sanitari, che controlleranno costantemente l'inventario in maniera del tutto indipendente.
Gli smart glasses invece (che sono un esempio di wearable devices) permettono di utilizzare la realtà aumentata al fine di raccogliere informazioni dettagliate sull'operato dei medici, che potranno decidere di condividerlo con i loro colleghi, che potranno eventualmente fornire un consulto da remoto in tempo reale. [11]
La prima Smart city basata sulla tecnologia Blockchain è nata nel distretto di Daimaruyu a Tokyo, in Giappone nel 2018.
Oltre 120 ettari sono stati bonificati per essere trasformati in una città intelligente, tramite la combinazione della Blockchain e l'Internet of Things. La tecnologia adottata è di tipo open source ed è stata creata dalla Linux Foundation. Si tratta di una blockchain che si basa su una serie di regole specifiche che permettono di validare l'ingresso di membri all'interno della blockchain e autorizzare le transazioni. Il colosso tecnologico

Fujitsu si è occupato di creare il software Virtuora DX, che permette tramite un servizio cloud ai partecipanti di condividere dati e smart contract.

A Daimaruyu ci sono 106 grattacieli, più di 4000 uffici, oltre 40 mila ristoranti e 90 mila negozi. Il distretto ha 13 stazioni ferroviarie e metro e 16 tra le più grandi aziende hanno deciso di avere lì la loro sede principale. [15] Tutti i dati che provengono dai sensori Iot dei bus, da parte dei negozi in merito alla disponibilità dei prodotti, dai ristoratori riguardo i tavoli disponibili o dalle aziende vengono condivise grazie all'infrastruttura innovativa del distretto. Chi si collega alla rete blockchain di Fujitsu potrà essere autorizzato o meno a accedere alla banca dati del distretto. Più il volume dei dati cresce e più saranno le informazioni e i servizi che ci saranno a disposizione.

L'internet of Things può portare con sé problemi sulla sicurezza della gestione dei dati, ma grazie all'adozione della blockchain i dati possono viaggiare in maniera sicura anche in un sistema complesso come quello di una città.

Secondo i dati diffusi da IDC, gli stati spenderanno nel 2021 45,3 miliardi di dollari in progetti di smart city, questo comprenderà anche l'utilizzo della blockchain. [16]

Questo tipo di tecnologia può essere utilizzata per assegnare un'identità digitale al cittadino in modo tale da permettergli di accedere a una rete interconnessa. Così facendo il cittadino può accedere a una serie di servizi di tipo professionale, governativo e privato come l'accesso a prestiti bancari o la gestione della propria proprietà o il pagamento delle tasse in estrema velocità e facilità.

Capitolo 4.2 Smart Home

Smart TV, condizionatori, lavatrici, macchine del caffè, serrature, sono solo alcuni tipi di elettrodomestici che possono essere interconnessi tra loro tramite la rete.

Sensori e dispositivi a uso domestico aumentano la sicurezza dell'abitazione ma riducono anche i consumi e comportano un'ottimizzazione della gestione delle risorse.

I sistemi più moderni solitamente presentano un “gateway” ovvero un hub centrale tramite il quale è possibile controllare il sistema anche in remoto tramite internet. Negli ultimi anni sono arrivati sul mercato anche dispositivi intelligenti con cui possiamo interagire tramite l’utilizzo della voce, riuscendo così a gestire i vari componenti della smart home.
In questo campo il leader è Amazon, a seguire Google e infine Apple.
Questo tipo di assistente virtuale è dotato di un microfono e di altoparlanti che gli permettono di interagire con il mondo esterno tramite comandi impartiti verbalmente. Questo è un dispositivo pensato per essere un vero e proprio assistente virtuale, infatti è possibile richiedere la lista degli impegni giornalieri, avviare la riproduzione di una canzone, richiedere il meteo e molto altro. La caratteristica da sottolineare è che impara sempre di più in seguito all’utilizzo e grazie all’algoritmo migliora costantemente l’interpretazione delle richieste. L’assistente virtuale è un esempio di machine learning.
Oggigiorno stanno arrivando sul mercato anche dispositivi per la casa dotati di algoritmi di apprendimento come ad esempio aspirapolveri che sono in grado di tornare alla loro postazione una volta che è terminato il loro utilizzo. Nissan ha applicato il software di parcheggio in autonomia delle sue macchine elettriche, per consentire a oggetti (tavoli, sedie, pantofole) di ritornare al loro “parcheggio” dopo l’utilizzo.
Questo tipo di tecnologia è già in uso all’hotel ProPilot Park Ryokan in Giappone.

