POLITECNICO DI TORINO

Dipartimento di Ingegneria Gestionale e della Produzione (DIGEP)

Corso di Laurea Magistrale in Ingegneria Gestionale

Politecnico di Torino

Tesi di Laurea Magistrale

Blockchain e NFT: Un'analisi critica e l'implementazione in un marketplace specializzato

Relatore	Candidato
Prof. Valentina GATTESCHI	Pietro Paolo DE CRESCENZO

Dicembre 2023

Indice

Elenco delle tabelle

Elenco delle figure

Capitolo 1

Introduzione

L'innovazione tecnologica ha da sempre permeato ogni aspetto della società umana, rivoluzionando e ridefinendo i modi in cui interagiamo con il mondo che ci circonda. Tra le più recenti innovazioni, la tecnologia blockchain si è affermata come una forza rivoluzionaria con il potenziale di ridefinire il panorama tecnologico, economico e sociale. Questa tesi di laurea esplora in dettaglio il mondo della blockchain, esaminando la sua evoluzione, le sue applicazioni attuali e future e il suo impatto su diversi settori industriali. Inoltre, nell'elaborato saranno descritte le funzionalità dello smart contract che è alla base di un progetto startup, che mira a creare un marketplace basato su NFT per orologi di lusso di seconda mano. Infine, è presente un'analisi delle caratteristiche fondamentali di diverse blockchain. Lo scopo dell'analisi è stato quello di individuare il framework che più si addicesse al caso aziendale in questione.

Il secondo capitolo si addentra nelle profondità della tecnologia blockchain, analizzando i suoi fondamenti, inclusi gli algoritmi di consenso, gli smart contract e i NFT (Non-Fungible Tokens), mettendo in luce le loro caratteristiche chiave e il loro ruolo nella creazione di un ecosistema blockchain robusto e sicuro.

Il terzo capitolo si concentra sull'applicazione odierna della blockchain in vari settori industriali, tra cui l'agroalimentare, l'energetico, l'edilizia e il lusso. Attraverso un'analisi approfondita, verranno esaminati i vantaggi e gli svantaggi dell'implementazione della blockchain in ciascun settore, rivelando come questa tecnologia stia trasformando processi e operazioni in modi innovativi.

Nel quarto capitolo, verrà presentata una soluzione blockchain sviluppata dall'autore della tesi per creare un marketplace dedicato all'acquisto e alla vendita di orologi di seconda mano. Questo marketplace utilizzerà i NFT per associare identità digitali ai singoli orologi, dopo un'attenta perizia da parte di un esperto,

consentendo una tracciabilità e una certezza senza precedenti nella compravendita di beni di lusso. In questo contesto, saranno presentati gli smart contract sviluppati per gestire le operazioni di creazione di NFT e l'associazione di metadati, fornendo un'illustrazione pratica dell'applicazione della blockchain in un contesto specifico.

Il quinto capitolo si immergerà nell'analisi delle diverse blockchain disponibili per lo sviluppo di smart contract, esaminando criteri come costo, scalabilità, ecosistema, storia e interoperabilità. Questa analisi aiuterà a delineare le sfide e le opportunità nell'implementazione di soluzioni blockchain, fornendo un quadro completo delle opzioni disponibili per gli sviluppatori.

Infine, il capitolo conclusivo ripercorrerà velocemente quanto spiegato nella tesi, fornendo delle lucide considerazioni su come sfrtuttare appieno il potenziale della blockchain e su quali siano i futuri sviluppi che ci immaginiamo nella soluzione da noi individuata.

In definitiva, questa tesi esplora il mondo in continua evoluzione della tecnologia blockchain, offrendo una visione approfondita delle sue applicazioni attuali e future in settori chiave, insieme a una soluzione pratica sviluppata per dimostrare il suo potenziale. La conoscenza acquisita in questo lavoro contribuirà a informare e ispirare futuri progressi nel vasto e affascinante contesto della blockchain.

Capitolo 2

Stato dell'arte

Nel 1982, David Chaum fu la prima persona di cui si ha notizia a proporre un protocollo simile a Blockchain nella sua tesi di dottorato [1]. Nel 1991, Haber e Stornetta descrissero una catena di blocchi sicura da un punto di vista crittografico. Nel 1998, Nick Szabo progettò il "bit gold", un meccanismo di valuta digitale decentralizzato. Nel 2008, Satoshi Nakamoto introdusse Bitcoin, una forma di denaro elettronico basata su una rete puramente peer-to-peer. Fu anche nel 2008 che il termine "Blockchain" fu utilizzato per la prima volta per indicare il registro distribuito alle spalle delle transazioni Bitcoin.

Nel 2013, Vitalik Buterin propose Ethereum nel suo whitepaper. Nel 2014, lo sviluppo di Ethereum fu finanziato attraverso una campagna di crowdfunding, e il 30 luglio 2015 la rete Ethereum divenne operativa. L'emergere di Ethereum implicava che fosse nata la cosiddetta "Blockchain 2.0", poiché, a differenza dei vari progetti Blockchain incentrati nello sviluppo di "altcoin" (cioè, altre criptovalute simili a Bitcoin), Ethereum permetteva alle persone di connettersi tramite applicazioni distribuite e senza la necessità di fiducia, sulla propria Blockchain. In altre parole, mentre Bitcoin fu sviluppato per un registro distribuito, Ethereum fu progettato per un archivio dati distribuito e per "smart contracts", ovvero piccoli programmi informatici.

Nel 2015, la Linux Foundation annunciò il progetto Hyperledger, un software open-source di Blockchain. L'obiettivo di Hyperledger è costruire una Blockchain aziendale, ed i framework di Hyperledger differiscono da quelli di Bitcoin ed Ethereum.

2.1 Introduzione alla blockchain

DLT è l'acronimo di "Distributed Ledger Technology", che in italiano significa "Tecnologia dei Registri Distribuiti". Si tratta di una tecnologia informatica che consente di registrare e condividere dati in modo distribuito tra diverse parti o nodi di una rete, senza la necessità di un'autorità centrale di controllo. La caratteristica principale della DLT è la sua capacità di garantire la sicurezza e l'integrità dei dati attraverso la decentralizzazione e la crittografia.

Uno dei tipi più noti di DLT è la blockchain, che è stata introdotta alle folle con la criptovaluta Bitcoin. Tuttavia, esistono anche altre forme di DLT che non utilizzano necessariamente una catena di blocchi, ma condividono comunque le proprietà di decentralizzazione, immutabilità e trasparenza dei dati. Le tecnologie dei registri distribuiti sono ampiamente utilizzate in una varietà di settori, oltre alle criptovalute, compresi l'approvvigionamento, la gestione delle supply chain, la tracciabilità degli alimenti, la registrazione dei diritti di proprietà e molto altro. Questa tecnologia è considerata promettente per migliorare l'efficienza e la sicurezza delle transazioni e dei processi aziendali.

Qualunque transazione inserita in tale registro è sottoposta ad un meccanismo di firma a doppia chiave asimmetrica, che funziona con un meccanismo simile a quello della firma digitale. Le DLT prevedono l'utilizzo di algoritmi crittografici che abilitano l'utente all'utilizzo del sistema mettendogli a disposizione una chiave pubblica ed una privata che viene usata per sottoscrivere le transazioni o per attivare gli smart contract o altri servizi collegati alla blockchain.

Con il termine 'distribuito' si intende l'assenza di un sistema centrale che possieda il libro mastro; infatti, questo è distribuito tra tutti i nodi, i quali ne detengono una copia. Le DLT prevedono pertanto un meccanismo di validazione basato sul consenso. Le modalità di gestione del consenso, unitamente alle logiche di impostazione del registro, rappresentano due fra i principali punti qualificanti della carta d'identità delle tecnologie Distributed ledger. All'interno di questo insieme trovano la loro collocazione le blockchain.

La logica centralizzata è rappresentata dal tradizionale 'Centralized Ledger' con un rapporto rigorosamente centralizzato Uno-A-Tanti, dove tutto deve essere gestito facendo riferimento ad un'autorità o sistema centralizzato. Nel centralized ledger la fiducia è nell'autorità o nel sistema che rappresenta il centro dell'organizzazione.

Il 'Decentralized Ledger' ripropone la logica della centralizzazione a livello locale con satelliti organizzati a loro volta nella forma di Uno-A-Tanti che si relazionano

a loro volta in una forma che ripete lo stesso modello gerarchco. Non c'è più un grande soggetto centrale, bensì tanti soggetti centrali. La fiducia anche in questo caso è delegata ad un soggetto centrale, più vicino, ma comunque centralizzato. Quindi, anche le organizzazioni basate sul decentralized ledger definiscono una governance fondata su delle forme di coordinamento di tipo centralizzato.

Il vero cambiamento è rappresentato dal 'Distributed Ledger', ovvero da una reale e completa logica distribuita dove non esiste più nessun centro, e dove la logica di governance è costruita attorno ad un nuovo concetto di fiducia tra tutti i soggetti. Nessuno ha la possibilità di prevalere e il processo decisionale passa rigorosamente attraverso un processo di validazione.

Nella figura 2.1 [2] sono mostrati i differenti gradi di centralizzazione appena citati e che un registro può avere.

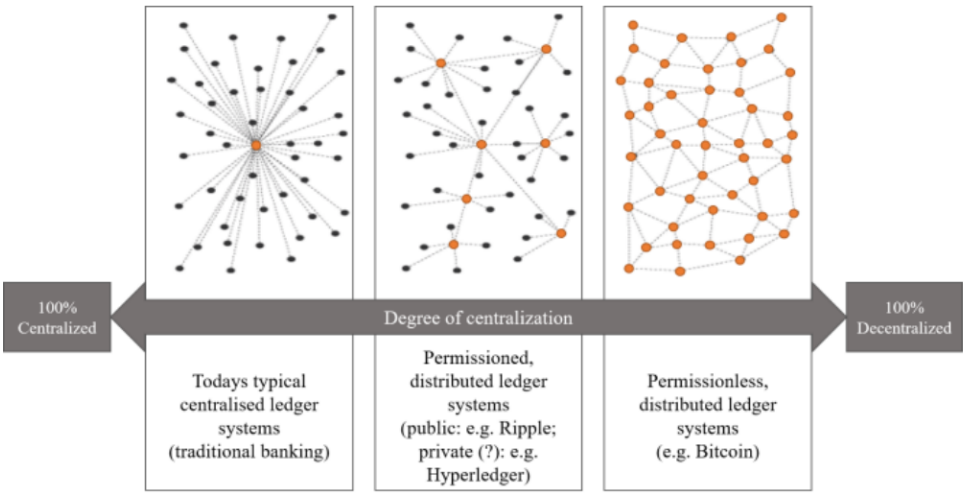

Figura 2.1: Raffigurazione di Centralized, Decentralized e Distributed Ledger

Per quanto riguarda la definizione di blockchain, non ne esiste una univoca. A seconda di come si voglia interpretare tale tecnologia, è possibile definirla in diversi modi. Di seguito, sono presenti due delle più comuni definizioni di blockchain:

1. La blockchain è una sottofamiglia della tecnologia DLT (Distributed Ledger Technologies) in cui il registro è strutturato come una catena di blocchi contenenti le transazioni e la cui validazione è affidata a un meccanismo di consenso, distribuito su tutti i nodi della rete nel caso delle blockchain permissionless o pubbliche, oppure su tutti i nodi che sono autorizzati a partecipare al processo di validazione delle transazioni da includere nel registro nel caso delle blockchain permissioned o private.

2. La blockchain è una struttura dati condivisa e "immutabile". È definita come un registro digitale le cui voci sono raggruppate in "blocchi" concatenati in ordine cronologico, e la cui integrità è garantita dall'uso della crittografia.

Quindi, la blockchain è quella particolare DLT che utilizza una catena di blocchi per organizzare e registrare i dati, i quali possono essere solo aggiunti. Le principali caratteristiche delle tecnologie blockchain sono l'immutabilità del registro, la trasparenza, tracciabilità delle transazioni e la sicurezza basata su tecniche crittografiche.

Dal punto di vista delle regole di gestione, ciascun blocco si aggiunge alla catena sulla base di un processo basato sul consenso distribuito su tutti i nodi della rete, ovvero con la partecipazione di tutti i nodi che vengono chiamati a contribuire alla validazione delle transazioni presenti in ciascun blocco e alla loro "inclusione" nel registro. La soluzione per tutte le transazioni è affidata ai nodi che sono chiamati a controllare e approvare tutte le transazioni creando una rete che condivide su ciascun nodo l'archivio di tutta la blockchain, e dunque di tutti i blocchi con tutte le transazioni. Ciascun blocco è per l'appunto anche un archivio per tutte le transazioni e per tutto lo storico di ciascuna transazione che, possono essere modificate solo con l'approvazione dei nodi della rete. Le transazioni possono essere considerate immodificabili (se non attraverso la riproposizione e la "ri-autorizzazione" delle stesse da parte di tutta la rete). Da qui il concetto di immutabilità.

La blockchain è una serie di blocchi che archiviano un insieme di transazioni validate e correlate da un marcatore temporale (timestamp). Ogni blocco include l'hash, ossia una funzione crittografica non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita, che identifica il blocco in modo univoco e che permette il collegamento con il blocco precedente.

I componenti basilari della blockchain sono:

- Nodo: sono i partecipanti alla blockchain e sono costituiti fisicamente dai server di ciascun partecipante;
- Transazione: è costituita dai dati che rappresentano i valori oggetto di "scambio" e che necessitano di essere verificati, approvati e poi archiviati;
- Blocco: è rappresentato dal raggruppamento di un insieme di transazioni che sono unite per essere verificate, approvate e poi archiviate dai partecipanti alla blockchain;
- Ledger: è il registro pubblico nel quale vengono "annotate" con la massima trasparenza e in modo immutabile tutte le transazioni effettuate in modo

ordinato e sequenziale. Il Ledger è costituito dall'insieme dei blocchi che sono tra loro incatenati tramite una funzione di crittografia e grazie all'uso di hash;

- Hash: identifica in modo univoco e sicuro ciascun blocco. Un hash non deve permettere di risalire al testo che lo ha generato.

La transazione contiene invece informazioni relative all'indirizzo pubblico del ricevente, le caratteristiche della transazione e la firma crittografica che garantisce sicurezza e autenticità della transazione. Un blocco non è altro che un contenitore di informazioni, dove il 65% dello spazio (ossia delle informazioni) è occupato dalle transazioni e dalle firme digitali. L'header è composto dagli hash (impronta digitale) del blocco. Poi ci sono delle informazioni extra come il tempo e il median time stamp che sono importanti per l'integrità della blockchain. Per quanto riguarda la dimensione di un blocco, questo in origine pesava 1 megabyte, ma con l'introduzione di un aggiornamento sono state spostate le firme in un'altra sezione del blocco, aumentando quindi la dimensione massima del blocco stesso a 4 megabyte. Inoltre, c'è da dire che tutte le transazioni non sono uguali in termini di byte.

2.2 Blockchain Permissionless e Permissioned

L'immutabilità è un grandissimo valore della blockchain che ovviamente garantisce anche alla sicurezza dei dati. Per cambiare, danneggiare o distruggere un registro centralizzato è necessario violare l'autorità centrale che lo gestisce. Nel caso della blockchain, invece è impossibile, in quanto sarebbe necessario violare tutte le copie del libro mastro possedute da tutti i partecipanti della blockchain e occorrerebbe farlo simultaneamente. Tale operazione è praticamente impossibile, anche se ovviamente occorre valutare la dimensione della blockchain in termini di partecipanti ovvero di nodi. Allo stesso tempo, non può nemmeno esistere un falso libro mastro, in quanto tutti i partecipanti sono in possesso di un'unica versione autentica che possono impugnare per un confronto e per la verifica. In questo modo, la fiducia e il controllo delle transazioni passano dall'autorità centrale a tutti i partecipanti. Le transazioni basate sulla blockchain non sono centralizzate e nascoste, ma sono decentralizzate e trasparenti, aperte a tutti. In questo caso appena descritto, la blockchain è di tipo permissionless, cioè non occorrono autorizzazioni da parte di alcuna autorità speciale per partecipare al controllo e all'aggiunta di transazioni.

Le blockchain che invece necessitano di autorizzazioni sono definite permissioned, basate su delle governance che attribuiscono a uno specifico gruppo di operatori la gestione e l'autorità nel definire gli accessi, i controlli, le autorizzazioni e soprattutto

la possibilità di aggiungere transazioni al registro distribuito. Le blockchain permissioned possono unire i valori di trasparenza, di immutabilità e di sicurezza delle blockchain garantendo a determinati soggetti come banche, imprese e pubbliche amministrazioni la possibilità di un controllo sulle modalità di esecuzione delle transazioni.

Le blockchain permissionless, di cui l'esempio più famoso e diffuso è rappresentato dalla blockchain Bitcoin, impediscono ogni forma di censura: nessuno è nella condizione di vietare che una transazione possa avvenire e che possa essere aggiunta al registro una volta che ha conquistato il consenso necessario tra tutti i nodi della blockchain. Le blockchain permissionless possono essere utilizzate come database globale per tutti quei documenti che hanno la necessità di essere assolutamente immutabili nel tempo a meno di aggiornamenti che richiedono la massima sicurezza in termini di consenso, come ad esempio i contratti di proprietà o i testamenti.

Le blockchain permissioned possono invece essere controllate e dunque possono avere una proprietà. Quando un nuovo dato o record viene aggiunto, il sistema di approvazione non è vincolato alla maggioranza dei partecipanti alla blockchain, bensì a un numero limitato di attori che sono definibili come 'trusted'. Questo tipo di blockchain possono essere utilizzate da istituzioni, grandi imprese che devono gestire filiere con una serie di attori, imprese che devono gestire fornitori e subfornitori, banche, società di servizi, operatori in ambito retail. Le blockchain permissioned permettono di definire speciali regole per l'accesso e la visibilità di tutti i dati. In altre parole, introducono nella blockchain un concetto di governance e di definizione di regole di comportamento. Infine, c'è da dire che le blockchain permissioned sono anche più performanti e veloci delle permissionless.
Nella figura 2.2 [3] è mostrato un riassunto delle varie tipologie di blockchain appena descritte:

	Permissionless	Permissioned
Public	• Anyone can join, read, write and commit • Hosted on public servers • Anonymous, highly resilient • Low scalability	• Anyone can join and read • Only authorised and known participants can write and commit • Medium scalability
Private	• Only authorised participants can join, read, and write • Hosted on private servers • High scalability	• Only authorised participants can join and read • Only the network operator can write and commit • Very high scalability

Figura 2.2: Comparazione delle caratteristiche tra blockchain permssionless/permissioned e pubbliche/private

Un particolare tipo di blockchain sono le blockchain Consortium, le quali sono reti distribuite controllate da un gruppo selezionato di nodi autorizzati, non aperte al pubblico come le blockchain pubbliche. Questi consorzi coinvolgono entità specifiche, come aziende o istituzioni, che condividono responsabilità nella gestione e validazione delle transazioni. Le decisioni sono prese attraverso un consenso tra i partecipanti, garantendo una maggiore scalabilità, privacy e controllo rispetto alle blockchain pubbliche. Questi consorzi possono adottare diverse strutture di consenso e governance per soddisfare le esigenze specifiche dei membri, consentendo la creazione di applicazioni personalizzate e sicure

2.3 Il ruolo dei miner nelle transazioni della blockchain Bitcoin

I miner sono un elemento chiave di Bitcoin [4] perché sono coloro che creano i blocchi e sostengono la decentralizzazione. Più c'è competizione tra i miner, più la rete è sicura; quindi, più è elevato l'hashrate (potenza di calcolo di Bitcoin). Per ogni blocco risolto, il miner ottiene il suo reward che serve a rientrare nei costi sostenuti per partecipare all'attività di mining. Il protocollo prevede che ogni 210.000 blocchi minati avvenga quello che è definito 'halving'. L'halving si verifica circa ogni 4 anni, essendo il tempo per minare un blocco pari a circa 10 minuti. Con halving si intende il dimezzamento delle reward ricevute dal nodo per minare il blocco. Questo processo è progettato per controllare l'offerta di Bitcoin e prevenire l'inflazione, limitando il numero di nuove monete che possono essere prodotte. Essendo bitcoin un asset scarso per definizione, ossia che la quantità massima di bitcoin prodotta è fissata a 21 milioni di bitcoin, il numero massimo di halving è 64. Si stima che il processo di creazione di nuovi bitcoin finirà nel 2140.

Nella figura 2.3 [5] è mostrato il grafico del fenomeno dell'halving.