Capitolo 4.3 Self-driving car

La self driving car ovvero un’autovettura autonoma è in grado di rilevare l’ambiente che la circonda e agire in maniera del tutto indipendente, senza bisogno dell’aiuto umano. Questo tipo di autovetture sono in grado di percepire l’ambiente esterno tramite l’utilizzo di Radar, Lidar, GPS e sensori. I sensori comunicano con un software che agirà secondo le condizioni esterne trasmesse.
La SAE (Society of Automotive Engineers) ha diviso le auto a guida autonoma in 6 livelli di autonomia.

Il livello 0: sono le auto che non sono dotate di nessun tipo di autonomia. Quindi sarà il conducente a guidare e l'auto interviene solo in alcune situazioni.
Il Livello 1: a questo livello i sensori della macchina possono intervenire con correzioni di piccola entità sullo sterzo ad' esempio per mantenere l'auto sulla corsia.
Il livello 2: Da questo livello si comincia a parlare di veicoli che hanno un certo grado di autonomia. In questo livello l'auto è in grado di controllare l'accelerazione e anche la frenata. L'auto è dotata di sistemi anticollisione
Il livello 3: In questo livello l'auto è in grado di guidare in autonomia. Può gestire l'accelerazione, la direzione e la frenata. In questo caso sarà richiesto l'intervento umano solo in caso in determinate situazioni in cui la guida autonoma non è permessa. Quindi chi guida avrà il solo compito di osservare la strada.
Il livello 4: presenta lo stesso grado di indipendenza del livello 3 ma in aggiunta l'auto è in grado di monitorare le condizioni del traffico e tramite il machine learning è in grado di prendere decisioni in base alle situazioni più tipiche dovute dal traffico.
Il livello 5: Questo è il grado più elevato di autonomia per un'auto. Si tratta infatti di automazione completa. A questo livello l'intervento umano non è necessario, quindi i passeggeri hanno la possibilità di disinteressarsi alla guida durante il tragitto. Le auto di questo livello si trovano in una situazione ambigua per quanto riguarda la loro libera circolazione a causa di buchi legislativi e la necessità di un aggiornamento delle infrastrutture. [17]

Si stanno inoltre sviluppando una moltitudine di applicazioni della blockchain all'interno dell'automotive. La prima applicazione la troviamo nell'ambito dell'identità dell'autovettura. BMW ma anche altre case automobilistiche si stanno occupando di creare una sorta di passaporto digitale dell'auto tramite la blockchain.
Nel momento in cui vogliamo vendere un'auto usata è necessario sapere quanti chilometri ha percorso, se ha avuto incidenti in passato e infine se il venditore ha rispettato in maniera regolare gli intervalli di

manutenzione. Queste informazioni possono essere facilmente falsificate, ma tramite la blockchain si può avere la garanzia che le informazioni non siano state manipolate.

Applicazioni come VerifyCar (che è ancora in via di sviluppo), danno la possibilità di trovare le risposte a queste domande attingendo alla blockchain. Il cliente può accedere a queste informazioni grazie all'app, infatti scansionando il QR Code presente sul dispositivo del venditore si potranno verificare tutte le informazioni dell'autovettura. In questo modo si può essere sicuri che le informazioni raccolte siano sicure e plausibili.

La blockchain può essere utilizzata inoltre per tracciare la fonte delle materie prime utilizzate nella catena di montaggio. In fase si assemblamento vengono utilizzati materiali provenienti da decine di intermediari, grazie alla blockchain è possibile tracciare il percorso delle materie prime. In questo modo una raffineria ha la possibilità di mostrare la provenienza delle sue materie prime.