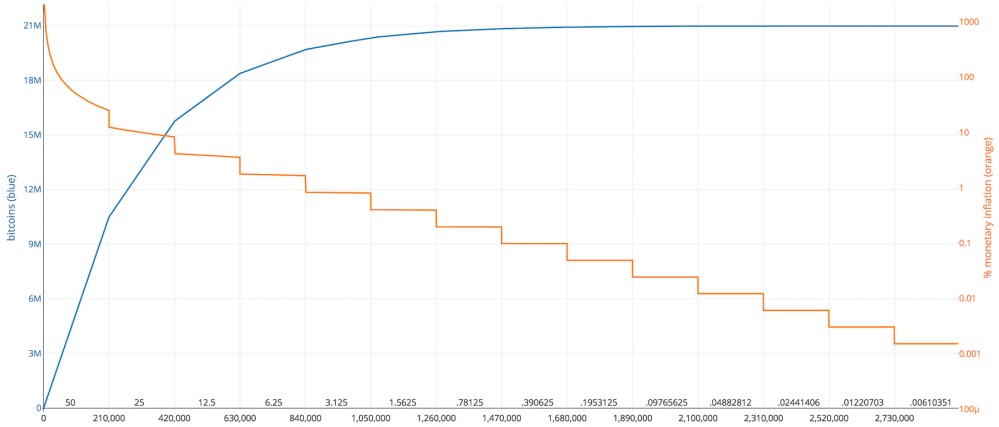

Figura 2.3: Rappresentazione grafica del fenomeno dell'halving

Esistono due tipi di attori/nodi nella rete Bitcoin: fullnode e miner. I primi detengono una copia di tutta la blockchain scaricata nel proprio hard disk e validano le transazioni, ma non è detto che le minino. In sostanza, i fullnode verificano se la transazione è sintatticamente corretta. Invece, i miner prendono le transazioni già controllate dai fullnode e minano il blocco contenente tali transazioni. In attesa che il miner mini la transazione (crei il blocco), queste ultime sono parcheggiate nella memory pool e quindi in questo momento le transazioni sono valide ma non confermate. Il miner sceglie dalla memory pool le transazioni con fee maggiori e le mette nel suo "candidate block", che avrà un riferimento all'ultimo blocco creato nella catena. Anche gli altri miner avranno il loro candidate block e saranno aggiornati con la catena. Quando un miner valida il blocco attraverso la PoW, lo distribuisce a tutti e questi lo verificano attraverso lo SHA256. Quindi, questo diventerà l'ultimo blocco della catena. La prima transazione di ogni blocco si chiama coinbase, ed è quella che riguarda la reward ottenuto dal blocco minato più tutte le fee che riceverà il miner stesso. Perché un nuovo blocco di transazioni sia aggiunto alla blockchain è necessario appunto che sia controllato, validato e crittografato. Solo con questo passaggio può poi diventare attivo ed essere aggiunto alla blockchain. Per effettuare questo passaggio, è necessario che ogni volta che viene composto un blocco venga risolto un complesso problema crittografico che richiede un cospicuo impegno anche in termini di potenza e di capacità elaborativa (nel caso di Bitcoin). Questa operazione viene definita come "mining", ed è svolta appunto dai miner. Il lavoro del miner è assolutamente fondamentale nell'economia della gestione delle blockchain. Chiunque può diventare un miner e può competere per essere il primo a risolvere il complesso problema matematico legato alla creazione di ogni nuovo blocco di transazioni in modo valido e crittografato che possa essere aggiunto alla blockchain. Trattandosi di un impegno importante, con notevole dispendio di

energie, il mining di criptovalute è un impegno che necessita di essere remunerato e incentivato. Per risolvere il problema crittografico è necessaria un'elevata potenza di calcolo e conseguentemente anche di energia elettrica. Più potenza di calcolo si ha a disposizione e più è probabile che si risolva il problema matematico. Agli albori di Bitcoin, era possibile minare dei blocchi anche da casa. Invece, man mano che sempre più nodi si sono uniti alla rete, è diventato sempre più improbabile. Per ovviare a tale problema, sono nate le cosiddette "mininig pool", ossia dei singoli individui che mettono insieme le proprie risorse di calcolo e partecipano al mining come un unico nodo. Nel caso in cui un blocco venga minato, le reward saranno divise tra i partecipanti della mining pool.

Nelle blockchain permissioned, il mining è svolto in funzione della governance, dall'autorità che attiva la blockchain stessa.

Nelle blockchain permissionless, il mining può essere svolto da qualsiasi partecipante alla blockchain e il miner viene incentivato con delle forme di remunerazione che dipendono dal tipo di regole o governance definite da ciascuna blockchain.

Nel caso in cui il processo di verifica dovesse rilevare un errore o una anomalia, il blocco viene rifiutato e tutti avranno visibilità del fatto che la transazione non è stata autorizzata. Diversamente, se tutte le transazioni sono validate, il blocco viene creato ed entrerà a far parte della blockchain a tutti gli effetti come un record pubblico permanente e immutabile: nessun partecipante alla blockchain potrà cambiarlo o rimuoverlo.

2.4 Funzionamento della firma digitale

La firma digitale è l'elemento chiave di tutte le blockchain: funge da autenticazione. La firma digitale risolve il problema dell'integrità poiché il messaggio inviato in un canale non sicuro potrebbe essere alterato da qualcuno nel mezzo. Inoltre, garantisce l'autenticità del mittente e il non ripudio, in quanto il mittente non può disconoscere il messaggio che ha inviato. Quindi, la chiave privata deve rimanere segreta perché è in grado di firmare le transazioni (messaggi).

Per capire al meglio il funzionamento della firma digitale, si consideri un esempio in cui ci sono due persone (mittente e ricevente) che vogliono scambiarsi un'informazione. Quindi, il mittente scrive un testo in chiaro (non ha subito alterazioni crittografiche) a cui è applicata una funzione crittografica SHA256. Una funzione crittografica prende un input e genera sempre un output corrispondente sempre all'input, ossia genera l'impronta digitale (digest) di quel messaggio. Dopodiché,

il mittente applica la sua chiave privata al messaggio crittografato, creando la firma digitale e l'autenticazione. Quindi, il mittente invia al ricevente il messaggio in chiaro, la firma digitale e la chiave pubblica. Il ricevente applicherà la chiave pubblica, che il mittente gli ha passato, sulla firma digitale ed ottiene il messaggio crittografato. Successivamente, applicherà lo SHA256 sul messaggio in chiaro, ottenendo il messaggio crittografato. Infine, il ricevente confronterà i digest (messaggi crittografati) e se sono uguali, allora significa che è stato proprio quel particolare mittente ad inviarlo. Nel caso in cui il testo in chiaro fosse stato alterato, quando il ricevente applica lo SHA256 al messaggio in chiaro i due digest risulterebbero diversi: quindi o non è stato quel mittente ad inviare il messaggio o il messaggio è stato alterato durante la trasmissione. La chiave pubblica è derivata dalla chiave privata, quindi solo quella chiave privata può generare quella chiave pubblica. La chiave privata è generata con un'entropia (serie di numeri casuali): più alta è l'entropia, più è forte la chiave privata. Al contrario, una chiave pubblica non può generare una particolare chiave privata. La chiave privata genera la firma digitale, la quale può essere verificata con la chiave pubblica e il messaggio che si vuole firmare. Questo processo è chiamato di "crittografia asimmetrica", in quanto ci sono due chiavi (pubblica e privata). La chiave pubblica si può distribuire senza un canale sicuro, mentre la chiave privata deve rimanere per l'appunto segreta.

In definitiva, la chiave privata fa due cose fondamentali: derivare la chiave pubblica e creare la firma digitale. La chiave pubblica non può derivare la chiave privata perché non ha tutte le informazioni per derivarla. Una chiave privata può derivare solo quella particolare chiave pubblica; non c'è un'altra chiave privata che derivi la stessa chiave pubblica. È necessario tenere segreta la chiave privata perché può creare la firma digitale che certifica che solo quella precisa persona (risolve il problema dell'autenticità) ha fatto quel tipo di firma, che assieme alla chiava pubblica (corrispondente a quella chiave privata) testimonia che il messaggio non sia stato alterato (risolve il problema dell'integrità). Inoltre, il mittente non può disconoscere il messaggio che ha fornito (proprietà di non ripudio).

2.5 Comparazione degli algoritmi di consenso

L'anonimato è sia una caratteristica molto cercata nella blockchain, sia può risultare un problema quando si vuole verificare la bontà delle azioni intraprese dai nodi. Infatti, per essere sicuri che gli utenti anonimi siano onesti quando aggiungono transazioni a un registro è necessario validare ogni transazione per accertarne la legalità (senza malizia, doppie spese, eccetera) e quindi inserire le transazioni in un blocco. L'accordo per l'aggiunta di un blocco alla blockchain avviene attraverso algoritmi di consenso. Questi algoritmi sfruttano il fatto che la maggior parte degli

utenti su una blockchain hanno un interesse comune nel mantenere la blockchain onesta. Un sistema blockchain utilizza un algoritmo di consenso per costruire la fiducia e memorizzare correttamente le transazioni nei blocchi. Di conseguenza, gli algoritmi di consenso possono essere considerati il cuore di tutte le transazioni delle blockchain.

Un protocollo di consenso è essenzialmente un insieme di regole seguite da ogni partecipante. Poiché la tecnologia blockchain è distribuita e priva di una fiducia universale, ha bisogno di un meccanismo di consenso distribuito per far sì che tutti i partecipanti siano d'accordo sullo stato attuale della Blockchain. Il consenso di una blockchain si basa sulla scarsità, in quanto controllare una maggiore quantità di una risorsa scarsa conferisce maggiore controllo sul funzionamento della blockchain. Sono stati progettati diversi meccanismi di consenso unici per le blockchain, tra cui: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Elapsed Time (PoET), Practical Byzantine Fault Tolerance (PBFT), Directed Acyclic Graph (DAG), Proof of Authority (PoA), Tendermint, Ripple, Scalable Byzantine Consensus Protocol (SCP), Proof of Bandwidth (PoB), Proof-of-Importance (PoI), Proof of Burn, Proof of Capacity, a seconda delle esigenze specifiche.

PoW, PoS, DPoS e PBFT sono i più comuni algoritmi di consenso. DAG è quello più diverso dagli altri algoritmi di consenso. PoET è stato sviluppato da Intel Corporation ed è utilizzato in Hyperledger Sawtooth. Pertanto, questi sei algoritmi di consenso sono ulteriormente approfonditi di seguito:

1. Proof of Work (PoW). PoW seleziona un problema che può essere risolto solo con la crittografia. Ad esempio, quando è il momento di creare e convalidare un blocco completo, il problema consiste nell'indovinare un valore "nonce" in modo tale che, utilizzando i dati della transazione e il valore del "nonce" come input per una funzione di hash, l'output del suo hash corrisponda alla difficoltà richiesta, ad esempio, iniziando con quattro zeri iniziali. Ogni nodo (anche chiamato nodo di mining) sulla rete sta indovinando diversi valori "nonce" in modo casuale fino a quando un nodo per primo trova il valore "nonce" corrispondente alla difficoltà. Pertanto, un nodo di mining deve impiegare molte risorse computazionali su questo processo (da cui il termine "work", ovvero "lavoro") e risolvere il problema più velocemente degli altri per riuscire a creare un blocco da collegare alla Blockchain e ottenere una ricompensa di mining, spesso sotto forma di criptovaluta. D'altro canto, le funzioni di hash sono importanti come rompicapo crittografico al centro dell'algoritmo di consenso PoW. La rete Bitcoin adotta la funzione di hash crittografico SHA-256. Un grosso problema con il processo di consenso PoW è che richiede

molto tempo ed elettricità per essere completato.

2. Proof of Stake (PoS). PoS è il secondo metodo di consenso più importante e richiede meno calcoli per il mining rispetto a PoW. PoS risolve i problemi di tempo e consumo di elettricità che affliggono PoW. PoS richiede che i nodi depositino una quota (o "stake") per essere scelti come prossimo minatore di blocchi. Quando un blocco viene scelto, il creatore riceverà le commissioni di transazione associate a quel blocco. Se il vincitore del blocco tenta di aggiungere un blocco non valido, perderà la propria quota. Nella sua prima fase di aggiornamento a Ethereum 2.0, la rete di Ethereum è passata dall'algoritmo di consenso PoW a PoS.

3. Delegated Proof-of-Stake (DPoS). Nel DPoS, tutti i detentori di token possono votare un certo numero di delegati e possono anche delegare il proprio potere di voto ad altri utenti. Più token detiene un titolare di token, maggiore è il potere di voto di cui dispone. I delegati sono responsabili della convalida delle transazioni e dei blocchi per garantire la sicurezza della rete. A differenza della maggior parte della potenza di calcolo in PoW o della maggior parte dei token in PoS, i detentori di token nel DPoS possono votare chi minerà nuovi blocchi e premiare solo i migliori miner. EOS è uno dei sistemi Blockchain che utilizza l'algoritmo DPoS.

4. Proof of Elapsed Time (PoET). Intel Corporation ha sviluppato PoET per consentire un modo diverso per determinare il vincitore che minerà un blocco. In PoET, ogni potenziale nodo di convalida richiede un tempo di attesa casuale generato in una piattaforma di calcolo attendibile, ad esempio Intel's SGX. Dopo l'attesa per il tempo assegnato, il primo nodo a terminare il tempo di attesa è il vincitore di convalida e può aggiungere il nuovo blocco. La piattaforma di calcolo attendibile consente a ogni nodo di avere una possibilità di essere il vincitore.

5. Practical Byzantine Fault Tolerant (PBFT). L'obiettivo della Fault Tolerance (FT) è risolvere un noto dilemma in cui alcuni attori sono disonesti, ma il consenso deve comunque essere raggiunto. Nel PBFT, a condizione che i nodi maliziosi siano minori di un terzo dei nodi totali nel sistema Blockchain, l'accordo sullo stato attuale della Blockchain sarà raggiunto. Un maggior numero di nodi nel sistema Blockchain incrementa la sua sicurezza. Hyperledger Fabric è attualmente basato su PBFT. Tuttavia, altre piattaforme stanno sperimentando varianti simili di questo algoritmo per migliorare la loro affidabilità e sicurezza.

6. Directed Acyclic Graph (DAG) si compone di vertici e archi (le connessioni tra di essi), distinguendosi così da altri protocolli di consenso. I vertici e

gli archi sono diretti, puntando in una sola direzione, e sono definiti aciclici in quanto non si verificano cicli tra i vertici. Ogni vertice rappresenta una singola transazione, eliminando la necessità di concetti di blocchi. Invece di raggruppare le transazioni in blocchi, ogni transazione si collega direttamente ad un'altra. Sebbene non vi sia un mining di tipo tradizionale, un'operazione di PoW minima viene eseguita quando un nodo invia una transazione per prevenire attacchi di spam e validare le transazioni precedenti. IOTA utilizza un algoritmo di consenso basato su DAG, sfruttando questa struttura per migliorare l'efficienza e la scalabilità della loro rete.

Nella figura 2.4, generata da me, è presente una tabella riepilogativa che ha lo scopo di confrontare i vari algoritmi di consenso descritti in base alle caratteristiche presenti nelle righe.

	PoW	PoS	DPoS	PoET	PBFT	DAG
Setup	Public permissionless / Private	Public permissionless / Private	Public / Private	Private permissioned or permissionless	Private permissioned	Public permissioned non-Blockchain
Cost of entry and returns	Relatively high cost of entry, but high returns	Low cost of entry, but low returns	Lower cost and lower returns than PoS	Very low cost of entry but low returns	All participate with no return	All participate with no return
Incentives	The winning miner receives new coins & transaction fees for the block validated.	The winner receives transaction fees with the new block. If a block winner attempts to add an invalid block, he loses his stake.	The threat of loss of reputation & income provides incentive for delegates to act honestly and keep the network secure.	The winning miner receives the transaction fees with the new block he validates	NO	NO
Finality	Probabilistic	Probabilistic	Probabilistic	Probabilistic	Immediate	Probabilistic
Scalability in network	High	Medium	Medium	Medium	Low	High
Energy efficiency	Very low	High	High (no miners required)	High	Medium (Some PBFT systems use PoW to prevent Sybil attack, but only after a set number of blocks and not for every block)	Medium (A small PoW operation when a node submits a transaction to ensure network is not being spammed)
Examples	Bitcoin, Litecoin, Monero, Dash, Zcash, Decred and more.	Ethereum, Cardano, Polkadot, BlackCoin, Peercoin	EOS, BitShares, Lisk, Steem, Ark, Nano and Tezos.	Hyperledger Sawtooth	Hyperledger Fabric, Ziliqa	IOTA

Figura 2.4: Differenze tra alcuni meccanismi di consenso

2.6 Blockchain 2.0: Ethereum

Ethereum è nata nel 2014 per mano del suo fondatore Vitalik Buterin. E' una piattaforma open source, decentralizzata e blockchain-based [6]. Lo scopo primordiale per cui è nata Ethereum è quello di creare un protocollo alternativo per la creazione di smart contract e applicazioni decentralizzate (dApps). Ethereum è una blockchain permissionless e pubblica; il suo digital asset nativo che alimenta il protocollo è l'Ether (ETH). Il meccanismo di consenso utilizzato da Ethereum è attualmente la PoS, anche se da settembre 2014 fino a settembre 2022 ha utilizzato la PoW, con delle differenze rispetto a Bitcoin dovute dalla mancanza del requisito di scarsità che contraddistingue bitcoin. Nel 2013 viene pubblicato il white paper di Ethereum e nel 2014 viene annunciato il lancio del progetto con la prima ICO e la pubblicazione del yellow paper. Nel 2015 viene minato il 'genesis block', ossia il primo blocco della catena.

Nel 2016 è avvenuto il DAO hack, in tale occasione una quantità sostanziosa di ETH viene sottratta da uno smart contract che descriveva una DAO. Questo evento ha portato all'hard fork tra ethereum classic e la versione attuale di Ethereum. In sostanza, si è raggiunto il consenso per modificare la chain e fare in modo che quell'hack non sia considerato. Nel 2019 viene annunciato e finanziato ETH2.0, il progetto che ha portato al passaggio da PoW a PoS. Nel 2020 viene avviata la Beacon Chain, una chain parallela ad Ethereum che rappresentava la nuova versione di Ethereum con la PoS. Successivamente la Beacon Chain ha fatto un merge verso la vecchia blockchain di Ethereum. Il merge è stata la fusione della Beacon chain (Ethereum 2.0 con PoS) e la vecchia chain PoW di Ethereum. È stato fuso l'execution layer della vecchia blockchain (che si occupava della gestione delle transazioni, dei balance ecc) con il consensus layer della Beacon chain, in modo da prendere lo stato della blockchain e continuare poi con il nuovo algoritmo di consenso.

Uno dei benefici del passaggio a PoS è stato il crollo dei consumi elettrici del 99,95% rispetto a PoW. Inoltre, in tale passaggio è stata modificata la coinbase di Ethereum al fine di raggiungere maggiore scalabilità. In questo modo la rete è diventata più accessibile a tutti in quanto è necessario depositare in staking 32ETH per diventare un validatore. Il valore di 32 ETH non è esiguo, ma è comunque minore dei soldi necessari per comprare tutte le attrezzature computazionali per diventare un miner con il PoW. Secondo il PoS, un utente può diventare un nodo validatore depositando 32ETH in un contratto ad hoc. Dopodiché, entra a far parte di una coda di attivazione, la quale serve per regolare il numero di validatori nuovi che entrano nella rete per evitare che la rete si destabilizzi. Dopo un certo

tempo, entra a far parte dei validatori della rete. I validatori vengono scelti randomicamente per proporre il nuovo blocco da validare in ogni slot (della durata di 12 secondi). Il loro compito è scegliere le transazioni dalla transaction pool e inserirle nel blocco. Per ogni slot, viene selezionato sempre in maniera randomica un comitato di validatori, i cui voti servono per determinare la validità del blocco. Ogni validatore ha la stessa probabilità di essere selezionato in ogni slot, per tale motivo chi ha più di 32 ETH da depositare in staking potrebbe decidere di creare più nodi validatori. Gli slot sono raggruppati in epoch, a loro volta composte da 12 slot. In Ethereum gli ultimi due blocchi selezionati sono considerati come dei blocchi di checkpoint. I validatori votano per la coppia di checkcpoint che considerano validi. Se la coppia di checkpoint attrae i voti per i 2/3 del totale degli ETH depositati, allora il blocco più recente diventa giustificato mentre quello più vecchio diventa finalizzato, in quanto già era stato giustificato precedentemente.

Nel PoS non è richiesto più un grande sforzo computazionale ma ci si basa sul potere economico che ha un nodo per mantenere la sicurezza della rete, ossia per raggiungere il consenso. Come nel PoW, è possibile manipolare il consenso ottenendo il 50%+1 dei nodi della rete; tuttavia, è quasi improbabile possedere o accordarsi con il 50%+1 dei nodi nel caso di reti molto grandi come Bitcoin o Ethereum.

I validatori ricevono delle reward quando il loro voto è consistente con la maggior parte dei voti degli altri validatori. I validatori ricevono la reward sia nel caso propongano il blocco che votino per validarlo. Di seguito è mostrata la formula utilizzata per il calcolo delle reward, escluse le fee arbitrarie che si possono guadagnare e che dipendono dalla congestione della rete:

$$BaseReward = EffectiveBalance * \frac{BaseRewardFactor}{BaseReawardPerEpoch * \sqrt{\#Balances}} \tag{2.1}$$

In particolare, BaseRewardFactor=64, BaseRewardPerEpoch=4, #Balances esprime il numero di nodi attivi e l'EffectiveBalance esprime quanto è il valore degli ETH depositati in staking dal nodo in questione.

Quindi, da tale formula si capisce che le reward sono direttamente proporzionali alla quantità depositata in staking dal validatore e inversamente proporzionale al numero di validatori della rete. Pertanto, un validatore si trova a gestire il trade off tra concentrare tutte le risorse su un solo nodo permettendo di guadagnare per ogni singola transazione di più, sia per lui che per tutti gli altri nodi, oppure creare più nodi aumentando la probabilità di essere scelto per validare, ma diminuendo le

reward sia per lui che per gli altri.

Inoltre, è previsto un meccanismo di penalizzazione in caso di comportamento scorretto di un nodo. Le penalità per la mancata partecipazione al voto sono uguali alle ricompense che il votatore avrebbe ricevuto se avesse partecipato al voto. Inoltre, non c'è nessuna penalità nel caso di errore nella proposta del nuovo blocco e non sono attribuite penalità nel caso in cui il voto non sia consistente con la maggior parte dei voti.

Lo slashing invece è un'azione più severa, che consente nella rimozione forzata di un validatore e quindi la perdita degli ETH associati a quel validatore. In tal caso, gli ETH però rimangono all'interno del contratto di deposito, solo che non sono più di proprietà di quel nodo. Ci sono 3 casi nei quali un validatore possa essere rimosso dalla rete:

- Proponendo e firmando due blocchi diversi nello stesso slot;
- Votando per un blocco che ne circonda un altro, modificando la cronologia della blockchain;
- Votando per due diversi blocchi candidati nello stesso slot.

2.6.1 Smart contract e Token

Uno smart contract è un insieme di regole che risiedono sulla blockchain per supervisionare uno scambio di asset. Lo smart contract può essere inteso come del codice scritto da sviluppatori e incorporato nella blockchain, che segue solo le sue regole interne ed esegue automaticamente i termini, ossia le clausole di un contratto, di una transazione quando certe condizioni si presentano e senza una terza parte fidata.

Lo smart contract è sancito dall'articolo 8-ter del Decreto Semplificazioni del D.L. 14 dicembre 2018, n.135, convertito in legge con L. 11 febbraio 2019 n.12. In questa circostanza lo smart contract è definito come un programma per elaboratore che opera su tecnologie basate a registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse.

Quindi, gli smart contract sono clausole contrattuali codificate nel linguaggio informatico, che vengono usate per la conclusione di rapporti negoziali, che hanno esecuzione automatica al verificarsi di certe condizioni definite in via preventiva dalle parti. Essendo la condizione contrattuale recepita dallo smart contract attraverso la logica 'if this, then that', esso può dare esecuzione esclusivamente a ciò per cui è stato preventivamente predisposto dal programmatore. Quindi, lo

smart contract dà esecuzione ad una volontà stabilita dalle parti prima, ex ante; pertanto, può affiancare un contratto più ampio in cui le parti perfezionano degli accordi all'esterno della blockchain, in modo classico. Il maggior beneficio è un considerevole aumento dell'efficienza, perché lo smart contract implica:

- Automatizzazione e certezza giuridica dell'esecuzione di obbligazioni contrattuali, visibili a tutti i partecipanti della rete e non solo alle parti coinvolte;
- Trasparenza delle obbligazioni contrattuali e dei loro risultati e risvolti tali da essere preimpostati e quindi 'pre-compresi' da tutti i partecipanti della blockchain;
- Immutabilità delle transazioni registrate e quindi l'impossibilità a modificare o annullare il contratto;
- Replicabilità delle transazioni nel caso in cui vengano immessi gli stessi input nello smart contract.

Talvolta è necessario che gli smart contract debbano aspettare l'accadere di alcuni eventi che si concretizzino nel mondo reale per attivarsi o per generare una transazione. Per questo motivo c'è bisogno di un mezzo che permetta alla blockchain di comunicare con il mondo esterno. Questa possibilità è garantita proprio dagli oracoli, i quali permettono di collegare il mondo reale con il mondo della blockchain, permettendo di immettere informazioni affidabili dall'esterno verso la blockchain. Ad esempio, l'oracolo può connettersi a una determinata borsa valori e portare nella blockchain le informazioni riguardo il prezzo delle azioni o di altri strumenti finanziari. In base a quello che è scritto nel contratto e a ciò che importa l'oracolo, il contratto compirà delle azioni.

Gli oracoli sono strutture esterne alla blockchain che tramite smart contract registrano dati sulla blockchain. Di solito, è preferibile aggregare dati provenienti da diverse fonti per ottenere una verità più oggettiva. Il problema principale degli oracoli è il modo in cui vengono collezionati, filtrati e trascritti i dati su blockchain. Ci sono delle organizzazioni, ad esempio Chainlink, che si occupano della notarizzazione di tali dati sugli smart contract.

Attraverso gli smart contract è possibile creare, movimentare e eliminare i token. Il concetto di token può essere inteso in diversi modi. Pertanto, è bene fare le seguenti precisazioni a riguardo. I token sono dei digital asset che circolano sulla rete blockchain. I digital asset possono essere:

- Nativi: operano in modo indipendente e utilizzano la propria blockchain (ETH per Ethereum o BTC per Bitcoin). Questi nascono insieme alla blockchain e la loro presenza è essenziale per la creazione e la sopravvivenza della blockchain.

- Secondari: rappresentano un valore o diritti che possono essere elettronicamente trasferiti o conservati, programmati su una blockchain già esistente. La loro assenza non intacca la vita della blockchain. I token secondari possono essere implementati solo sulle blockchain Turing Complete, ossia quelle blockchain su cui è possibile eseguire un software, come Ethereum, Polygon, Avalanche, eccetera;

I token non possono essere generati su Bitcoin, in quanto non possiede un vero e proprio linguaggio di programmazione, ma è possibile eseguire solo alcuni script, le cui capacità sono intenzionalmente limitate alla transazione nel quale vengono inseriti. Pertanto, Bitcoin non ha una nozione di stato dal punto di vista della programmazione sulla chain; in particolare è mantenuto lo stato della chain (transazioni, quantità di BTC, ecc..) ma non è possibile salvare delle variabili in generale e poi richiamarle, ma devono essere ripetute per ogni transazione.

Inoltre, i token si differenziano in tipologie in base alla natura tecnologica: fungibili o non fungibili. I token fungibili sono quelli che possono essere scambiati con qualcosa di identico. Alcuni esempi sono: BTC, CBDC, stablecoin oppure i loyalty token come i punti fragola di Esselunga. Invece, i token non fungibili hanno degli attributi unici e identificativi. Questi tipi di token servono per la gestione dell'identità digitale, progetti di tracciabilità digitale (digital twin) o per rappresentare collectibles.

I token si differenziano anche in tre tipologie in base a ciò che rappresentano:

- Utility: i token di utilità sono destinati a fornire l'accesso digitale a un'applicazione o a un servizio;

- Security: i token security rappresentano asset come partecipazioni in sottostanti fisici reali, società o flussi di guadagni o un diritto ai dividendi o pagamenti di interessi. In termini di funzione economica, i token sono analoghi ad azioni, obbligazioni o derivati;

- Payment: i token di pagamento sono sinonimo di criptovalute e non hanno ulteriori funzionamenti o collegamenti ad altri progetti di sviluppo. I token possono in alcuni casi sviluppare solo la funzionalità necessaria ed essere accettati come mezzo di pagamento per un periodo di tempo.

Ogni token, idealmente, può essere costruito ad hoc, ma col tempo sono emersi degli standard comuni per semplificare la creazione sia dal punto di vista tecnico che normativo. Alcuni degli standard più utilizzati sono:

- ERC20: fungibile e può essere utility, security o payment;
- ERC721: non fungibile, rappresenta un unico bene fisico e/o virtuale;
- ERC1155: token standard che ha la capacità di memorizzare sotto il suo controllo, token che possono agire come se fossero un token ERC20 o ERC721, o entrambi allo stesso tempo sotto lo stesso indirizzo.

Attraverso gli smart contract è anche possibile creare delle dApp, le quali sono sostanzialmente delle applicazioni il cui back-end è eseguito totalmente o in parte su blockchain, e facendo riferimento a uno o più smart contract. Uno dei pro delle dApp è che non possono cessare di funzionare e sono sempre raggiungibili, a meno che non sia la blockchain sottostante a smettere di esistere. Inoltre, le dApp garantiscono la privacy, sono incensurabili poiché la blockchain Ethereum è pubblica, garantiscono l'integrità dei dati e sono trustless. Invece, alcuni dei punti a sfavore sono: lo sviluppo e la manutenzione più complessa, le performance che non sono paragonabili a quelle di un server centralizzato, i rischi di congestione della rete e il maggiore sforzo nella realizzazione della UX.

2.6.2 Il layer 2

La transazione è l'operazione più basilare che si può fare sulla blockchain. Ogni transazione modifica lo stato della chain e pertanto, per essere eseguita richiede il pagamento di una certa quantità di ETH, che serve a comprare la quantità di gas necessaria per far avvenire la transazione correttamente. Ogni operazione che consuma le risorse della rete ha un costo. Una transazione ha una finalità in una rete distribuita quando non è possibile cambiarla se non con uno sforzo significativo e disruptive.

Il problema principale delle blockchain è sintetizzato dal trilemma: scalabilità, sicurezza e decentralizzazione. È considerato un trilemma in quanto è impossibile ottenere queste tre caratteristiche appieno e contemporaneamente, ma al massimo due, sacrificando la restante. Per scalabilità si intende la capacità di reagire ad un carico di transazioni sempre maggiore, il che dipende sia dagli algoritmi di consenso che dal numero di nodi della rete. Un'altra criticità da gestire è la congestione della rete, in quanto più la rete è affollata e più bisogna pagare per incentivare i validatori a registrare più velocemente la transazione, perché la rete può processare solo una certa quantità di transazioni per blocco.

Per risolvere questi problemi di scalabilità sono state create le blockchain di tipo layer 2 [7], le quali sono delle blockchain di secondo livello che utilizzano la proprietà di sicurezza della blockchain layer 1 e permettono di essere scalabili nella blockchain

layer 2. La blockchain di tipo layer 2 processa le transazioni sulla propria blockchain e poi le invia al livello 1 per eseguire la prova della validità e immetterle on-chain. Un esempio di blockchain layer 2 è Polygon, il cui funzionamento permette di aggregare i blocchi tramite una procedura crittografica chiamata Merkle Root, che è una struttura ad albero attraverso la quale da un singolo hash che rappresenta il blocco si riesce a risalire a quali sono gli hash dei blocchi che formano l'hash generale. Ad ogni checkpoint, l'hash complessivo viene notarizzato sulla blockchain di Ethereum. Questo meccanismo permette di abbattere i costi e migliorare la scalabilità.
Nella figura 2.5 [8] è rappresentata la procedura del Merkle Root, che permette di ottenere le caratteristiche appena descritte.

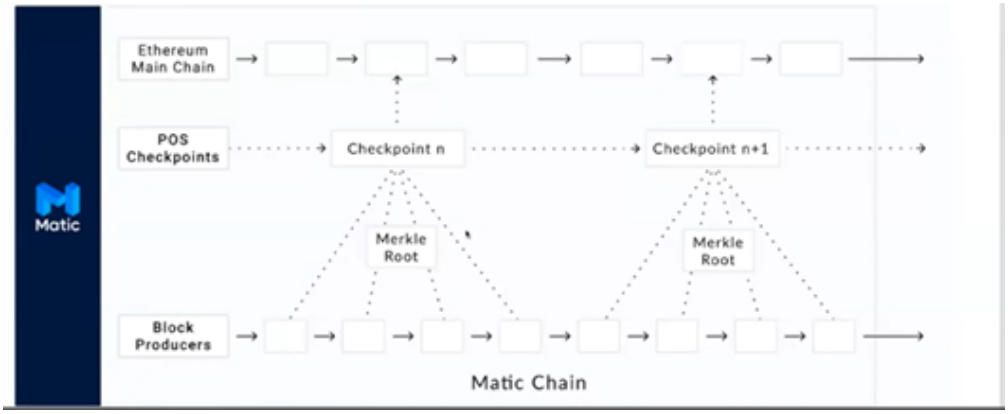

Figura 2.5: Rappresentazione del Merkle Root di Polygon

Capitolo 3

Le possibili applicazioni della blockchain nei diversi settori industriali

Nell'epoca digitale in cui viviamo, la tecnologia si è rivelata una forza di cambiamento profondo che ha un impatto significativo sulla nostra quotidianità e sulle industrie in cui operiamo. Tra le innovazioni più rilevanti degli ultimi anni, la blockchain è emersa come una tecnologia rivoluzionaria, superando il suo ruolo originale di semplice supporto alle criptovalute. La sua capacità di creare un registro condiviso, trasparente e sicuro dei dati ha aperto la strada a una serie di applicazioni innovative in un'ampia gamma di settori industriali.

Questo capitolo si dedicherà all'analisi delle applicazioni della blockchain in vari settori industriali, mettendo in luce le opportunità, i punti di forza, le sfide e le implicazioni economiche associate. Esploreremo in che modo la blockchain stia ridefinendo la gestione delle transazioni aziendali, la protezione dei dati, l'ottimizzazione delle operazioni e la creazione di valore per i clienti. Dal mondo finanziario all'ambito sanitario, dalla logistica alla gestione dell'energia, la blockchain sta emergendo come un'innovazione trasversale, con ciascun settore che offre un terreno fertile per l'adozione della tecnologia, ma allo stesso tempo presentando sfide uniche da superare. Durante il corso di questo capitolo, esamineremo applicazioni specifiche della blockchain in determinati settori, evidenziando come essa possa rivoluzionare processi, migliorare la sicurezza dei dati e creare nuove opportunità economiche. Inoltre, affronteremo le sfide e le preoccupazioni legate all'integrazione della blockchain in questi contesti. Dalla questione della scalabilità alla gestione delle identità digitali e alla conformità normativa, è fondamentale comprendere le criticità che possono emergere nell'adozione di questa tecnologia.

In una ricerca condotta da PwC [1], sono stati mostrati i settori industriali che hanno espresso un maggiore interesse per l'adozione di questa tecnologia. I risultati di questa indagine hanno rivelato che i tre settori più avanzati nell'implementazione della blockchain sono: finanziario, manifatturiero ed energetico, in quest'ordine. La figura 3.1 illustra i risultati dell'indagine condotta da PwC.

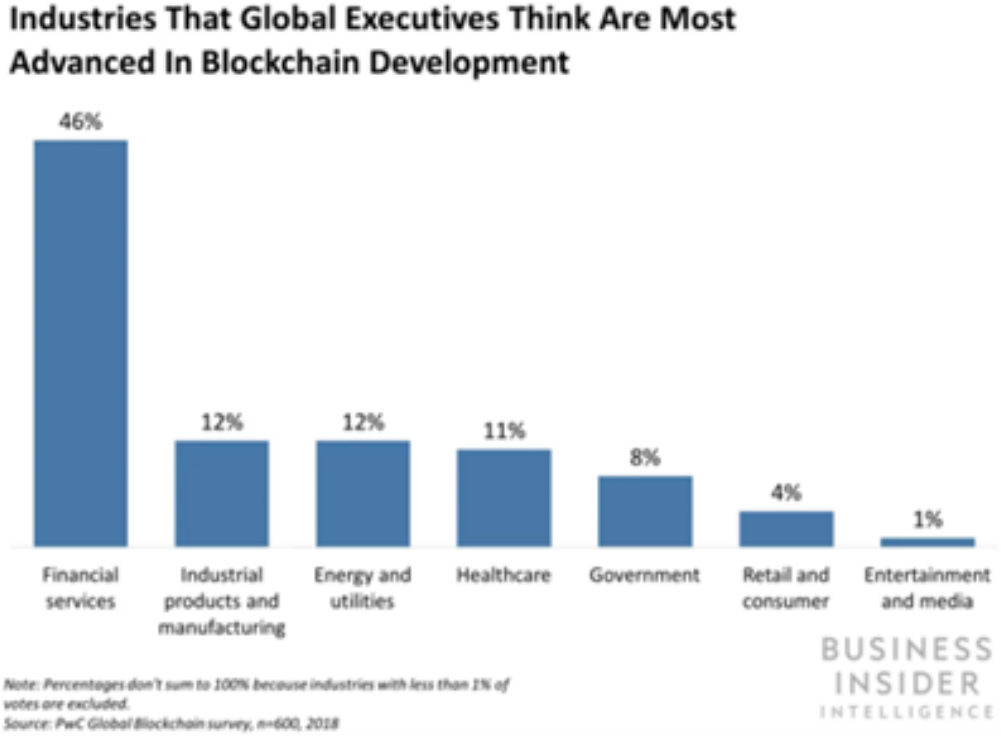

Figura 3.1: I settori industriali più avanzati nello sviluppo della blockchain

3.1 Quando è utile applicare la blockchain

Come molti altri sistemi tecnologici ad alto potenziale sviluppati nel corso del tempo, anche la blockchain è soggetta al rischio di essere sovrastimata o sottovalutata dagli operatori di mercato, mettendo a repentaglio notevoli risorse finanziarie nel primo caso e la competitività aziendale nel secondo. Pertanto, è essenziale adottare un

[1] `https://research.aimultiple.com/blockchain-applications/`

approccio razionale nella decisione d'investimento. PwC [2], fornitore mondiale di servizi professionali di advisory, ha sviluppato un metodo di indagine efficace per determinare in quali circostanze la blockchain possa avere un impatto significativo e positivo su un particolare settore industriale. Questo metodo si basa su 10 domande chiave, alle quali bisogna rispondere in modo binario (sì o no), e le conclusioni sono tratte in base al numero di risposte affermative e negative.

1. C'è una forte necessità di scambi di asset (fisici e virtuali) tra gli attori dell'ecosistema?
2. È necessario disporre di un repository comune tra le diverse parti coinvolte nel processo produttivo?
3. Il processo produttivo è specializzato e complesso, con un certo numero di intermediari?
4. Esiste la necessità di misure di sicurezza robuste?
5. È richiesta una tracciabilità delle operazioni complessa, con "prove" immutabili nel tempo?
6. Si desidera automatizzare i processi e le transazioni quasi in tempo reale?
7. È necessario condividere soluzioni tra i vari attori dell'ecosistema?
8. Per ragioni di conformità, si vuole la possibilità di verificare e monitorare continuamente le diverse fasi?
9. Si intende costruire un processo produttivo basato sulla fiducia tra i diversi attori dell'ecosistema?
10. Si sta considerando l'uso della blockchain per automatizzare i processi aziendali?

Nel caso in cui si risponda in modo affermativo a meno di 4 domande, la blockchain non dovrebbe essere considerata come un'opportunità per migliorare le prestazioni del settore, poiché i costi di sviluppo di tale tecnologia potrebbero superare i benefici. In questo scenario, sarebbe più opportuno ricorrere a soluzioni tradizionali, centralizzate e meno dispendiose. Tuttavia, se le risposte affermative sono pari o superiori a 5, il settore può essere considerato "preparato per la blockchain", con la prospettiva di un notevole aumento della produttività e una

[2] `https://www.pwc.com/us/en/industries/financial-services/library/cryptocurrency-questions.html`

significativa riduzione dei costi.