Infine, grazie alla blockchain è possibile ricaricare le auto elettriche in maniera più semplice. Questo perché i proprietari di auto elettriche molto spesso riscontrano difficolta a causa della molteplicità di contratti differenti che sono collegati alle colonnine di ricarica. Si sta pensando invece di far interagire l'auto direttamente con la colonnina di ricarica redigendo uno smart contract apposito, rendendo tutto molto più semplice. [18]

A questo proposito mi vengono in mente molti altri ambiti di applicazione derivanti dall'attribuzione di un wallet a un'autovettura a guida autonoma che ha la capacità di creare smart contract con l'ambiente che lo circonda. La macchina a guida autonoma potrebbe portaci sul posto di lavoro e in maniera automatica dirigersi verso il parcheggio a pagamento più vicino e pagare autonomamente il prezzo del parcheggio tramite uno smart contract. Oppure se l'auto necessità di interventi di manutenzione potrebbe dirigersi verso l'officina più vicina per essere riparata e poi tornare dal proprietario una volta finito il lavoro. Tutto questo mette i brividi e fa pensare a un'auto che svolge anche il ruolo di autista; proprio per questo credo che le case automobilistiche che offriranno questo servizio chiederanno in cambio un abbonamento mensile. Il noleggio con conducente cambierà e il ruolo dell'autista tenderà a scomparire. Sicuramente si creeranno nuovi lavori che richiederanno conoscenze più approfondite dell'ambito tecnologico annesso a questa

industria. In un futuro non sarà più sufficiente saper guidare un'auto per lavorare ma sarà richiesto un grado di istruzione sempre maggiore e una specializzazione maggiore rispetto a quella richiesta oggi.

Capitolo 4.4 Energia

I pannelli solari a uso domestico e in ambito più ampio le energie rinnovabili sono in continua crescita. La blockchain può essere utilizzata per permettere a utenti di scambiare criptovalute in cambio di energia direttamente tramite piattaforme apposite senza l'utilizzo di intermediari. Power Ledger è una Start Up che permette di ai propri utenti di vendere e comprare in maniera peer to peer energia rinnovabile. Tra i principali servizi che offre la piattaforma c'è la possibilità di vendere energia rinnovabile e la gestione di colonne di ricarica per veicoli elettrici con pagamenti immediati.[3]

Capitolo 4.5 Caso Studio

Il caso studio che viene preso in oggetto riguarda la città di Shanghai in Cina e l'organizzazione tedesca no profit MXC Foundation, che insieme stanno lavorando allo sviluppo del software "Smart City IoT Standard MXC Protocol" creato per il progetto di smart city di Shangai attraverso il quale i dispositivi interconnessi della città utilizzano piattaforme blockchain. Quindi MXC insieme allo Shanghai Yangpu district stanno lavorando per adottare il protocollo low power wide area network (LPWAN) che avrà il ruolo di processare la connessione wireless dei dispositivi IoT nella città di Shangai Yangpu. Il LPWAN è un tipo di telecomunicazione wireless che è a bassa potenza, alimentata quindi tramite batterie piccole, ed è ad ampio raggio: copre oltre 2 km di aree urbane. Questo tipo di tecnologia IoT è adatta per città e per il monitoraggio a lungo temine. [19,20,21] I dati verranno raccolti tramite la piattaforma " Interchain Data Market MXC " che si occuperà di verificare e garantire l'integrità dei dati che viaggiano all'interno della città.

MXC Foundation è specializzata in questo settore e sta lavorando anche a progetti di smart city a New York e in South Korea.

L'accordo è stato stipulato con l'intento di creare una strategia specifica per il potenziamento della raccolta dati e dell'analisi di questi all'interno della smart city. [22,23] Il direttore del dipartimento di scienza e tecnologia del distretto di Yangpu di Shangai ha dichiarato: "Il distretto di Shanghai e MXC stanno collaborando alla costruzione di città intelligenti e allo sviluppo del settore IoT. Con questa partnership ci aspettiamo di aumentare l'efficienza e migliorare la vita dei nostri cittadini". Il governo cinese ha sempre fatto in modo di avere un controllo sempre maggiore sui dati dei propri cittadini arrivando all'introduzione di censure sull'utilizzo di internet. A partire dalla partnership con MXC Foundation nascono una serie di domande: L'utilizzo della blockchain per maneggiare i dati avrà l'effetto di aumentare la riservatezza dei dati dei cittadini e sottrarli al controllo dello stato grazie alla decentralizzazione delle informazioni? Oppure è un altro metodo del governo cinese per aumentare il controllo sui propri cittadini? Credo che la risposta sarà determinata dal tipo di blockchain che verrà utilizzata per raccogliere le informazioni. Se verrà adottata una blockchain pubblica (Permisionless) è priva di un'entità centrale quindi le informazioni dei cittadini saranno fuori il controllo del governo cinese; se invece verrà adotta una blockchain privata (permissioned) lo stato cinese sarà l'autorità centrale e quindi avrà il pieno controllo delle informazioni [24,25,26].