Inoltre, un altro strumento utile ai fini dell'identificazione del tipo di blockchain da usare è stato fornito dal World Economic Forum [3] nel 2018. Questo strumento è progettato per consentire un'analisi iniziale rapida per determinare se la blockchain è una soluzione appropriata per un problema definito. Non ha l'obiettivo di fornire una risposta finale autorevole, ma di assistere i decision-maker senior nella valutazione di se impegnare risorse nell'esplorazione di una soluzione basata su blockchain per uno specifico ambito di problemi e, in caso affermativo, a quale scala farlo. Si spera che spostare l'attenzione sul problema aziendale e non su una soluzione specifica mitighi gli effetti dell'entusiasmo che circonda questa tecnologia e favorisca un approccio pratico, riducendo il rischio di sperimentazioni avventate. L'albero decisionale è composto da una serie di 11 domande che aiutano a definire se la blockchain è l'approccio corretto per una specifica attività aziendale o meno. Nella figura 3.2 è rappresentato lo schema di cui si è appena parlato:

[3] `https://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf`

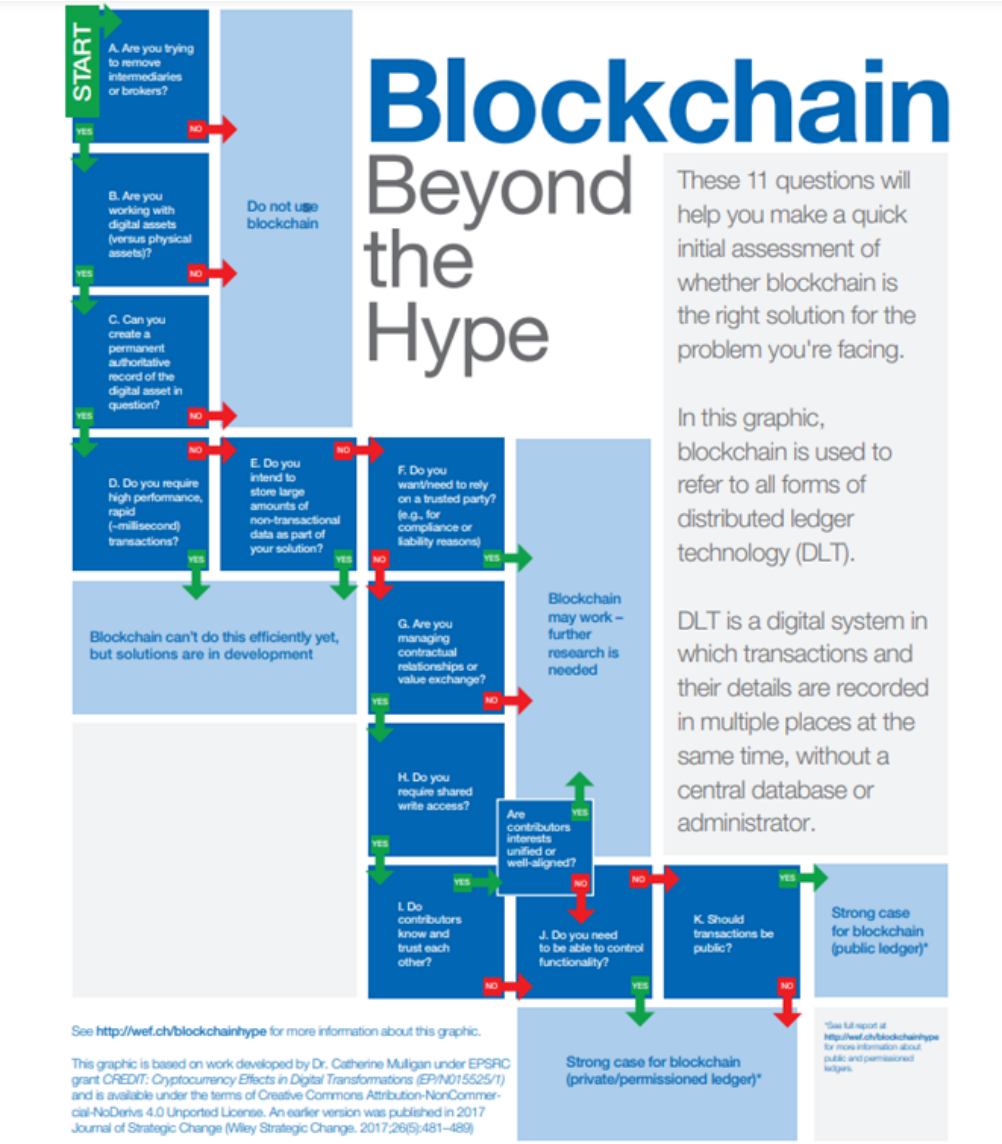

Figura 3.2: Albero decisionale per l'implementazione della blockchain

3.2 Settore edile

Nel contesto dell'Architettura, Ingegneria e Costruzione (AEC), che rappresenta una parte significativa dell'economia, si osserva una notevole frammentazione, con la maggioranza delle imprese operanti come PMI e spesso con limitate competenze digitali. Questi sono anche stati identificati come i fattori limitanti per la crescita della produttività e l'innovazione nel settore AEC. Inoltre, il settore è sotto pressione per migliorare la sua sostenibilità ambientale, vista la massiccia quantità di

materiali consumati e i rifiuti prodotti. Ad esempio, nel Regno Unito, il settore delle costruzioni consuma oltre 400 [9] milioni di tonnellate di materiali all'anno, rendendolo il principale consumatore di risorse naturali del Paese e generando il 62% dei rifiuti totali del Regno Unito. La gestione e lo smaltimento dei rifiuti possono rappresentare fino al 30% dei profitti prima delle imposte delle imprese edili. Queste sfide richiedono una transizione da un modello lineare "prendi-fai-smaltisci" a un approccio circolare e basato sulle prestazioni, con l'obiettivo di mitigare l'impatto ambientale complessivo del settore e allo stesso tempo creare valore.

Nonostante si siano compiuti progressi nella riutilizzazione, riconversione e riciclo dei materiali, l'adozione dei principi dell'economia circolare (CE) nel settore AEC è ancora un'area in evoluzione. Pertanto, la comprensione di come garantire la sua durata a lungo termine è un problema in gran parte inesplorato. L'approccio dell'economia circolare mira a massimizzare il valore dei materiali e dei prodotti, estendendo la loro vita utile e rigenerandoli al termine del ciclo di vita. Spesso, la transizione a un modello circolare richiede una rivisitazione dei modelli di business, una riconsiderazione e una riprogettazione delle pratiche commerciali e un'azione collettiva da parte degli attori nell'ecosistema della catena di approvvigionamento. Tuttavia, l'applicazione dei principi dell'economia circolare spesso si verifica in modo frammentato o non è diffusa su larga scala. La complessità degli edifici, la frammentazione della catena di approvvigionamento a più livelli, la tendenza a breve termine, la mancanza di un caso aziendale chiaro, la mancanza di incentivi e la distribuzione diseguale dei costi e dei benefici rappresentano alcune delle sfide più significative nell'implementazione su larga scala dell'economia circolare nel settore delle costruzioni.

A causa dell'enorme produzione di rifiuti di materiali e delle emissioni di gas serra nel settore delle costruzioni, è essenziale integrare il concetto di economia circolare nella catena di approvvigionamento al fine di aumentare i tassi di riciclaggio. L'utilizzo di dati digitali, automazione, connettività e accesso digitale può affrontare le sfide che il settore delle costruzioni deve affrontare. La blockchain rappresenta una delle soluzioni tecnologiche che sta contribuendo a garantire sicurezza, trasparenza e visibilità nella catena di approvvigionamento. Con ciascuna azienda che mantiene una copia del registro distribuito e ha accesso alle informazioni digitali, il processo diventa completamente automatizzato, evitando il lungo e costoso processo di riconciliazione. La tecnologia blockchain ha il potenziale per trasformare una vasta gamma di attività nella catena di approvvigionamento, dalla tracciabilità dell'origine dei prodotti alla reingegnerizzazione dei processi aziendali e al potenziamento della sicurezza. La condivisione efficiente delle informazioni attraverso la blockchain consente di tracciare in modo trasparente i materiali e altre informazioni ambientali lungo la catena di approvvigionamento delle costruzioni a più livelli per l'intero

ciclo di vita dei prodotti. In termini di benefici nella sostenibilità della catena di approvvigionamento circolare, la blockchain può contribuire a una maggiore tracciabilità e trasparenza dei materiali, alla riduzione delle emissioni di carbonio ed energia, all'ottimizzazione delle risorse e dell'energia, alla migliore collaborazione tra le parti interessate lungo il ciclo di vita del prodotto, all'incremento della qualità dei materiali, alla consegna più rapida, all'aumento della produttività e alla riduzione dei costi operativi.

3.2.1 Esempi di applicazione della blockchain nel settore edile

La prima applicazione della tecnologia blockchain può trovare utilizzo nell'efficace gestione dei progetti di costruzione e nella trasparenza dei pagamenti. Ogni progetto di costruzione di grandi dimensioni comporta contratti complessi e condizioni specifiche. Durante l'intero ciclo di vita di un progetto, è spesso una sfida garantire una collaborazione su tutti i livelli tra tutte le parti coinvolte, conformemente ai termini del contratto. Inoltre, i ritardi nei pagamenti e i problemi connessi alla gestione della liquidità sono problemi persistenti in questo settore.

Vediamo come la tecnologia blockchain possa risolvere queste problematiche nel settore delle costruzioni. Iniziamo dall'esempio dei pagamenti ai lavoratori attraverso gli smart contract. Nel sistema proposto, ogni lavoratore che accede al cantiere edile presenterà la propria carta d'identità per ragioni di sicurezza e salute. Pertanto, le informazioni sui tempi trascorsi sul cantiere saranno ottenute in questo modo e registrate sulla blockchain. Questo registro distribuito basato su blockchain sarà condiviso tra il committente, il consulente e l'appaltatore. Sulla base dei termini concordati riguardanti il numero di ore lavorate, lo smart contract verrà eseguito, e il relativo pagamento verrà inizializzato ai lavoratori.

Lo stesso concetto verrà applicato durante la fase di costruzione. Il team che svolge i lavori di costruzione dovrà essere registrato sulla blockchain, e i compiti loro assegnati dovranno essere menzionati sulla piattaforma blockchain. Durante la costruzione effettiva, è necessario seguire specifiche predefinite e procedure di controllo di qualità, che saranno supervisionate dall'ingegnere del cantiere, dal controllore di qualità e dal project manager. E una volta completata la supervisione, i risultati del controllo di qualità saranno anch'essi registrati sulla blockchain. E se i risultati sono soddisfacenti in conformità con le condizioni predefinite, il contratto intelligente rilascerà il pagamento ai lavoratori e aggiornerà il progresso del progetto.

Tuttavia, la semplice registrazione del completamento del lavoro non è sempre sufficiente, poiché i progetti di costruzione sono molto più complessi. Solitamente sorgono imprevisti, come incidenti gravi legati alla salute e alla sicurezza sul cantiere, che possono comportare reclami e dispute aggiuntive. In un sistema di gestione della costruzione basato su blockchain, ogni incidente legato alla salute e alla sicurezza e ogni registrazione di condizioni di lavoro non sicure sul cantiere possono essere registrati sul registro condiviso, e successivamente possono essere avviate le relative misure di mitigazione del rischio. Per questa fase, l'uso di sensori IoT insieme alla blockchain può essere molto utile, poiché questi strumenti possono fungere da fonte affidabile di dati. Le informazioni critiche ottenute da questi sensori possono essere registrate sulla blockchain e quindi elaborate da un contratto intelligente. Se si raggiungono determinate soglie e livelli di trigger, il contratto intelligente può notificare la persona appropriata sul cantiere per prepararsi alla mitigazione del rischio o per modificare il piano di costruzione. Prendiamo ad esempio una gru; la sua operatività efficace è cruciale per il progresso del progetto, ma allo stesso tempo, eventuali errori nelle sue operazioni possono causare gravi problemi di salute e sicurezza. Con i sensori IoT installati, lo stato operativo di una gru può essere facilmente seguito e registrato sul sistema blockchain. Se i sensori registrano che la gru sta sollevando un peso superiore al suo limite consentito o se ci sono venti estremi che possono mettere a repentaglio la sicurezza dei lavoratori sul cantiere, allora, attraverso un contratto intelligente, verrà attivato un allarme di sicurezza che notificherà l'operatore della gru e il responsabile del progetto sul cantiere per adottare le misure appropriate per prevenire incidenti dovuti a sovraccarichi o cattive condizioni meteorologiche.

Inoltre, la tecnologia blockchain può rivoluzionare la catena di approvvigionamento attuale del settore delle costruzioni, rendendola più robusta. Progettisti, appaltatori e fornitori sono oggi molto più preoccupati dei materiali utilizzati nei progetti di costruzione per motivi quali rigorosi standard di qualità, salute e sicurezza, normative sui materiali e sostenibilità. La soluzione potrebbe essere una blockchain ibrida in cui le imprese utilizzano la chain con permessi per le transazioni in background, mentre i clienti e altri possono effettuare transazioni e accedere alle informazioni collegate a una blockchain pubblica. Questa piattaforma sfrutta i vantaggi della blockchain per fornire una conciliazione automatizzata in cui ogni stakeholder partecipante può conservare una singola copia di un registro distribuito e avere accesso istantaneo alle informazioni aggiornate. La blockchain offre una soluzione ideale per tracciare i materiali da costruzione, come il calcestruzzo prefabbricato o l'acciaio, lungo la catena di approvvigionamento. Inoltre, poiché ogni transazione lungo la catena di approvvigionamento è registrata e visibile sulla blockchain, diventa più semplice tenere traccia della consegna dei materiali. La

supply chain abilitata dalla blockchain può far risparmiare molto tempo nella gestione dei registri dei materiali, che possono essere aggiornati in qualsiasi momento sullo stato di utilizzo.

Per comprendere meglio questo concetto, prendiamo ad esempio una trave d'acciaio. Il ciclo di vita di una trave d'acciaio inizia dalla sua produzione e termina quando viene utilizzata nella costruzione. In questo sistema proposto, ogni trave registrata nel sistema blockchain può essere tracciata attraverso un ID univoco. Inoltre, tutte le specifiche di fabbricazione e progettazione di una trave saranno sempre disponibili sulla blockchain. Inoltre, man mano che la trave d'acciaio si sposta lungo la catena di approvvigionamento, ogni cambio di proprietà e i dettagli del trasporto saranno anch'essi aggiunti alla blockchain. Grazie a questa soluzione abilitata dalla blockchain, l'intera catena di approvvigionamento per la costruzione può diventare trasparente e robusta. La blockchain può anche svolgere un ruolo essenziale nella modellazione delle informazioni sulla costruzione o BIM. Ma per comprendere appieno come la blockchain possa aggiungere valore al BIM, è importante comprendere il concetto di base del BIM. La Modellazione delle Informazioni sulla Costruzione o BIM [4] è un processo che tratta rappresentazioni digitali di beni reali. Questo modello digitale contiene una vasta gamma di informazioni sul bene, come la sua geometria 3D, informazioni sulla gestione della costruzione come tempi, costi e metriche di esercizio e manutenzione del bene. Il BIM è utilizzato per progettare e documentare progetti edilizi e infrastrutturali. Ogni dettaglio di un edificio è modellato nel BIM. Il modello può essere utilizzato per analisi volte all'esplorazione di opzioni di progettazione e per creare visualizzazioni che aiutino gli stakeholder a capire com'è l'edificio dopo la sua costruzione. È importante notare che il BIM è molto più di un semplice modello informatico: include anche il metodo di lavoro digitale, che descrive come il modello si integra nel sistema generale di gestione del progetto, come saranno gestite le informazioni in ingresso e in uscita e come i partecipanti al progetto costruiranno, utilizzeranno e gestiranno il modello. L'implementazione della blockchain può facilitare lo sviluppo del BIM e può persino contribuire a sfruttarne appieno il potenziale. I progetti di ingegneria contengono vaste quantità e tipi di dati e decisioni di progettazione e gestione altrettanto numerose. Una volta implementata la blockchain nel BIM, può fungere da fonte unica di verità per questi dati. In un sistema basato su blockchain, il registro condiviso registrerà un percorso di verifica delle approvazioni di progettazione, la verifica dei dati e le decisioni di gestione del progetto. E queste informazioni fungeranno da fonte unica di verità che coprirà tutti gli aspetti del progetto ed eliminerà qualsiasi tipo di controversia tra le parti coinvolte. Una volta

[4]https://medium.com/techskill-brew/blockchain-applications-in-the-construction

implementata la blockchain, il BIM insieme ad altre informazioni dalla blockchain, come informazioni sulla catena di approvvigionamento, la provenienza dei materiali, i dettagli dei pagamenti, eccetera, renderà il BIM una rappresentazione digitale ancora più completa di un bene reale. Pertanto, attraverso la blockchain, il cliente può garantire la qualità delle forniture valutando i criteri di progettazione stabiliti dal BIM, ai quali l'appaltatore dovrà attenersi. In questo modo, i controlli di qualità saranno molto trasparenti e le collaborazioni diventeranno simultaneamente più efficaci. Pertanto, la blockchain agirà come un'infrastruttura sottostante per rafforzare ulteriormente qualsiasi tipo di modello BIM.

La maggior parte dei progetti non si ferma alla consegna del bene, ma continua fino alla fine del ciclo di vita del bene e proprio per questi casi, il concetto di gemello digitale [10] sta guadagnando terreno nel settore. Il gemello digitale è una rappresentazione digitale di un bene reale. La principale differenza tra BIM e Digital Twin è che il BIM è solo una rappresentazione di ciò che dovrebbe essere l'oggetto del mondo reale. In contrasto, un gemello digitale è una copia digitale di un bene esistente. Un gemello digitale incorpora una visione olistica in cui la gestione, il funzionamento e la manutenzione di un bene vengono eseguiti durante tutto il suo ciclo di vita, dal concetto iniziale alla manutenzione e al riciclo. Il digital twin degli oggetti fisici realizza appieno il suo potenziale con i sensori Internet of Things (IoT). I dati in tempo reale catturati dai sensori IoT installati sugli oggetti fisici/beni possono fornire informazioni in tempo reale sulle prestazioni del bene al gemello digitale. Quindi, il gemello digitale si aggiorna e diventa un cruscotto informativo e uno strumento di reportistica ricco di informazioni per la gestione del bene. In poche parole, un gemello digitale, insieme all'input dai sensori IoT su un bene fisico reale, replica un sistema del mondo reale e cambia con quel sistema nel tempo. Prendiamo ad esempio un ponte, dotato di sensori IoT per misurare il carico veicolare e altre condizioni del traffico. I dati provenienti da questi sensori forniranno al gemello digitale un'informazione sempre aggiornata: il gemello digitale si aggiorna in base ai dati. Attraverso il gemello digitale, il team di manutenzione del ponte può individuare le aree in cui il ponte sta invecchiando o è difettoso e necessita di interventi. In questo modo, la manutenzione preventiva può evitare guasti alle attrezzature prima che si verifichino e ridurre il rischio di incidenti. I dati acquisiti dai sensori IoT [11] saranno registrati sulla blockchain, impedendo così agli hacker di attaccare o manipolare i dati una volta che i dati sono stati aggiunti alla blockchain. Inoltre, i dati registrati serviranno anche come condizione d'ingresso per attivare riparazioni automatiche tramite smart contract. Ad esempio, se una certa parte del bene subisce un guasto inaspettato, attraverso il Gemello Digitale e la Blockchain, sarebbe facile identificare esattamente quali elementi hanno causato il problema, chi era responsabile del suo montaggio e quali aziende di produzione contattare per procurare quella parte. Pertanto, l'integrazione della tecnologia

blockchain può svolgere un ruolo cruciale nell'ottimizzazione delle prestazioni dei progetti, in particolare dove la produttività dei progetti è fondamentale, come nelle autostrade, ferrovie, ponti, edifici, eccetera.

3.3 Settore agroalimentare

Il valore del mercato delle applicazioni blockchain nel settore agroalimentare è pari a 285,34M€ [5] nel 2022 ed è previsto che raggiungerà i 7,378 miliardi di € nel 2031, con un CAGR del 43,76% nel periodo di previsione 2022-2031.

Le moderne catene di approvvigionamento stanno diventando sempre più intricate a causa della globalizzazione. Pertanto, è un fenomeno normale che le organizzazioni esternalizzino la produzione, la logistica e altre attività. Tuttavia, la lunghezza e la complessità della catena di approvvigionamento comportano un aumento della probabilità di frodi sui prodotti e di carenza di fiducia tra le parti coinvolte nella catena di approvvigionamento. Le questioni legate alla sicurezza alimentare sono diventate un problema di rilevanza mondiale e hanno attirato sempre più l'attenzione del pubblico negli ultimi anni, a causa dei numerosi problemi nell'industria alimentare attuale, come lo scandalo della carne di cavallo del 2013 [12] dovuto a frodi sull'etichettatura alimentare in Europa, un focolaio di salmonella in più Stati degli USA nel 2017 e lo scandalo delle uova contaminate in Svizzera, Hong Kong e in 15 stati dell'UE nello stesso anno. Pertanto, la tracciabilità è una richiesta urgente nelle industrie della catena di approvvigionamento, soprattutto nell'agroalimentare.

Inoltre, la maggior parte degli attori nella catena di approvvigionamento alimentare, come produttori e operatori logistici, in particolare le PMI, ha scarsa conoscenza della blockchain e non ha iniziato ad agire su questa nuova tecnologia. Pertanto, anche se la tecnologia blockchain è considerata una tecnologia promettente e una soluzione ideale per aumentare la fiducia tra gli attori multipli nella catena di approvvigionamento e migliorare l'efficienza del flusso di finanza, prodotti e informazioni, essa è ancora nella fase embrionale.

La catena di approvvigionamento alimentare è una catena complessa che include flussi finanziari, flussi di merci e flussi di informazioni, coinvolgendo tutte le imprese collaboranti, dai fornitori di materie prime, ai produttori, ai soggetti logistici, ai grossisti, ai rivenditori e ai consumatori. Il sistema di tracciabilità alimentare è considerato come un sistema di registrazione, che contribuisce a identificare

[5] https://www.insightaceanalytic.com/report/global-blockchain-in-the-agriculture

l'origine di tutti gli input alimentari, come materie prime, additivi e confezioni. Pertanto, i membri della catena di approvvigionamento possono individuare i prodotti interessati da un problema di sicurezza alimentare ed eseguire rapidamente un richiamo del prodotto. I ricercatori concordano tutti sul fatto che una terza parte sia necessaria nella catena di approvvigionamento per garantire l'accuratezza e la sicurezza delle informazioni; poiché la mancanza di coordinamento tra gli attori nella catena di approvvigionamento alimentare causa ritardi nelle informazioni, asimmetria delle informazioni e quindi influisce sulla qualità delle informazioni condivise, causando inefficienza. Sebbene alcune innovazioni applicate per scopi di tracciabilità dei prodotti siano già state utilizzate, come il codice a barre, i tag RFID e l'EDI, è necessario sviluppare ulteriormente applicazioni tecnologiche per la tracciabilità nella catena di approvvigionamento alimentare.

3.3.1 Caso Wal-Mart

Wal-Mart è famoso per la sua efficiente gestione della catena di approvvigionamento attraverso grandi centri di distribuzione e sistemi avanzati di informazione come la Gestione degli Inventari da parte del Fornitore (VMI), lo Scambio Elettronico di Dati (EDI) e l'Identificazione a Radiofrequenza (RFID). Inoltre, Wal-Mart è stato un pioniere nell'adozione della tecnologia fin dall'apertura del primo negozio nel 1962. Ad esempio, quasi tutti i negozi Wal-Mart hanno adottato il sistema di Codice a Barre Universale (UPC) nella metà degli anni '80, il che ha migliorato notevolmente la produttività alla cassa e la gestione dell'inventario, portando all'espansione del settore al dettaglio. Wal-Mart è stato anche uno dei primi a adottare i tag RFID a partire dal 2003 e ha richiesto ai suoi primi 100 fornitori di utilizzare questa tecnologia sulle casse e sui pallet di spedizione entro gennaio 2005 per migliorare la gestione del loro inventario.

Anche per quanto riguarda la blockchain, Wal-Mart è noto per la sua posizione proattiva nell'adozione della tecnologia ed è in prima linea nello sviluppo di una catena di approvvigionamento alimentare basata su blockchain. Ad esempio, Wal-Mart ha aperto il Wal-Mart Food Safety Collaboration Centre (WFSCC) a Pechino nel 2016 [13] e ha collaborato con IBM [5] e l'Università Tsinghua per migliorare la sicurezza alimentare in Cina. Inoltre, uno dei movimenti più avanzati nell'ambito della blockchain è stato rappresentato dai due progetti pilota (per la carne suina in Cina e per i manghi che transitano dall'America del Sud agli Stati Uniti) per migliorare la tracciabilità nella catena di approvvigionamento alimentare, con l'obiettivo di garantire la sicurezza alimentare, migliorare la velocità di richiamo, mantenere una buona reputazione tra i consumatori e ridurre i costi. Wal-Mart ha depositato diversi brevetti per sistemi basati su blockchain, tra cui un sistema di gestione delle cartelle cliniche, un mercato per la rivendita di prodotti acquistati, un

sistema "Smart Package" per tracciare informazioni dettagliate sui pacchi, come il contenuto del pacchetto, le condizioni ambientali e la posizione, e una rete elettrica alimentata da Bitcoin o altre valute digitali.

Walmart è nota da tempo come leader nella gestione della catena di fornitura. Tuttavia, la sua abilità non è riuscita a isolarla da un problema che affligge il settore dei trasporti da decenni: enormi discrepanze nei dati nella fatturazione e nel processo di pagamento per i corrieri, che hanno richiesto costosi sforzi di riconciliazione e causato lunghi ritardi nei pagamenti. Quindi, Walmart Canada ha aperto la strada a una soluzione: ha utilizzato la blockchain per creare un sistema automatizzato per la gestione delle fatture e dei pagamenti ai suoi 70 corrieri di terze parti. Walmart Canada consegna oltre 500.000 spedizioni all'anno a centri di distribuzione e negozi in tutto il Canada, utilizzando sia la propria flotta di autotrasporto che corrieri di terze parti. Il servizio essenziale di spostare un'enorme quantità di merci (molte delle quali deperibili) attraverso confini, fusi orari e climi diversi rappresenta un'enorme sfida operativa. Ad esempio, ogni carico spedito richiede il monitoraggio di punti dati come posizioni delle fermate, litri di carburante e aggiornamenti della temperatura che devono essere calcolati in modo indipendente e incorporati in ciascuna fattura. Con oltre 200 punti dati che dovevano essere presi in considerazione nelle fatture, è facile vedere come il processo di fatturazione e pagamento potrebbe essere pieno di discrepanze nei dati. Inoltre, con il 70% delle fatture che richiedevano sforzi di riconciliazione, si sono verificati costi di transazione più elevati e corrieri insoddisfatti in attesa dei pagamenti. Un'analisi ha identificato la causa principale del problema: l'uso di più sistemi informativi tra Walmart Canada e i suoi operatori che non potevano comunicare tra loro. Di conseguenza, la riconciliazione doveva essere eseguita manualmente: un processo dispendioso in termini di tempo e lavoro, pieno di incoerenze. Uno dei leader tecnologici di Walmart Canada ha suggerito di automatizzare il processo creando una rete blockchain, che supererebbe il problema dei sistemi aziendali incompatibili e stabilirebbe un'unica fonte di verità condivisa per tutte le parti. Ma c'erano degli scettici perché, a quel punto, la tecnologia blockchain non era stata utilizzata in una funzione sostanziale e fondamentale per l'azienda. Inoltre, c'erano molteplici versioni di blockchain. Per aiutarlo, Walmart Canada si è rivolto a DLT Labs, leader nello sviluppo e nell'implementazione di soluzioni aziendali innovative utilizzando la tecnologia di contabilità distribuita. Poco tempo dopo, Bison Transport, uno dei corrieri di Walmart Canada, si è unito al team incaricato di sviluppare una rete. Una versione pilota, che inizialmente coinvolgeva solo Walmart Canada e Bison Transport, è stata lanciata nel gennaio 2019 dopo essere stata esaurientemente testata. Ha avuto successo e nel marzo 2021 la rete, nota come DL Freight, è stata estesa ad altri 69 vettori. Il sistema raccoglie continuamente informazioni in ogni fase: dall'offerta d'acquisto del corriere alla prova di consegna

e all'approvazione del pagamento. Queste informazioni vengono automaticamente acquisite e sincronizzate in tempo reale e sono visibili solo alle parti coinvolte nella transazione. A detta di tutti, il sistema ha avuto un enorme successo. Prima di DL Freight, oltre il 70% [6] delle fatture veniva contestato. Oggi meno dell'1% delle fatture presenta discrepanze e queste controversie possono essere facilmente segnalate e risolte rapidamente. Controlli ed equilibri automatizzati possono e devono essere integrati nel sistema blockchain, sia per prevenire errori che per identificare opportunità per migliorare le prestazioni. Ad esempio, le informazioni del vettore relative alle miglia percorse e al carburante consumato vengono automaticamente confrontate con i dati dell'Internet of Things (IoT) riportati da dispositivi indipendenti sui camion e qualsiasi discrepanza viene immediatamente evidenziata. Questi controlli ed equilibri si traducono in un sistema di autoapprendimento. Poiché più vettori viaggiano tra punti di partenza e di arrivo identici nel tempo, la cronologia delle prestazioni dei vettori viene aggregata e confrontata automaticamente con ogni viaggio successivo, aiutando sia Walmart che i vettori a ottimizzare le loro operazioni.

[6]https://hbr.org/2022/01/how-walmart-canada-uses-blockchain-to-solve-supply-chain

3.3.2 Comparazione tra un normale sistema di tracciabilità con uno basato su blockchain nel settore agroalimentare

Di seguito, presenterò un confronto tra un sistema di tracciabilità tradizionale e uno basato sulla tecnologia blockchain. Per ciascuna di queste soluzioni, è stato esaminato come soddisfano i requisiti dei criteri di confronto e delle caratteristiche tecniche. Nella figura 3.3 [14], è stato utilizzato il colore rosso per evidenziare gli svantaggi o le sfide esistenti, il colore verde chiaro per indicare piccoli vantaggi per il tipo di sistema considerato e il colore verde scuro per rappresentare vantaggi significativi.

Comparison criteria	Traditional electronic traceability system	Electronic traceability system based on blockchain technology
Suitability of database	Records (claimed) variable states, versatile	Records transactions, well suited for recording transformations
Data quality and veracity	Data provider must check and vouch for data quality and veracity	Data provider must check and vouch for data quality and veracity, but fraud frequency may be lower, as risk of getting caught is higher
Immutability, integrity and transparency	Data elements can be overwritten; needs additional recording (transaction log or similar) to document this	Only the transactions are recorded, which means a higher level of integrity and transparency of the claimed values
Confidentiality	Easy to integrate tiered levels of access	Can be done, but to some degree it goes against the philosophy of what a blockchain implementation is meant to support
Trust	Based on trust in the food business and the brand	Still based on trust in the food business and the brand, but trust may be higher because of higher degree of data integrity and transparency
Robustness	Duplication, back-up, and other means of providing robustness must be provided by external processes	Robustness and duplication of data is built into the system
Speed and efficiency	As good as you can get	Significant overhead related to duplication, error checking, consensus mechanisms, and calculating the state of variables based on transactions
Interoperability	There is a plethora of systems, implementations, and database structures, there are a number of standards for TRU identification and Electronic Data Interchange, and there are very few standards defining how the recorded data elements should be named and measured. This means that system interoperability (exchange of data) is a big problem.	Blockchain-based systems are less diverse; they all record transactions (transformations) rather than state values, and they are all immutable. Interoperability and data interchange between blockchain-based food traceability systems is easier than between existing systems, any many of the success stories reported is because a higher degree of interoperability has been achieved.

Figura 3.3: Confronto tra un sistema di tracciabilità tradizionale e uno basato sulla tecnologia blockchain

Ci sono costi e benefici minori legati ai primi cinque criteri di confronto, come

indicato dalla sfumatura verde chiara. I due criteri in cui la differenza tra i sistemi di tracciabilità è maggiore sono "velocità ed efficienza", che favorisce fortemente un sistema tradizionale, e "interoperabilità", che favorisce fortemente un sistema basato su blockchain.

Quando si decide tra un'implementazione tradizionale di un sistema di tracciabilità elettronica e uno basato su blockchain, è importante determinare quali siano le qualità del sistema più importanti. Se la trasparenza, l'integrità e la robustezza del database sono importanti, allora una soluzione basata su blockchain può essere molto rilevante. D'altra parte, se la velocità e la riservatezza dei dati sono considerate le caratteristiche più importanti del sistema, probabilmente un sistema tradizionale di tracciabilità elettronica è migliore.

La rilevanza e l'utilità dell'interoperabilità migliorata non dovrebbero essere sottovalutate. Mentre l'interoperabilità è tecnicamente possibile per i sistemi tradizionali di tracciabilità, è difficile ottenere un gruppo ampio e diversificato di aziende a concordare su quali standard e formati dati utilizzare. È probabilmente più facile ottenere che un ampio e diversificato gruppo di aziende accetti di utilizzare tutti sistemi basati su blockchain, e quindi un'interoperabilità significativamente migliorata sarà un effetto collaterale molto desiderato di tale decisione.

Infine, anche se i sistemi tradizionali possono essere più vecchi e rigidi, hanno quasi sempre punti di forza unici e i dati che contengono sono preziosi. Quindi, invece di insistere sulla sostituzione di tali sistemi, qualsiasi sistema blockchain dovrebbe poggiare sui sistemi legacy delle parti. La sua capacità di farlo è uno dei suoi grandi vantaggi.

3.4 Settore energetico

Il valore globale del mercato delle blockchain nel settore delle utilities energetiche era di 127,5 [7] milioni di dollari nel 2018 e si prevede che raggiungerà i 1.564,0 milioni di dollari entro il 2026, registrando un tasso di crescita annuale composto (CAGR) del 37,6% durante il periodo di previsione.

La tecnologia blockchain sostiene il trading energetico [15] in una vasta gamma di mercati delle materie prime, tra cui l'energia elettrica, il petrolio greggio, il gas naturale e i prodotti raffinati. Le soluzioni basate su blockchain possono essere

[7] `https://www.fortunebusinessinsights.com/industry-reports/blockchain-in-energy-utilities-market-101776`

integrate in ciascun settore aziendale, contribuendo alla produzione, raffinazione, distribuzione e commercio al dettaglio di informazioni legate a prezzi, gestione delle posizioni, logistica e reportistica dei rischi. L'implementazione della tecnologia blockchain offre opportunità come il bilanciamento in tempo reale delle transazioni tra offerta e domanda e la possibilità di effettuare trading energetico peer-to-peer, nonché di collegare stazioni di ricarica per veicoli elettrici (EV). A causa di questi fattori, l'interesse delle organizzazioni di servizi pubblici per la tecnologia blockchain sta crescendo.

Nonostante la blockchain sia stata applicata in vari settori energetici come quello petrolifero e del gas naturale, è importante dire che il settore in cui questa tecnologia abbia trovato più terreno fertile è quello della produzione di energia elettrica. Ciò è dovuto a delle caratteristiche intrinseche che il settore dell'energia elettrica possiede a differenza degli altri sottosettori dell'energia. In particolare:

1. Struttura del mercato: Il mercato dell'energia elettrica è spesso più frammentato e decentralizzato rispetto al mercato del petrolio e del gas. Ciò significa che ci sono più attori indipendenti, come produttori di energia rinnovabile, consumatori finali e veicoli elettrici, che possono trarre vantaggio da una piattaforma blockchain per il trading e la gestione dell'energia.

2. Energia rinnovabile: La produzione di energia elettrica da fonti rinnovabili, come il sole e il vento, è in crescita. La blockchain può aiutare a gestire in modo più efficiente l'energia generata da queste fonti, consentendo agli utenti di condividere l'energia in eccesso con la rete o di negoziarla direttamente tra loro.

3. Digitalizzazione dell'energia elettrica: Il settore dell'energia elettrica è stato più rapidamente digitalizzato rispetto al settore petrolifero e del gas. Questo ha reso più facile l'adozione della tecnologia blockchain, poiché la digitalizzazione è una base essenziale per sfruttare appieno il potenziale della blockchain.

Indipendentemente dall'origine dell'energia elettrica, essa viene trasportata attraverso reti elettriche e distribuita in base alle necessità dei consumatori. L'eccezione a questa fase di trasmissione si verifica solo in presenza di impianti fotovoltaici o parchi eolici offshore. L'energia elettrica è prodotta da diversi produttori in varie nazioni e successivamente scambiata attraverso un mercato. Per fornire energia ai consumatori, sono necessari due tipi di servizi. Uno è fornito dall'operatore di rete, responsabile del trasporto e della distribuzione dell'energia elettrica, dalla sua consegna dai produttori ai consumatori e dal monitoraggio dei consumi energetici dei clienti. L'altro servizio è offerto dai commercianti. Nella maggior parte dei

paesi europei, si opera in un mercato aperto, il che significa che il consumatore non può scegliere l'operatore di rete, ma può selezionare il fornitore di energia elettrica in base al prezzo di acquisto proposto. L'industria energetica presenta una caratteristica peculiare: l'energia elettrica è difficile da stoccare su larga scala come una merce fisica. Il principale ostacolo è che l'energia elettrica deve essere generata in quantità sufficiente per soddisfare le esigenze di tutti gli utenti, ma per farlo è necessario prevedere in anticipo il consumo energetico. Nonostante il sistema di fornitura energetica sia oggi molto automatizzato e moderno, specialmente se confrontato con le sue fasi iniziali di sviluppo, la presenza umana in questo sistema limita notevolmente le sue potenzialità, inclusa la capacità di ridurre il ciclo di pianificazione e di aumentare la scala. Per superare queste sfide, è necessario un sistema che soddisfi i seguenti requisiti:

1. la capacità di pianificare automaticamente il consumo e la distribuzione a livello micro.
2. la possibilità di scalare orizzontalmente il sistema, con la possibilità di testarlo inizialmente in una comunità separata.
3. la massima fiducia nell'integrità del sistema.

La tecnologia Blockchain [16] risponde a tutti questi requisiti. Le sue caratteristiche principali consentono di effettuare microtransazioni, di garantire la scalabilità e di fornire un elevato livello di fiducia.

3.4.1 Relazione tra blockchain e settore dell'energia

La tecnologia Blockchain sta progressivamente assumendo un ruolo di rilievo nel mondo moderno e, quando ci si riferisce al settore energetico, la Blockchain viene impiegata per una varietà di scopi. In tutti i casi, però, la tecnologia Blockchain garantisce trasparenza nel settore della vendita di energia, promuove la disciplina nei pagamenti, ottimizza i costi dell'acquisto di elettricità e gestisce il consumo stesso. Nel Parlamento europeo[8] sono state condotte ricerche sulle potenziali applicazioni della tecnologia Blockchain nel settore energetico. Ci sono diverse situazioni in cui l'utilizzo della tecnologia Blockchain nel settore energetico può migliorare il funzionamento del settore stesso:

1. La tecnologia del Registro Distribuito (DLT) permette alle famiglie di generare energia verde e di scambiarla tra vari partecipanti, contribuendo a cambiare e democratizzare il settore energetico.

[8] `https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_IT.pdf`

2. La DLT può agevolare la creazione di un nuovo ecosistema commerciale, facilitare lo scambio di energia nei veicoli elettrici e garantire un rigoroso controllo dei certificati di carbonio e del tracciamento delle energie rinnovabili, migliorando la rendicontazione energetica.

3. I meccanismi alternativi di pagamento e donazione implementabili tramite le DLT possono contribuire a sostenere l'elettrificazione delle comunità rurali svantaggiate.

4. La DLT promuove la ricerca di nuove soluzioni tecniche a basso consumo energetico e rispettose dell'ambiente.

La tecnologia Blockchain costituisce la base per il monitoraggio automatico, il tracciamento e la registrazione delle informazioni, svolgendo un ruolo fondamentale in un settore tanto vitale. Un tratto distintivo della tecnologia Blockchain è l'assenza di forme di credito, il che significa che, per motivi tecnologici, non è possibile ricevere elettricità non pagata né fornirla senza ricevere il dovuto pagamento.

Nel contesto dell'Internet dell'Energia, la tecnologia Blockchain può essere applicata in sei differenti contesti:

1. Veicoli Elettrici - Le auto elettriche rappresentano una soluzione efficace per affrontare le problematiche ambientali, ma una delle sfide principali è la disponibilità limitata di stazioni di ricarica. La tecnologia Blockchain può contribuire a migliorare la situazione mediante stazioni di ricarica private basate su smart contract e registri distribuiti. Le applicazioni sviluppate per i veicoli elettrici consentono agli utenti di registrare le proprie stazioni di ricarica e di metterle a disposizione degli altri utenti. Il pagamento avviene in base al tempo di utilizzo della stazione attraverso l'uso di smart contract.

2. Protezione delle Informazioni - Il sistema informativo dell'Internet dell'Energia si basa sulla tecnologia Blockchain grazie ai benefici della decentralizzazione, che contribuisce a risolvere questioni legate alla sicurezza. I principali problemi per i sistemi fisici e informativi sono la fuga di informazioni, gli attacchi informatici e i virus. La tecnologia Blockchain è in grado di operare in tempo reale e, grazie alla sua natura decentralizzata, impedisce la modifica o la cancellazione delle informazioni nei blocchi della catena.

3. Certificazione e Scambio di Carbonio - La tecnologia Blockchain può fornire al mercato del carbonio un sistema in grado di tracciare il flusso del carbonio, registrando tutte le transazioni e i certificati. Identificatore, data e registro

vengono conservati nei blocchi della catena, e il commercio del carbonio avviene tramite smart contract.

4. Virtual Power Plant - Questo settore dell'Internet dell'Energia sfrutta la caratteristica principale della tecnologia Blockchain: la decentralizzazione. Questa caratteristica aiuta le virtual power plant nella pianificazione e distribuzione delle risorse. Tuttavia, le transazioni tra virtual power plant e utenti possono comportare costi elevati. Nell'ambito delle applicazioni transazionali, la tecnologia Blockchain offre affidabilità e trasparenza, oltre a piattaforme che risultano più convenienti dal punto di vista finanziario. La tabella 3.1 [17] mostra un confronto tra una VPP tradizionale e una basata sulla tecnologia Blockchain.

	VPP convenzionale	**VPP basata su blockchain**
Trasparenza dell'informazione	Basso	Alto
Sicurezza del sistema informativo	Basso	Alto
Costi di transazione	Alto	Basso
Informazione lato domanda	Non in tempo reale	In tempo reale

Tabella 3.1: Confronto tra VPP convenzionale con VPP basata su blockchain

5. Sinergia del sistema multi-energetico - Nel mondo reale, ci sono diverse fonti di elettricità ed è molto difficile combinarle in un unico sistema per il controllo e il funzionamento a causa delle diverse caratteristiche fisiche dell'energia. Gli scienziati propongono di utilizzare la tecnologia Blockchain per unire l'elettricità in un unico sistema o piattaforma, indipendentemente dalla fonte. La Blockchain registra le informazioni sulla produzione e i costi in tempo reale in qualsiasi sistema energetico. Poiché la Blockchain consente di lavorare in un sistema in tempo reale, è possibile generare prezzi marginali di diverse fonti di energia in diverse regioni anche in tempo reale. Le informazioni sui prezzi marginali consentono di ottimizzare il funzionamento dei sistemi, seguire istruzioni automatiche ed effettuare calcoli dei costi tramite l'uso di contratti intelligenti.

6. Domanda di elettricità - Grazie ai servizi di risposta alla domanda, è possibile rispondere rapidamente al bisogno di elettricità, rappresentando anche lo strumento tecnico più economico per fornire riserve. Tuttavia, in relazione a questa risposta rapida, sorgono problemi riguardo al controllo dell'elettricità, la misurazione dell'elettricità e altri aspetti.