Capitolo 5: Conclusioni

Questo studio ha cercato di spiegare in modo dettagliato come la comprensione di tecnologie innovative quali la Blockchain e Internet of things possa portare al miglioramento delle condizioni aziendali. Queste tecnologie possono infatti essere definite "disruptive": la loro introduzione ha creato nuovi mercati ancora in via di sviluppo. Con il mio lavoro di ricerca ho raccolto tutte le informazioni fondamentali per spiegare dettagliatamente il funzionamento della blockchain e dell'IoT e soprattutto i loro ambiti di applicazione. L'obiettivo di questa tesi è di permettere ai manager e agli imprenditori di comprenderne il funzionamento e quindi di dar loro la possibilità di interrogarsi su come potrebbero essere utilizzate e implementate all'interno dell'industria, al fine di innovare il proprio settore e di conseguenza aumentarne l'integrità e il tracciamento dei dati.

Nei capitoli sono stati analizzati i numerosi pro ma anche i contro sui quali è necessario interrogarsi e trovare una soluzione. Vi sono alcuni problemi, però, che devono ancora essere risolti; uno di questi potrebbe essere l'enorme consumo di energia richiesta da queste tecnologie. Proprio per questo motivo è necessario avere una visione generale dei vantaggi che un'impresa o anche un governo può ricavare dall'impiego di queste tecnologie, ma soprattutto è importante considerare i limiti che si presentano e le sfide in termini di sviluppo che vengono richieste dalle esigenze del mercato. È importante inoltre che i manager si assicurino continuamente della correttezza delle informazioni sui prodotti aziendali inserite all'interno della blockchain per evitare che venga meno la posizione di fiducia garantita dagli smart contract (come ad esempio nel caso di BMW, in cui viene tracciata la provenienza di ogni componente tramite la blockchain). [2,27,28,]

Abbiamo visto come per i policy maker è possibile ottenere un risparmio di tempo e denaro, aumentare la tracciabilità dei prodotti (come abbiamo visto nell'esempio dei supermercati che utilizzano la blockchain per dimostrare l'autenticità dei propri prodotti) e infine aumentare la fiducia degli stakeholder tramite l'utilizzo di smart contract che possono essere combinati a sensori IoT, i quali verificano il raggiungimento delle condizioni impostate prima di completare il contratto. Grazie a questa ricerca è stato possibile evidenziare

che il mercato è propenso ad accogliere questo cambiamento e che in alcuni ambiti risulta fondamentale l'applicazione. Sono emersi i numerosi buchi legislativi che necessitano di un intervento da parte dei governi e quindi i pericoli per le aziende e non solo. I futuri studi dovranno concentrarsi specialmente sulla legislazione riguardante gli smart contract e del sistema di raccolta fondi tramite ICO effettuato dalle aziende operanti nella blockchain, molte delle quali avendo la propria sede a Singapore potrebbero essere difficilmente perseguibili.

Un ulteriore stimolo di riflessione sulla legislazione è dato dall'eventualità in cui la blockchain possa procurare un danno economico a causa di uno smart contract che non funziona correttamente. Risulta difficile stabilire a chi possa essere imputata la colpa nel seguente caso. Credo che la blockchain e l'IoT siano delle tecnologie che subiranno il più forte sviluppo nei prossimi decenni e che potrebbero rivelarsi una risorsa fondamentale e indispensabile per le aziende del futuro. [3,29,30]

Bibliografia

[1] https://www.ilsole24ore.com/art/la-disruption-e-moda-ma-spesso-viene-confusa-l-accelerazione-tecnologica-AClycWT?refresh_ce=1

[2] Garavaglia, R. (2018). Tutto su Blockchain: Capire la tecnologia e le nuove opportunità. [ebook] Hoepli. Available at: https://www.perlego.com/book/1432625/tutto-su-blockchain-capire-la-tecnologia-e-le-nuove-opportunit-pdf