3.4.2 Blockchain per portare efficienza nel mercato dei carbon credit

Il Protocollo di Kyoto ha introdotto tre meccanismi basati sul mercato per contrastare e ridurre l'aumento recente della concentrazione di gas serra (GHG), stimolare lo sviluppo sostenibile attraverso il trasferimento di tecnologia e investimenti, e promuovere sforzi di conservazione dell'energia e riduzione delle emissioni nel settore privato. Il principale focus di questi meccanismi è sul principale GHG, ossia il biossido di carbonio (CO2). I crediti di carbonio sono stati identificati, insieme alla tassa sul carbonio, come la strategia più efficace dal punto di vista dei costi contro il cambiamento climatico, poiché rappresentano una strategia vantaggiosa per facilitare la mitigazione dei GHG. Possono essere definiti come sistemi di "compensazione" al fine di garantire l'equilibrio tra le emissioni di GHG e la quantità di mitigazioni certificate. Questa strategia consente agli attori che non possono permettersi di mitigare direttamente le proprie emissioni di compensarle acquistando crediti da altri attori, mentre premia i produttori netti di mitigazioni consentendo loro di vendere le loro mitigazioni certificate. Un tale sistema ha portato allo sviluppo di mercati del carbonio adeguati allo scambio dei crediti. Tuttavia, i crediti di carbonio presentano diversi problemi [9], tra cui:

- Mancanza di standardizzazione: Il mercato dei crediti di carbonio è stato caratterizzato dalla mancanza di standardizzazione nelle metodologie di misurazione e certificazione delle riduzioni delle emissioni. Ciò ha reso difficile il confronto tra diversi progetti e la verifica dell'efficacia delle riduzioni delle emissioni;
- Rischio di double spending: A causa della mancanza di un sistema centralizzato di registrazione delle riduzioni delle emissioni, esiste il rischio di doppio conteggio, cioè la stessa riduzione delle emissioni potrebbe essere reclamata da più parti;
- Speculazione e frode: In alcuni casi, il mercato dei crediti di carbonio è stato soggetto a speculazione e frode, con operatori che cercano di trarre vantaggio da schemi di investimento poco chiari.

L'uso della tecnologia blockchain per tokenizzare crediti di carbonio e altri schemi di incentivi ambientali può fornire una piattaforma di gestione intelligente per la certificazione e il commercio dei diritti di emissione di carbonio, introducendo benefici rilevanti. Potrebbe rafforzare il monitoraggio, la segnalazione e la verifica degli impatti delle azioni climatiche; migliorare la trasparenza e la tracciabilità delle azioni climatiche evitando manipolazioni e asimmetrie informative; accorciare radicalmente il ciclo di sviluppo degli asset di CO2 e ridurre i costi di transazione legati alla certificazione dei crediti di carbonio; costruire fiducia tra le azioni

climatiche; creare meccanismi inventivi per le azioni climatiche accessibili a tutti; e sostenere la mobilitazione delle finanze verdi.

3.5 Settore assicurativo

Il mercato globale delle blockchain nel settore delle assicurazioni è stato valutato a 496,9 [9] milioni di dollari nel 2021 e si prevede che raggiungerà i 32,9 miliardi di dollari entro il 2031, con un tasso di crescita annuale composto (CAGR) del 52,4% dal 2022 al 2031.

L'attenzione del settore assicurativo verso tale tecnologia è tangibile anche in Italia; infatti, nel 2021 il settore che ha avuto più applicazione della tecnologia blockchain è stato quello finanziario e assicurativo (con il 50% [10] degli investimenti).

Un rapporto di Juniper Research [11] ha mostrato che l'assicurazione basata su blockchain trasformerà l'amministrazione dei sinistri; risparmiando 10 miliardi di dollari in costi a livello globale entro il 2024, rispetto a 1,1 miliardi di dollari nel 2021. I fornitori di assicurazioni sfrutteranno sempre di più i vantaggi dell'aumentata trasparenza dei processi e della condivisione dei dati in tempo reale. I dati presenti sulle reti blockchain sono accessibili a tutte le parti, eliminando la duplicazione degli sforzi e riducendo al minimo le frodi. Entro il 2030 le polizze assicurative verranno fatte per l'80%[12] online, con una crescita annuale media del +22%. Secondo un rapporto di Bain [13], il valore complessivo delle assicurazioni globali al 2030 sarà di circa 10 mila miliardi di dollari. Il settore assicurativo, quindi, subirà una crescita esponenziale rispetto alla situazione attuale, e non è difficile immaginare che questa crescita possa trovare un validissimo alleato nella blockchain.

Uno studio della BCG rivela che il settore assicurativo, dall'applicazione della digitalizzazione su larga scala, trarrebbe vantaggi pari ad una riduzione dell'indicatore denominato "combined operating ratio", che rappresenta il rapporto fra spese generali e costi di risarcimento dei sinistri sulla raccolta premi assicurativi, tra il 5% e il 13%, che equivarrebbe a circa 200 miliardi di dollari. Ciò sarebbe dovuto anche dal fatto che le blockchain hanno il potenziale per rendere altre tecnologie digitali,

[9] `https://www.alliedmarketresearch.com/blockchain-in-insurance-market-A11767`

[10] https://www.repubblica.it/tecnologia/2022/01/21/news

[11] https://www.juniperresearch.com/press/blockchain-based-insurance-claim

[12] https://www.insuranceup.it/it/business/polizze-digitali-entro-il-2030-saranno-l80

[13] https://www.bain.com/insights/the-future-of-insurance-as-risks-mount-insurers

come le analisi avanzate, l'intelligenza artificiale (IA) e i software di automazione, molto più produttive.

Le compagnie di assicurazioni [18] possono sviluppare una blockchain che coinvolge solo l'assicurazione o possono incorporare aspetti dell'ecosistema circostante. Le differenze nelle caratteristiche tra le blockchain comportano che, nel caso delle blockchain specifiche per l'assicurazione, si ottengano maggiori benefici in termini di efficienza nelle attività manuali e di verifica, oltre a una riduzione dei tempi di gestione. Nel caso delle blockchain integrate nell'ecosistema assicurativo, la vasta disponibilità di dati consente alle compagnie di ottenere una maggiore profondità nell'analisi dei rischi, conferendo loro un vantaggio competitivo nell'offrire prodotti adattati alle specifiche sfide dell'ambiente in cui operano. La figura 3.4, creata da BCG[14], mostra la comparazione dell'impatto sui tempi e sui costi di una gestione di un sinistro tradizionale con una basata su blockchain.

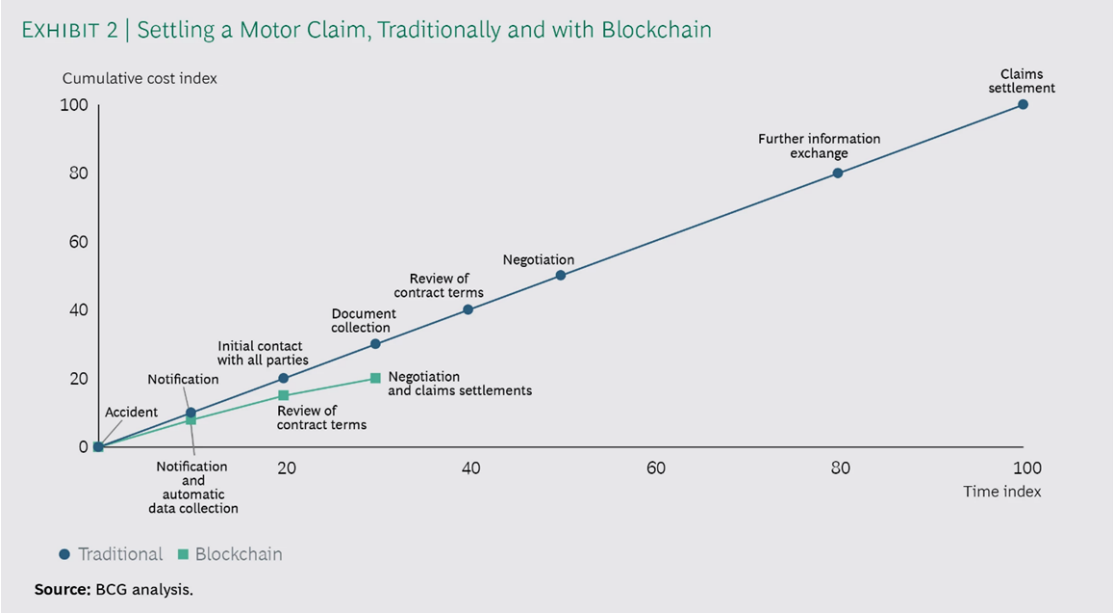

Figura 3.4: Differenza della gestione di un sinistro con o senza blockchain

La tecnologia digitale non viene adeguatamente sfruttata per supportare la determinazione dei premi o l'identificazione di frodi. Attraverso l'impiego di dati provenienti da diverse fonti e integrati in una blockchain, come ad esempio i dati

[14] `https://www.bcg.com/publications/2018/first-all-blockchain-insurer`

telemetrici di un veicolo, le segnalazioni di polizia del proprietario del veicolo e il registro delle riparazioni, è possibile ottenere una valutazione più precisa del profilo di rischio di un individuo, compresa la probabilità di presentare richieste fraudolente.

Le blockchain, sia quelle specifiche per l'ambito assicurativo [19] che quelle integrate nell'ecosistema, consentono alle compagnie di assicurazione di sfruttare gli smart contract per automatizzare ulteriori processi operativi. Si immagini quanto la burocrazia potrebbe essere ridotta mediante la registrazione di un'assicurazione sui voli, un tipo di copertura relativamente semplice, su una blockchain. Attualmente, la gestione dei reclami in caso di ritardo di un volo assicurato richiede una significativa quantità di lavoro manuale. L'assicurato deve raccogliere documentazione dall'aeroporto di destinazione relativa all'orario esatto di arrivo, mentre l'assicuratore deve verificare la fonte e l'accuratezza della documentazione e confrontarla con il contratto di assicurazione. Solo dopo aver completato questi passaggi è possibile effettuare il pagamento, spesso senza generare un margine positivo. Mediante l'utilizzo di una blockchain, l'intero processo potrebbe essere automatizzato. Un ritardo di volo confermato dai dati dell'aeroporto scatenerebbe automaticamente un pagamento, che verrebbe immediatamente accreditato sul conto dell'assicurato al momento del suo arrivo a destinazione. Fizzy, un servizio offerto dalla compagnia di assicurazioni AXA in Francia, già offre un'assicurazione sui voli che utilizza la tecnologia blockchain in questo modo.

3.5.1 Tecnologie a servizio della blockchain nel mondo assicurativo

La tecnologia blockchain rappresenta un passo fondamentale e cruciale nell'evoluzione del settore assicurativo attraverso l'adozione delle opportunità offerte dalla digitalizzazione. Il valore aggiunto [20] significativo viene dato dall'integrazione dell'Internet delle cose (IoT), dell'analisi dei dati (Data Analytics) e dell'intelligenza artificiale (AI) nella blockchain. IBM ha già sviluppato una piattaforma che, grazie a sensori IoT, è in grado di rilevare i comportamenti a rischio del conducente e le violazioni delle norme stradali, oltre a raccogliere una vasta gamma di informazioni riguardanti aspetti tecnici del veicolo, condizioni meteo, traffico e percorso, mettendo tutto a disposizione quasi in tempo reale. Questa innovazione può essere sfruttata dalle compagnie assicurative per offrire servizi personalizzati in base al profilo di ciascun conducente e può essere replicata per milioni di veicoli in circolazione. Questo ci permette di valutare concretamente l'impatto economico e sociale di tali soluzioni.

3.5.2 Ostacoli tecnici e gestionali per la diffusione della blockchain nel settore assicurativo

Attualmente, l'idea di sviluppare una compagnia di assicurazioni basata completamente su blockchain rappresenta solo un progetto in fase di sviluppo. Tuttavia, esistono ostacoli significativi sia di natura gestionale che tecnologica che devono essere affrontati prima di poter realizzare questa visione:

- Collaborazione: La creazione di una blockchain che coinvolga partecipanti esterni richiede un attento bilanciamento, specialmente quando questi partecipanti esterni sono concorrenti. Le aziende devono essere disposte a condividere alcune parti delle loro operazioni, che potrebbero essere considerate come elementi distintivi rispetto alla concorrenza.

- Conoscenza: La maggior parte delle compagnie assicurative ha avuto una limitata esposizione alle blockchain e non comprende appieno come questa tecnologia potrebbe contribuire alla loro strategia aziendale. Inoltre, potrebbero mancare delle competenze tecniche necessarie per avviare un pilota di progetto basato su blockchain, e queste lacune devono essere colmate attraverso la formazione.

- Governance: Mentre le blockchain pubbliche, come quelle utilizzate da Bitcoin, sono aperte a tutti e seguono spesso un modello di governance open-source, le blockchain rilevanti per le compagnie assicurative tendono a essere private, limitate a compagnie assicurative, partner e clienti invitati. Questo richiede un approccio di governance diverso, che può diventare complicato quando è necessario bilanciare i benefici con l'aumento dei partecipanti.

- Standard e Protocolli: La blockchain è ancora una tecnologia giovane, e ci sono stati vari tentativi di impostare degli standard per l'avvio e la gestione delle blockchain individuali. Questi standard non sono sempre compatibili tra loro, e le tecnologie o i "protocolli" che dovrebbero garantire l'interoperabilità non sono sempre utilizzati in modo uniforme. Inoltre, è importante notare che i regolatori non hanno ancora emesso linee guida definitive riguardo agli standard blockchain.

3.6 Settore del lusso

La lotta dell'industria della moda di lusso [21] contro la contraffazione dura da decenni, con i marchi che spesso investono risorse proprie per fermare la distribuzione di prodotti falsi e recuperare i clienti ingannati, a causa di un sostegno non sempre sufficiente e omogeneo da parte dei regolatori a livello globale. Con la crescita del

mercato di seconda mano e del suo sviluppo nei canali online, i contraffattori e i proprietari di prodotti falsi hanno scoperto nuovi modi per ottenere profitto.

Storicamente, i marchi di moda di lusso realizzavano i loro prodotti artigianalmente in piccole quantità nella loro regione d'origine. La combinazione di una lavorazione di alta qualità e la percezione della rarità dei prodotti giustificava i loro prezzi elevati. I consumatori che desiderano possedere articoli di lusso ma non possono permetterseli a prezzo pieno o che si interessano alla sostenibilità stanno sempre più rivolgendo la loro attenzione al crescente mercato dei prodotti di lusso di seconda mano, che è stato valutato a 4,9 [15] miliardi di euro nel settore del lusso nel 2021. La figura 3.5 è una previsione dello sviluppo del mercato globale dei beni di lusso di seconda mano.

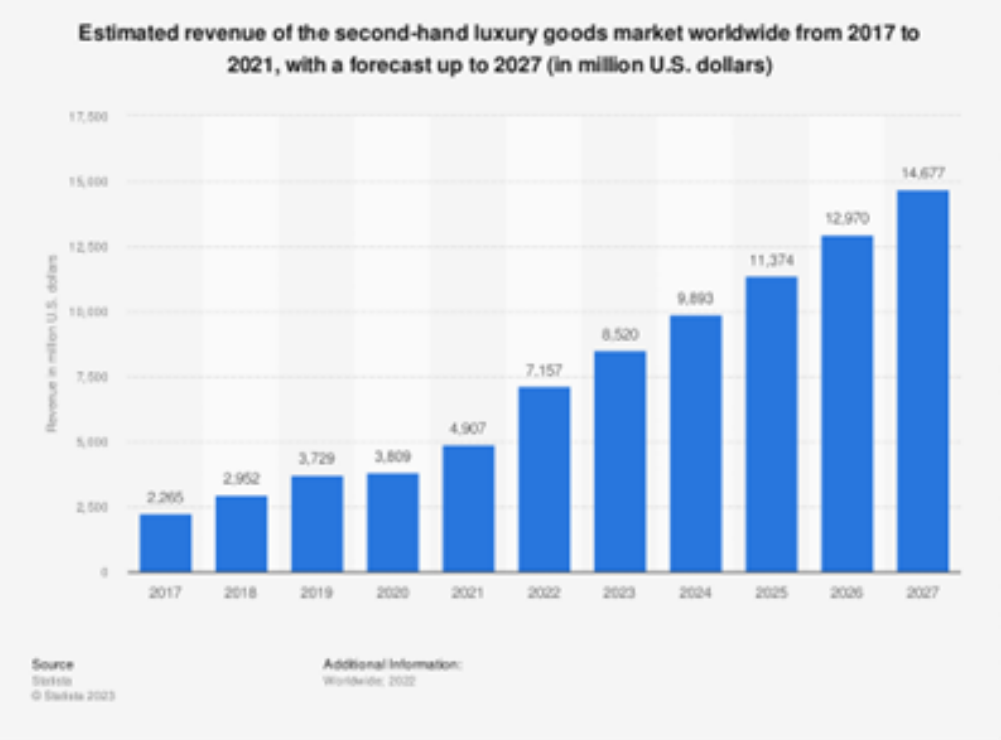

Figura 3.5: Previsione della grandezza del mercato dei beni di lusso di seconda mano

L'acquisto di articoli usati può portare a incertezze riguardo all'autenticità. Molti

[15] `https://www-statista-com.ezproxy.biblio.polito.it/statistics/1315892/secondhand-luxury-market-revenue/`

brand di lusso non offrono prodotti di seconda mano, quindi il mercato della rivendita è controllato da venditori non affiliati direttamente ai marchi di prestigio. I acquirenti devono fidarsi dei venditori e dei documenti di autenticità lungo il ciclo di vita del prodotto. Ma la produzione di articoli contraffatti è diventata molto sofisticata, rendendo difficile distinguere il vero dal falso, un compito riservato a pochi esperti nel mondo. Le contraffazioni costano miliardi ai brand ogni anno. La produzione di prodotti falsi è cresciuta notevolmente grazie alla riduzione dei costi di fabbricazione nelle aziende asiatiche.

Il rapporto globale sulla contraffazione di marchi del 2018 ha stimato che la contraffazione ha causato perdite di 98 miliardi di dollari nel 2017, di cui le vendite online di prodotti contraffatti hanno rappresentato 30,3 [16] miliardi di dollari. Tuttavia, è difficile misurare le perdite effettive. In effetti, è molto probabile che gli acquirenti di prodotti contraffatti non avrebbero mai acquistato prodotti autentici in primo luogo. Ciò non significa che la contraffazione non sia dannosa per i marchi di lusso, ma che i suoi effetti sono piuttosto insidiosi.

Il prestigio del lusso si basa sull'unicità e la scarsità. Se un articolo di lusso diventa comune, perde il suo valore sul mercato, vanificando gli investimenti in ricerca, design e pubblicità. Con l'avanzare della qualità delle imitazioni, diventa sempre più arduo distinguere il falso dall'autentico, causando danni significativi ai marchi di lusso. Di conseguenza, la contraffazione impatta i brand in vari modi: perdite economiche, riduzione dei profitti, sovrapproduzione, reclami fraudolenti sulla garanzia, richieste di risarcimento per danni o lesioni, e danni all'immagine del marchio e del prodotto.

La tecnologia blockchain può essere una soluzione alla contraffazione e può fornire ai marchi maggiore controllo sulle vendite di prodotti di seconda mano, non sottovalutando l'incremento della fidelizzazione che ne deriverebbe da iniziative post-vendita intraprese nei confronti dei clienti. Quindi, dando ai prodotti di lusso fisici un'identità digitale, sia il marchio che il consumatore possono tracciare il loro ciclo di vita dalla produzione delle materie prime ai proprietari, dimostrando la loro autenticità. Inoltre, la tecnologia blockchain può ridurre significativamente i costi operativi nel settore della moda e del lusso al dettaglio fornendo migliori strumenti di gestione dei dati, migliorando la gestione della catena di approvvigionamento e riducendo il rischio di mercati di prodotti contraffatti e grigi. La blockchain fornisce uno strato leggero e facilmente integrabile per la riconciliazione dei dati tra le linee di servizio e le operazioni. L'autenticità della tecnologia blockchain è

[16] https://uk.fashionnetwork.com/news/Luxury-brands-lose-30-3-billion

una grande opportunità per i marchi di lusso alle prese con il crescente volume di prodotti contraffatti, specialmente nel mercato di rivendita. Si stima che uno su dieci prodotti di marca venduti sia falso, con l'OCSE che stima il mercato della contraffazione valere 3 [17] trilioni di dollari nel 2022.

3.6.1 Aura Blockchain

Il Consorzio Blockchain Aura [22] è stato istituito nel mese di aprile del 2021 come il primo consorzio globale del lusso al mondo e ha visto la partecipazione di tre importanti attori del settore del lusso: LVMH, il Gruppo Prada e Cartier (che fa parte di Richemont). A ottobre 2021, si è unito al consorzio anche il Gruppo OTB. Questa collaborazione tra concorrenti ha dato vita a una soluzione innovativa per affrontare le sfide comuni relative all'autenticità, alla responsabilità nell'approvvigionamento e alla sostenibilità in un contesto digitale sicuro.

Fino a questo momento, sono stati creati oltre 15 [18] milioni di token che consentono di collegare i prodotti di lusso alla blockchain di Aura. Alcune Maison di LVMH, tra cui Hublot, Bvlgari e Louis Vuitton, sono già attive su questa piattaforma. Questi marchi gestiscono anche i loro dati e si attengono ai più rigidi standard in materia di privacy dei clienti. Le informazioni sono immutabilmente registrate sulla blockchain, rendendole al riparo da qualsiasi manipolazione o tentativo di accesso non autorizzato.

La tecnologia blockchain di Aura utilizza un codice univoco per fornire registrazioni verificate dei prodotti, che includono la cronologia della proprietà, i dati sull'autenticità del prodotto e l'origine dei materiali. Quando un cliente acquista un prodotto, riceve un certificato crittografato che contiene informazioni sulla sua produzione. L'innovativa tecnologia di Aura collega gli identificatori dei prodotti agli identificatori dei clienti, creando una struttura sicura e non duplicabile basata su una catena di blocchi digitali. Questo consente ai consumatori di accedere all'intera storia del prodotto e alla certificazione dell'autenticità in ogni fase del processo, dalla materia prima alla vendita finale. Queste informazioni possono essere associate ai prodotti tramite diversi metodi, tra cui codici QR o etichette RFID, che alcuni marchi, come Prada, stanno già utilizzando. In questo modo, i consumatori possono fare riferimento a dati affidabili per seguire l'intero ciclo di vita del prodotto senza la necessità di convalida da parte di terzi. Aura funge

[17] `https://www.nssmag.com/it/fashion/31263/moda-fake`

[18] https://www.pradagroup.com/it/news-media/press-releases

anche da piattaforma narrativa che consente ai marchi di lusso di comunicare direttamente con i consumatori, condividendo storie uniche sulla qualità dei materiali, sull'artigianato e sulla creatività, rafforzando così il legame tra clienti e marchio.

Per quanto riguarda il funzionamento del sistema Aura, ogni nuovo prodotto viene registrato in modo digitale su un registro condiviso, che è sicuro e non riproducibile, contenente informazioni uniche. Quando un consumatore effettua un acquisto, può ottenere il certificato Aura tramite l'applicazione del marchio. Le informazioni contenute nel certificato vengono mantenute nel tempo, anche quando un prodotto viene rivenduto e successivamente acquistato da altri. Aura è basata su una blockchain privata, il che significa che l'accesso completo ai dati è concesso solo alle aziende che fanno parte della rete (ciascun marchio è l'unico titolare dell'accesso ai propri dati relativi ai marchi e ai clienti). Uno dei principali vantaggi di una blockchain privata è che tutti i partecipanti possono contribuire alle informazioni all'interno dello stesso sistema, ma solo alcuni membri sono autorizzati a consultarle. Inoltre, Aura opera su una rete di soli 30 nodi, garantendo la conoscenza della loro posizione e del consumo energetico.

L'azienda italiana di abbigliamento Loro Piana, che si è unita al consorzio a marzo 2023, ha l'obiettivo di utilizzare la tecnologia blockchain per migliorare la tracciabilità della sua catena di fornitura lungo le varie fasi di possesso dei prodotti. Questo aspetto è particolarmente significativo per i marchi di moda di lusso, che creano prodotti di alta qualità con l'aspettativa che possano essere tramandati di generazione in generazione. L'uso della blockchain da parte di Loro Piana fornisce ai clienti un codice QR univoco che permette loro di seguire il percorso di produzione del prodotto lungo la catena di fornitura. Inoltre, fornisce loro un certificato di prodotto digitale, semplificando il trasferimento di proprietà poiché i clienti possono tracciare la storia di possesso del prodotto fino alle sue origini presso Loro Piana.

LV Diamonds utilizza la blockchain in modo analogo a Loro Piana, fornendo un file digitale crittografato che registra peso, colore, purezza e qualità del taglio di ogni diamante. Queste informazioni, a prova di falsificazione, sono disponibili per ogni possessore di diamanti, garantendo un trasferimento dei dati sicuro, efficiente e affidabile.

Anche i gioiellieri utilizzano la blockchain per verificare le riparazioni dei beni di lusso. Ad esempio, Cartier utilizza la tecnologia blockchain di Aura per convalidare le transazioni di riparazione e condividere le condizioni dei suoi pezzi con i proprietari.

3.7 Vantaggi di questo lavoro di tesi

Viste le problematiche appena elencate che affliggono il settore del lusso, ho pensato insieme ad altri due ragazzi appassionati di blockchain di provare a creare una soluzione, chiamata Watchain, che mira a offrire trasparenza e affidabilità per gli acquirenti di orologi di lusso nel mercato secondario. La soluzione proposta consiste nella creazione di un marketplace C2C in cui l'operazione di compravendita è finalizzata solo dopo che un esperto orologiaio abbia ispezionato con cura l'orologio, preso nota delle caratteristiche del segnatempo e che le abbia immesse su blockchain generando un NFT da consegnare al cliente finale insieme al suo orologio. Ad oggi esistono sicuramente aziende che offrono una parte di quello che vorremmo offrire noi. Ad esempio, esistono piattaforme per la compravendita prettamente di orologi, anche se non dedicate esclusivamente ai privati. Allo stesso tempo, esiste qualche entità che certifica gli orologi tramite NFT, anche se non nel momento della compravendita. In definitiva, la novità apportata da Watchain sta nel mettere insieme queste varie offerte e aggregarle in un'unica soluzione, al fine di aggredire il mercato della compravendita di orologi tra privati, il quale al giorno d'oggi è affetto da forti asimmetrie informative. Per ridurre l'effetto di queste ultime, Watchain si affida alla blockchain, la quale è portatrice di trasparenza e affidabilità.

Capitolo 4

Watchain

Watchain è un progetto startup nato a giugno 2023 in occasione del Project Work lanciato da MasterZ, un corso formativo e introduttivo alla tecnologia Blockchain. Il progetto è stato ideato da me, Leonardo Scantamburlo (full stack developer) e Mirco Zancone (UX/UI designer). In questo capitolo verranno descritti l'architettura del sistema, dello smart contract e delle funzionalità che caratterizzano l'attuale configurazione dello smart contract. Dopodiché, spiegherò in dettaglio come abbiamo intenzione di applicare questo strumento tecnologico innovativo nel mercato degli orologi di lusso di seconda mano.

4.1 Architettura del sistema

Il centro gravitazionale della soluzione proposta è composto dal Marketplace C2C e dalla dApp. Attorno a questi due elementi avverranno le interazioni tra i vari componenti. In particolare:

- Marketplace C2C: un classico marketplace su cui i privati (acquirenti e venditori) entrano in contatto e avviano la compravendita. In questa sezione rientra tutto il mondo WEB2 di Watchain, composto anche dal sito web che rappresenterà l'azienda.
- Front-end dApp: l'interfaccia della dApp che permetterà agli utenti (buyer/seller, watchmaker e brand) di reperire le informazioni riguardo ai NFT e interagire in modo agevole con la blockchain.

L'architettura della soluzione Watchain include differenti attori, componenti e moduli esterni che interagiscono tra di loro.

Le tipologie di attori che si interfacciano con Watchain sono:

- Buyers/Sellers: sono i compratori e i venditori di orologi di lusso di seconda mano. Questi utilizzeranno il marketplace C2C per entrare in contatto e per inizializzare la compravendita.

- Watchmakers: sono gli esperti orologiai che, una volta che il compratore ha eseguito il pagamento per l'acquisto dell'orologio verso Watchain, analizzeranno l'orologio fisicamente per giudicare se le caratteristiche descritte dal venditore corrispondano effettivamente alla realtà. Dopo aver ispezionato il segnatempo, i watchmaker avvieranno la procedura di creazione del NFT attraverso la dApp.

- Brands: sono tutte le aziende produttrici di orologi che sarebbero intenzionate a creare delle collezzioni caratterizzate da pezzi limitati. In questo caso, interagendo con la dApp, sarebbero in grado di immettere sul mercato il nuovo orologio assieme al NFT.

Per quanto riguarda il back-end della dApp, questo è caratterizzato da:

- Smart Contract: il contratto intelligente creato da noi rifacendoci allo standard ERC-721 e adattandolo alle nostre esigenze. Attraverso questo contratto è possibile creare, trasferire e aggiornare il NFT.

- NFT e IPFS: nella fase di creazione del token, questo dovrà essere associato ad un tokenURI. Nel nostro caso, il tokenURI coincide con il link di IPFS, il database decentralizzato su cui andremo a fare lo storage dei metadati del NFT.

- Polygon: la blockchain più adatta alle nostre esigenze. Su Polygon andremo a deployare lo smart contract e a registrare tutte le transazioni e modifiche allo stato del NFT. A sua volta, Polygon immetterà queste informazioni sulla blockchain di tipo Layer-1 Ethereum.

Inerentemente ai moduli esterni che serviranno a Watchain per portare avanti la sua attività, troviamo:

- Metamask: un'estensione per accedere alle applicazioni distribuite abilitate per Ethereum. Consente agli utenti di creare e gestire le proprie identità, così quando la dApp ha bisogno di eseguire una transazione e scrivere dati sulla blockchain, l'utente ottiene un'interfaccia sicura per revisionare la transazione prima di approvarla o rifiutarla. Anche Watchain utilizzerà Metamask come mezzo per sostenere i costi di creazione del NFT e altre operazioni.

- Payment Gateway: la piattaforma di pagamento è un modulo esterno su cui il sistema si affida per finalizzare i pagamenti. Consente agli utenti di pagare gli orologi con valute tradizionali, che sono molto più utilizzate delle cryptocurrency al momento. Inoltre, Watchain si servirà dei tradizionali metodi di pagamento per remunerare gli esperti orologiai per l'ispezione portata a termine.

Le relazioni tra gli attori, i moduli esterni e il back-end della dApp sono sintetizzate nella figura 4.1:

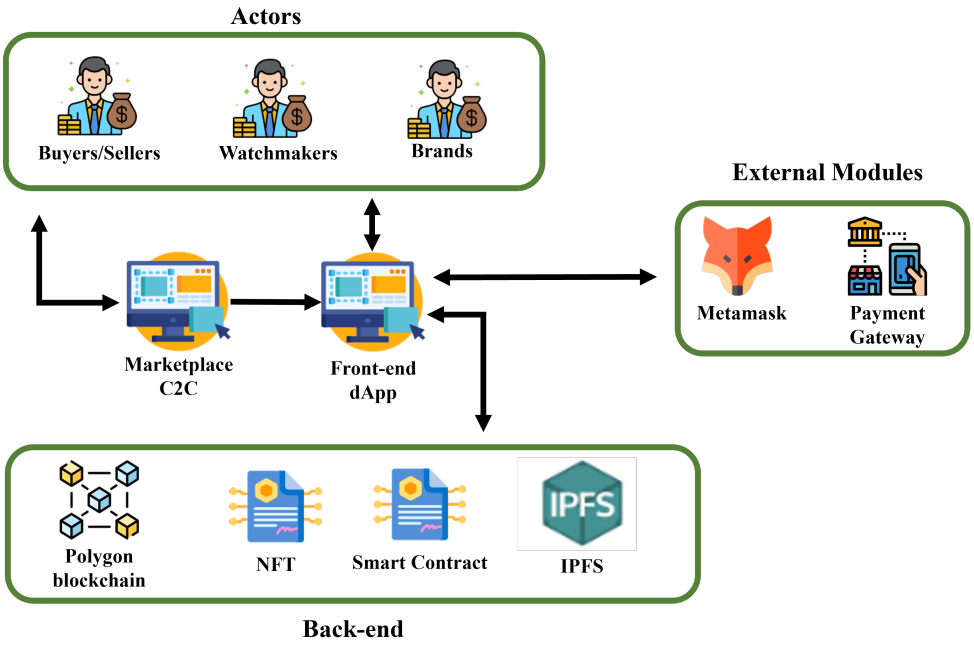

Figura 4.1: Architettura del sistema

4.2 Architettura dello smart contract e dei metadati

Lo smart contract funge da interfaccia per la blockchain Polygon. Il motivo della scelta di questa blockchain sarà trattato nel capitolo 5. Lo smart contract di Watchain è stato deployato attraverso Remix IDE, il quale è uno strumento online che fornisce un ambiente di sviluppo completo per la scrittura, il test e la distribuzione di contratti intelligenti su Ethereum. Ecco alcune delle caratteristiche principali di Remix IDE:

- Editor di contratti intelligenti: Remix offre un editor integrato che consente agli sviluppatori di scrivere contratti intelligenti in Solidity, il linguaggio di programmazione utilizzato per Ethereum;
- Debugger: Remix fornisce un debugger integrato che consente agli sviluppatori di eseguire il debug dei loro contratti intelligenti passo dopo passo, il che è fondamentale per individuare e risolvere bug nei contratti;
- Compiler: Remix include un compilatore Solidity che consente agli sviluppatori di compilare i loro contratti intelligenti in bytecode che possono essere distribuiti sulla blockchain;
- Testing: È possibile testare i contratti intelligenti all'interno dell'ambiente Remix IDE, consentendo agli sviluppatori di eseguire test unitari e di integrazione per garantire il corretto funzionamento dei contratti;
- Deploy: Remix permette di distribuire contratti intelligenti su una blockchain Ethereum o su una rete di test direttamente dall'IDE;
- Integrazione con Metamask: Puoi collegare Remix IDE al tuo portafoglio Metamask per interagire con la blockchain direttamente dall'IDE;

Lo smart contract implementato da noi si chiama 'Watchain'. Questo segue lo standard ERC-721 e consente di eseguire le seguenti funzionalità chiave:

- Creazione di certificati come NFT: Il nostro smart contract consente la creazione di nuovi certificati per orologi di lusso come token non fungibili (NFT). Chiamando la funzione appropriata, possiamo coniare un certificato unico associato a un orologio specifico, andando a storare le sue caratteristiche e stabilendo così la sua originalità sulla blockchain. Questo garantisce l'unicità e l'immutabilità di ciascun certificato;
- Trasferimento di proprietà: Nel caso in cui un orologio di lusso venga venduto o cambi proprietà, il contratto intelligente facilita il trasferimento del certificato

corrispondente da un proprietario all'altro. Questa funzione di trasferimento garantisce un registro trasparente e immutabile delle transizioni di proprietà per ciascun orologio. La blockchain agisce come una fonte affidabile della storia della proprietà, rafforzando la fiducia e l'autenticità;

- Distruzione del certificato: Alcune situazioni possono rendere un certificato invalido o obsoleto, come danni irreparabili o la scomparsa dell'orologio. In tali casi, il nostro contratto intelligente fornisce un meccanismo per distruggere il certificato, rimuovendolo efficacemente dalla blockchain. Ciò garantisce l'accuratezza e l'affidabilità dei record dei certificati;

- Interrogazione dei dati del certificato: Per verificare l'autenticità di un orologio di lusso, chiunque può interrogare i dati del certificato memorizzati sulla blockchain. Il nostro contratto intelligente consente il recupero di dettagli specifici relativi a un determinato certificato. Ciò include l'identificativo unico dell'orologio, la storia della proprietà, le specifiche dell'orologio (marca, modello, calibro del movimento, eccettera), la valutazione delle condizioni, la documentazione di supporto (foto, PDF), il valore di mercato e altre informazioni rilevanti. La trasparenza e l'accessibilità di questi dati favoriscono la fiducia e la credibilità;

- Aggiornamento del certificato: Nel caso in cui un orologio venga manutenuto, sarà possibile associare il token associato al segnatempo con le nuove informazioni e immagini. Questa funzione permette di tracciare l'evoluzione delle condizioni dell'orologio;

Quindi, il NFT mintato da Watchain, attraverso lo smart contract che sarà descritto di seguito, permette di tracciare la storia dell'orologio in una maniera trasparente e accessibile, facendo in modo che la proprietà e il valore del pezzo siano protetti.

Nella versione attuale della nostra soluzione, solo l'utente che ha inizialmente implementato il contratto intelligente (Watchain) ha l'autorità per coniare e aggiornare i dati del certificato. Tuttavia, per migliorare ulteriormente la funzionalità e le possibilità di collaborazione, prevediamo di implementare un sistema di controllo degli accessi nelle future versioni. Questo sistema consentirà ai nostri partner fidati di aggiornare e coniare i certificati direttamente sulla blockchain, espandendo la portata e la scalabilità della soluzione. Tale scelta permetterebbe, inoltre, anche di rendere più decentralizzato il sistema. Le informazioni riguardanti le caratteristiche dell'orologio che in futuro l'esperto orologiaio dovrà individuare, valutare e inserire nell'apposita dashboard sono riportate di seguito:

- Certificate ID

- Brand
- Model
- Reference
- Year
- Diameter
- Gross weight
- A vote (from 0 to 100) for:
  - Condition
  - Watch conformity
  - Bracelet conformity
- Date of estimation
- Last date of sell
- Eventually, a comment from watchmaker
- Eventually, a comment from expert
- For every side of watch:
  - Front
    - Photo
    - Lumes
    - Description of:
      - Bezel
      - Glass
      - Hands
      - Dial
      - Polishing
      - Water Resistance
  - Back
    - Photo
    - Lug width
    - Case material

    - Case
  - Side
    - Photo
    - Crown
    - Pushers
  - Bracelet
    - Photo
    - Description
    - Code
    - Material
    - Endlink
    - Endlink code
  - Buckle
    - Photo
    - Description
    - Code
- Serial number photo
- Serial number on case
- Case back photo
- Case back description
- Case back reference
- Movement photo
- Movement caliber
- Movement description
- Serial number on movement
- Box photo
- Box presence
- Box reference
- Papers photo

- Papers presence
- Warranty card photo and pdf
- Purchase invoices presence
- Maintenance invoices presence
- Certificate presence
- Country code
- Other accessories
- Watchmaker
  - Inspected by
  - Date of inspection
  - Company
  - Company address
  - Registration number
- Expert
  - Validated by
  - Date of validation
- Owner
  - Email
  - Full name
  - Date of birth

Tuttavia, per semplicità, il NFT mintato a scopo dimostrativo in questa tesi avrà solo le seguenti caratteristiche descritte nella tabella 4.1.

Di seguito mostrerò le funzioni dello smart contract che permetteranno di ottenere tutte le funzionalità sopra elencate. Inoltre, analizzerò se il metodo di storage è decentralizzato, quanto è permanente lo storage e se qualcuno, e chi in tal caso, è capace di modificare il dato on-chain. Infine, spiegherò come sarà possibile reperire tutte le informazioni dall'utente che ha ottenuto il proprio certificato NFT, o da un utente qualsiasi.

I metadati salvati del NFT dimostrativo saranno:

Dato	**Tipologia**
Marca	string
Modello	string
Referenza	string
Anno di produzione	int
Nome validatore	string
Codice della scatola	int
Seriale	string
URL foto fronte	string
URL foto retro	string
URL lato dx	string
URL lato sx	string

Tabella 4.1: Elenco dei tipi di dati utilizzati per la creazione del NFT dimostrativo

- Marca dell'orologio: Rolex
- Modello dell'orologio: Datejust
- Referenza dell'orologio: 162200
- Anno di produzione: 2000
- Nome esperto: Marco Rossi
- Numero della scatola: 30.00.71
- Numero seriale orologio (garanzia): 4418415

È bene dire che i suddetti metadati potrebbero essere salvati anche nello smart contract direttamente. Tuttavia, questo comporterebbe una maggiore dimensione del codice. Di conseguenza, ciò si tradurrebbe in maggiori costi in fase di deployment sulla blockchain e nelle altre situazioni come il minting, transferring e così via. Pertanto, Watchain ha pensato di implementare lo storage di tutti i dati su IPFS in un primo momento, sia per fare in modo che i costi restino bassi in fase di test sia per testare quali dati siano più soggetti a modifiche. Una volta che la soluzione sarà consolidata e il progetto potrà sostenere costi maggiori senza problemi grazie ad una brand identity di rilievo, si penserà a se e quali dati dovranno essere integrati nello smart contract stesso, rendendoli non più soggetti a modifiche. Inoltre, bisogna specificare per evitare equivoci che i metadati su IPFS associati al token possono essere aggiornati e modificati, ma allo stesso tempo sulla blockchain rimarrà per sempre la traccia della modifica avvenuta e del link che riporta sia ai dati vecchi

che ai nuovi, in modo che la storia dell'orologio non vada persa.