[3] Chiap, G., Ranalli, J. and Bianchi, R. (2019). Blockchain. Tecnologia e applicazioni per il business: Tutto ciò che serve per entrare nella nuova rivoluzione digitale. [ebook] Hoepli. Available at: https://www.perlego.com/book/1432551/blockchain-tecnologia-e-applicazioni-per-il-business

[4] https://en.bitcoin.it/wiki/Genesis_block

[5] https://it.cointelegraph.com/news/bitcoin-turns-ten-on-anniversary-of-genesis-block

[6] Iuon-Chang Lin and Tzu-Chun Liao . International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017 (DOI: 10.6633/IJNS.201709.19(5).01)

[7] https://it.wikipedia.org/wiki/Blockchain

[8] https://it.wikipedia.org/wiki/Problema_dei_generali_bizantini

[9] Kulkarni, K. (2018). Learn Bitcoin and Blockchain: Understanding blockchain and Bitcoin architecture to build decentralized applications. [ebook] Packt Publishing. Available at:

https://www.perlego.com/book/800663/learn-bitcoin-and-blockchain-understanding-blockchain-and-bitcoin-architecture-to-build-decentralized-applications-pdf

[10] https://www.wired.it/economia/business/2019/05/01/blockchain-rischi/

[11] Za, S. (2018). Internet of Things: Persone, organizzazioni e società 4.0. [ebook] LUISS University Press. Available at: https://www.perlego.com/book/1078936/internet-of-things

[12] https://www.filodiritto.com/internet-things-una-nuova-sfida-il-diritto

[13] https://assodel.it/internet-of-things-un-mercato-da-1-567-mld-di-dollari/

[14] https://www.blockchain4innovation.it/iot/iot-e-blockchain-il-binomio-alla-base-della-digital-transformation/

[15] https://it.businessinsider.com/e-a-tokyo-la-prima-smart-city-sicura-e-interconnessa-grazie-alla-blockchain/?refresh_ce

[16] https://www.am.pictet/it/blog/articoli/tecnologia-e-innovazione/la-blockchain-al-servizio-delle-smart-city [16]

[17] https://webthesis.biblio.polito.it/7888/1/tesi.pdf

[18] https://www.bmw.com/it/innovation/blockchain-automotive.html

[19] https://rfid.it/connettivita-iot-tecnologie-lpwan-a-confronto/

[20] https://www.blockchain4innovation.it/mercati/smart-energy/iot-e-blockchain-mxc-foundation-per-la-smartcity-di-shanghai/

[21] https://en.wikipedia.org/wiki/Yangpu_District

[22] https://www.iotforall.com/press-releases/press-mxc-blockchain-smart-city-integration-shanghai/

[23] www.cryptonomist.ch/2019/03/11/shanghai-smart-city-blockchain/

[24] https://www.smartcitiesworld.net/news/news/shanghai-integrates-blockchain-standard-3960

[25] https://coinrivet.com/how-blockchain-in-china-is-powering-smart-cities/

[26] Bhattacharjee, S. (2018). Practical Industrial Internet of Things Security: A practitioner's guide to securing connected industries. [ebook] Packt Publishing. Available at: https://www.perlego.com/book/778071/practical-industrial-internet-of-things-security-a-practitioners-guide-to-securing-connected-industries-pdf

[27] Triberti, C., Castellani, M., Pomi, P. and Turato, A. (2019). Blockchain. Guida pratica tecnico giuridica all'uso. [ebook] Go Ware. Available at: https://www.perlego.com/book/1080368/blockchain-guida-pratica-tecnico-giuridica-alluso-pdf

[28] Capasso, N. (2018). BITCOIN per tutti!: Come Guadagnare con Criptovalute e Blockchain. [ebook] HOW2 Edizioni. Available at: https://www.perlego.com/book/1087681/bitcoin-per-tutti-come-guadagnare-con-criptovalute-e-blockchain-pdf

[29] Cellini, P. (2018). La rivoluzione digitale. [ebook] LUISS University Press. Available at: https://www.perlego.com/book/1083848/la-rivoluzione-digitale-pdf

[30] https://www.blockchain4innovation.it/iot/iot-e-blockchain-il-binomio-alla-base-della-digital-transformation/