Per quanto riguarda le foto, un esempio per chiarire la tipologia di foto di cui si necessita è mostrato nella figura 4.2:

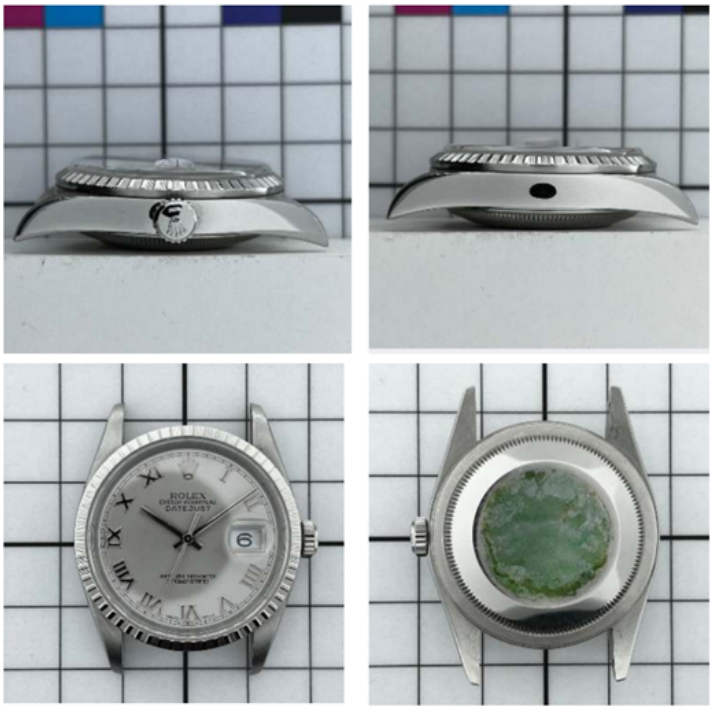

Figura 4.2: Immagini utilizzate nei metadati del NFT

È fondamentale dire che salvare un'immagine su blockchain può essere complicato e costoso. Per ovviare a questo problema, è possibile utilizzare altre soluzioni che permettono di salvare delle foto pubblicamente e in modo decentralizzato. Ad esempio, Watchain utilizzerà la tecnologia IPFS (InterPlanetary File System), la quale permette di archiviare e distribuire dei contenuti in modo peer to peer. Il sistema è stato progettato per rendere più resistente e decentralizzato internet. Ogni file o contenuto archiviato su IPFS è associato ad un hash crittografico univoco generato dal contenuto stesso. Tale hash funge da 'indirizzo' per il contenuto. Utilizzando IPFS, i metadati vengono archiviati in un file e quindi il suo hash viene incorporato nel token NFT stesso. In questo modo, i metadati possono essere recuperati da qualsiasi nodo IPFS che li abbia in memoria, garantendo la disponibilità e la resistenza. Nel nostro caso, Tutte queste informazioni vengono salvate nella blockchain IPFS, attraverso Pinata, la quale è utile perché offre una

serie di servizi e funzionalità che semplificano l'utilizzo di IPFS e lo rendono più accessibile per sviluppatori e utenti finali. Pinata risulta particolarmente utile per gli sviluppatori che desiderano sfruttare i vantaggi di IPFS senza doversi preoccupare di dettagli complessi di gestione dei dati. Inoltre, è possibile decidere se i dati debbano essere leggibili pubblicamente da chiunque oppure limitando all'accesso ai dati ai soli utenti autorizzati. Nel nostro caso, tutte le funzioni di scrittura possono essere chiamate solo dal proprietario del contratto. Questa caratteristica deriva dalla feature 'ownable' con la quale si è strutturata il contratto. Notiamo che tutte le informazioni sono sulla blockchain, tranne:

1. Informazioni private del proprietario: indirizzo email / nome completo / data di nascita;

2. Prezzo stimato dall'esperto;

I tipi di dati appena menzionati, che sono fuori dalla blockchain (off-chain), non sono inclusi nel NFT per ragioni comprensibili. Questa scelta è necessaria per rispettare la privacy degli utenti e per evitare analisi indesiderate sull'evoluzione delle stime dei prezzi e dei modelli di orologi presenti nel mercato tramite l'uso della blockchain. Per tali ragioni, queste informazioni saranno conservate in un database privato di Watchain. Sviluppando questa soluzione basata su blockchain e sfruttando le capacità del contratto intelligente, miriamo a creare un sistema sicuro e trasparente per l'emissione di certificati che garantiscono l'originalità degli orologi di lusso. I metadati relativi al NFT saranno accessibili a tutti. Tuttavia, per garantire la privacy di alcuni dati sensibili, si è scelto di crittografare questi dati sensibili attraverso la funzione di hash SHA256.

4.2.1 Minting

La funzione 'mint' è importata dalla libreria Open Zeppelin, la quale ci ha permesso di rifarci allo standard ERC721. In sostanza, tale funzione fa sì che venga creato un token con un ID (in questo caso il primo token mintato assumerà ID=0) e che tale token sia indirizzato verso un wallet. Quindi, la funzione 'mint' riceverà come input l'indirizzo del wallet del proprietario e il tokenID. Successivamente, la funzione 'mint' chiama la funzione 'setTokenURI', grazie alla quale al token con quel particolare ID, appartenente a quel determinato wallet, è associato quel particolare certificato. Il certificato conterrà tutti i metadati dell'orologio di cui ho parlato sopra. In particolare, i metadati saranno salvati in IPFS e il link per recuperare i metadati dovrà essere inserito in fase di minting nella sezione tokenURI. Inoltre, è importante notare che queste informazioni appena elencate possono essere aggiunte solo dall'owner del contratto (Watchain), cioè chi l'ha deployato sulla blockchain, una volta sola e quindi nessuno potrà cambiarle o cancellarle finché la

blockchain Polygon esisterà. Anche se la società che ha creato il token non esistesse più, il codice identificativo rimarrebbe per sempre on-chain. Quanto appena detto è derivato dalla feature 'onlyowner' del contratto. La funzione mint controlla, inoltre, che il wallet di destinazione non sia il wallet 0, ossia il wallet che si utilizza per bruciare il NFT, rendendolo irrecuperabile.

La funzione è riportata nella figura 4.3:

```
function mint(address ownerAddress, string memory tokenURI)
    public
    onlyOwner
    returns (uint256)
{
    uint256 tokenId = _nextTokenId++;
    _mint(ownerAddress, tokenId);
    _setTokenURI(tokenId, tokenURI);

    return tokenId;
}
```

Figura 4.3: Funzione di minting

Nel file .json sarà possibile andare a recuperare tutte le caratteristiche dell'orologio inserite dall'esperto validatore. Bisogna però specificare che i dati ritenuti sensibili, come ad esempio il seriale dell'orologio, non saranno espressi esplicitamente. Infatti, al seriale sarà applicata la crittografia SHA256, la quale restituirà un digest associato a quel seriale. È bene notare che non sarà possibile risalire al seriale da quel digest. In questo modo, per dimostrare che si è il proprietario di quel seriale bisognerà applicare lo SHA256 al seriale e confrontare che i digest siano uguali. Questo procedimento di protezione dei dati può essere ripetuto anche per altri tipi di dati. La scelta di nascondere il seriale identificativo dell'orologio risiede nel fatto che questi potrebbero essere usati per produrre dei fake, in modo tale che, se presentato ad un concessionario risulterebbe esistente e venduto come originale.

4.2.2 Burning

Un'altra funzionalità contemplata dallo smart contract è la possibilità di distruggere per sempre un token già creato. Tale azione è possibile compierla attraverso la funzione 'burn', riportata nella figura 4.4:

```
function burn(uint256 tokenId) public onlyOwner {
    _burn(tokenId);
}
```

Figura 4.4: Funzione di burning

In sostanza, invocando la funzione 'burn' e inserendo l'ID del token da voler bruciare, il token viene inviato all'indirizzo del wallet 0, non potendolo più recuperare. In particolare, poiché una volta che un qualunque dato è stato immesso sulla blockchain non può essere cancellato o modificato, lo stratagemma che si utilizza per 'eliminarlo' è inviare il token a un indirizzo per il quale è matematicamente certo che non esistano le chiavi private. Quindi, se nessuno è a conoscenza della chiave privata, tutto ciò che è inviato a tale indirizzo, non è recuperabile in alcun modo. Come si nota dalla parola 'onlyOwner' nella funzione, solo il proprietario del certificato può compiere questa azione.

4.2.3 Updating

Per aggiornare un certificato, bisogna invocare la funzione 'updateCertificate' (figura 4.5), la quale necessita come input del tokenID e il nuovo tokenURI, ossia del nuovo link IPFS. Tale funzione si avvale sempre della funzione 'setTokenURI', che permette di associare ad un particolare tokenID un nuovo tokenURI. E' possibile selezionare il token di cui si vuole aggiornare il metadata e modificare il link che riporta al .json su IPFS. Ovviamente, una volta aggiornato, il token avrà delle nuove caratteristiche, ma in blockchain sarà registrato per sempre la transazione che registra la variazione del link che riporta ai metadata e chi l'ha fatta avvenire. Anche in questo caso, la funzione di aggiornamento del certificato può essere portata a termine solo da Watchain, ossia il soggetto che ha deployato il contratto su blockchain e quindi ne risulta il proprietario.

```
function updateCertificate(uint256 tokenId, string memory tokenURI)
    public
    onlyOwner
{
    _setTokenURI(tokenId, tokenURI);
}
```

Figura 4.5: Funzione di updating

4.2.4 Transferring

Al fine di trasferire il token da un wallet ad un altro, è necessario chiamare la funzione 'safeTrasferFrom'. Quest'ultima richiede in input l'indirizzo del proprietario del token, l'indirizzo di chi riceverà il token e il tokenID. Inoltre, verifica che l'indirizzo del destinatario non sia l'indirizzo 0 e che l'indirizzo mittente detenga realmente quel determinato token. La funzione 'safeTransferFrom' richiama la funzione 'update' dello smart contract ERC721, la quale è riportata nella figura 4.6:

```
function _update(address to, uint256 tokenId, address auth) internal virtual returns (address) {
    address from = _ownerOf(tokenId);

    // Perform (optional) operator check
    if (auth != address(0)) {
        _checkAuthorized(from, auth, tokenId);
    }

    // Execute the update
    if (from != address(0)) {
        // Clear approval. No need to re-authorize or emit the Approval event
        _approve(address(0), tokenId, address(0), false);

        unchecked {
            _balances[from] -= 1;
        }
    }

    if (to != address(0)) {
        unchecked {
            _balances[to] += 1;
        }
    }

    _owners[tokenId] = to;

    emit Transfer(from, to, tokenId);

    return from;
}
```

Figura 4.6: Funzione di transferring

4.3 Interrogazione dello smart contract da parte degli utenti

In questa sezione saranno riportate alcune interazioni che possono avvenire con lo smart contract, utilizzando l'explorer della blockchain di riferimento, che nel nostro caso è PolygonScan. Una delle prime informazioni che si possono ottenere dal contratto è la quantità di token detenuta da un particolare address.

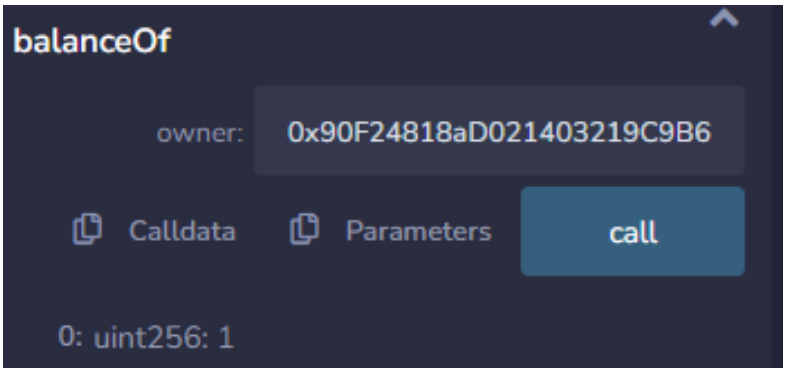

Figura 4.7: Chiamata della funzione BalanceOf

Tale informazione è possibile ottenerla invocando la funzione 'balanceOf' (figura 4.7) e inserendo come input l'address di cui si vuole sapere il numero di token detenuti. Premendo su 'call', fuoriesce che l'address detiene un solo token in questo caso. Il token è proprio quello corrispondente all'orologio sopra descritto. Infatti, chiamando la funzione 'ownerOf' (figura 4.8) e inserendo come input il tokenID del token corrispondente al segnatempo preso a titolo esemplificativo, sarà restituito proprio l'address in cui è conservato quel determinato NFT.

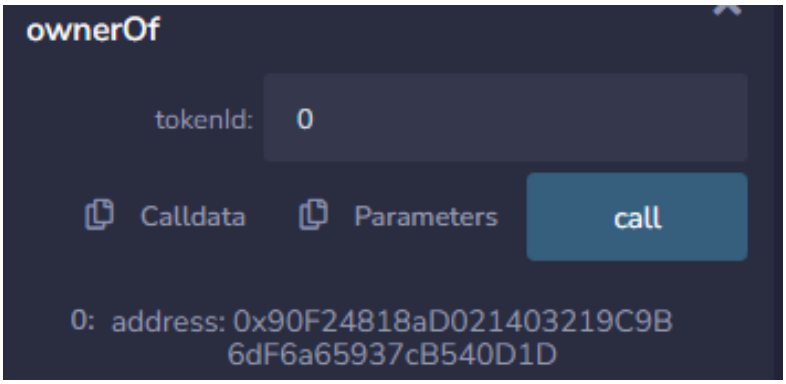

Figura 4.8: Chiamata della funzione OwnerOf

Infine, se si vuole indagare sui metadata relativi al token in questione, è possibile chiamare la funzione 'tokenURI', la quale chiederà come input il tokenID.

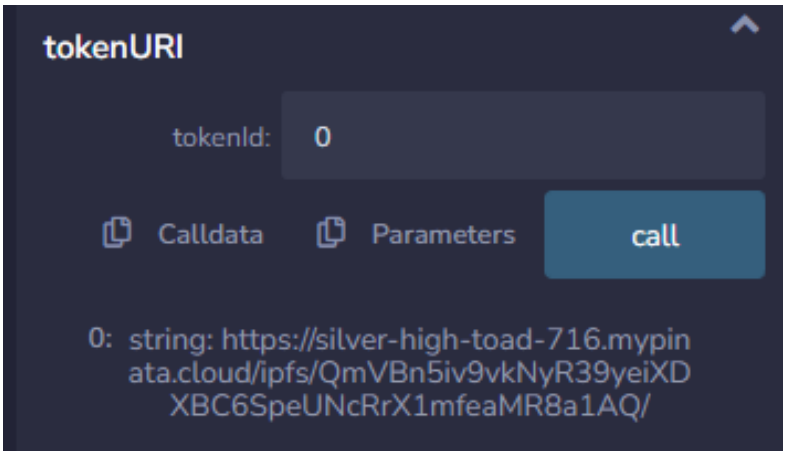

Figura 4.9: Chiamata della funzione TokenURI

Nel nostro caso, inserendo l'ID '0' e invocando la funzione, è restituito il link che riporta alla repository in cui sono contenuti i metadata su IPFS, come mostrato dalla figura 4.9.

Figura 4.10: Pagina di IPFS in cui sono custoditi i metadata

In questo esempio, la cartella contiene due file: il .json in cui sono riportati le caratteristiche dell'orologio e le immagini relative al segnatempo in questione. Per quanto riguarda le immagini, sono le stesse che sono state rappresentate nella figura 4.2. Mentre, le caratteristiche dell'orologio sono espresse nel formato .json, come mostrato in figura4.11:

```
[
 {
  "-\tMarca dell'orologio: Rolex"
 },
 {"-\tModello dell'orologio: Datejust"
 },
 {"-\tReferenza dell'orologio: 162200"
 },
 {"-\tAnno di produzione: 2000"
 },
 {"-\tNome esperto: Marco Rossi"
 },
 {"-\tNumero della scatola:  30.00.71"
 },
 {"-\tNumero seriale orologio (garanzia): bdc6b1a28b7459d562bdf6ce94fb37dc69098d38aa0813f275e1a9ae720ecedc"
 }
]
```


Figura 4.11: Rappresentazione dei metadata in formato .json

4.4 Tech Stack

Le tecnologie coinvolte in questo progetto includono:

1. React
2. Node.js
3. Solidity
4. JavaScript
5. Polygon

Analizzandole nel dettaglio:

1. React è una libreria per lo sviluppo dell'interfaccia utente basata su JavaScript. È gestita da Facebook e da una comunità di sviluppatori open source. Anche se React è una libreria piuttosto che un linguaggio, è ampiamente utilizzata nello sviluppo web. La libreria è stata lanciata per la prima volta nel maggio 2013 ed è ora una delle librerie frontend più comuni per lo sviluppo web. React offre varie estensioni per il supporto architetturale dell'intera applicazione, come Flux e React Native, oltre all'UI. I punti di forza di React sono:
   - Creazione semplice di applicazioni dinamiche: React semplifica la creazione di applicazioni web dinamiche perché richiede meno codifica e offre maggiore funzionalità, a differenza di JavaScript, dove la codifica spesso diventa complessa molto rapidamente;
   - Miglioramento delle prestazioni: React utilizza il Virtual DOM, creando così applicazioni web più veloci. Il Virtual DOM confronta gli stati precedenti dei componenti e aggiorna solo gli elementi nel DOM reale che sono stati modificati, anziché aggiornare nuovamente tutti i componenti, come fanno di solito le applicazioni web convenzionali;
   - Componenti riutilizzabili: I componenti sono i mattoni di costruzione di qualsiasi applicazione React, e di solito un'applicazione è composta da molti componenti. Questi componenti hanno la propria logica e i propri controlli e possono essere riutilizzati in tutta l'applicazione, riducendo notevolmente il tempo di sviluppo dell'applicazione;
   - Flusso di dati unidirezionale: React segue un flusso di dati unidirezionale. Ciò significa che quando si progetta un'app React, gli sviluppatori spesso nidificano i componenti figlio all'interno dei componenti genitori. Poiché i dati fluiscono in una sola direzione, diventa più facile individuare errori e sapere dove si è verificato un problema in un'applicazione in un determinato momento;

- Può essere utilizzato per lo sviluppo sia di applicazioni web che mobili: Sappiamo già che React è utilizzato per lo sviluppo di applicazioni web, ma non è tutto ciò che può fare. Esiste un framework chiamato React Native, derivato da React stesso, che è estremamente popolare e viene utilizzato per creare splendide applicazioni mobili. Quindi, in realtà, React può essere utilizzato per creare sia applicazioni web che mobili;

2. Node.js (Node) è un ambiente di runtime open source multipiattaforma per l'esecuzione di codice JavaScript. Node è ampiamente utilizzato per la programmazione lato server, consentendo ai programmatori di utilizzare JavaScript per il codice lato client e lato server senza dover imparare un linguaggio aggiuntivo. Node viene talvolta chiamato un linguaggio di programmazione o un framework di sviluppo del software, ma né l'uno né l'altro è vero; è strettamente un runtime JavaScript. Node incorpora il motore JavaScript V8, lo stesso utilizzato in Google Chrome e in altri browser. È scritto in C++ e può funzionare su macOS, Linux, Windows e su altri sistemi. Il motore analizza ed esegue il codice JavaScript. Può funzionare indipendentemente da un ambiente del browser, incorporato in un'applicazione C++ o implementato come programma autonomo. Il motore V8 compila internamente il JavaScript, utilizzando processi just-in-time (JIT) per velocizzare l'esecuzione.

3. Solidity è un linguaggio di programmazione orientato ai contratti intelligenti (smart contracts) basato su Ethereum. La sua principale forza risiede nella sua progettazione specifica per lo sviluppo di contratti intelligenti, offrendo una solida sicurezza e un ambiente predefinito per l'implementazione di applicazioni decentralizzate. Le caratteristiche chiave includono la tipizzazione statica, che previene errori comuni, e il supporto per la programmazione orientata agli oggetti, rendendo la scrittura di contratti più intuitiva e manutenibile. Solidity è anche ben supportato dalla comunità Ethereum, con una vasta documentazione e una crescente base di sviluppatori. Infine, la sua compatibilità con lo standard EVM (Ethereum Virtual Machine) garantisce l'interoperabilità con altri contratti e applicazioni sulla rete Ethereum.

4. JavaScript è un linguaggio di programmazione ampiamente utilizzato per lo sviluppo web, noto per diverse caratteristiche che ne evidenziano la forza. Prima di tutto, la sua esecuzione lato client consente di creare interattività sul web direttamente nel browser dell'utente, migliorando l'esperienza utente. Inoltre, JavaScript è un linguaggio versatile che può essere utilizzato per sviluppare applicazioni sia lato client che lato server, grazie a runtime come Node.js. La vasta comunità di sviluppatori ha creato una vasta gamma di librerie e framework che semplificano lo sviluppo e la manutenzione delle applicazioni. Inoltre, la sintassi di JavaScript è flessibile e facile da apprendere,

rendendolo accessibile a una vasta gamma di programmatori. Infine, la costante evoluzione del linguaggio e gli standard ECMAScript garantiscono una crescita continua e un migliore supporto delle ultime tecnologie web.

5. Polygon è una blockchain di tipo layer 2 che ha rivoluzionato il mondo delle criptovalute e della tecnologia blockchain, offrendo una soluzione scalabile per l'Ethereum. La sua storia inizia con il nome Matic Network e si è evoluta per diventare Polygon, un ecosistema blockchain multifunzionale. Il suo primo grande punto di forza è l'integrazione con l'Ethereum Virtual Machine (EVM), che consente agli sviluppatori di eseguire contratti intelligenti Ethereum sulla rete Polygon senza dover riscrivere il codice. Il layer 2 di Polygon è noto per affrontare le sfide di congestione e lentezza di Ethereum, offrendo transazioni più veloci e meno costose. Grazie alle diverse sidechain e soluzioni di scaling che compongono l'ecosistema, Polygon offre un'ampia gamma di opzioni per gli sviluppatori, permettendo loro di scegliere la soluzione più adatta alle proprie esigenze, dal punto di vista della sicurezza e della decentralizzazione. Un altro punto di forza è l'ampio supporto di progetti di sviluppo e la collaborazione con importanti dApps, come Aave, Decentraland e QuickSwap, che hanno adottato la tecnologia Polygon per migliorare le prestazioni e ridurre i costi operativi. Inoltre, Polygon ha investito in strumenti di sviluppo, offrendo una gamma di strumenti e documentazione per facilitare il processo di sviluppo di applicazioni su questa rete. L'ecosistema di Polygon è un punto di forza notevole, con un'ampia adozione da parte di progetti DeFi, NFT, dApps e molto altro. Questi progetti si affidano alla scalabilità di Polygon per offrire servizi più accessibili e convenienti ai loro utenti, contribuendo a ridurre i costi operativi e migliorare le prestazioni. La criptovaluta nativa di Polygon, MATIC, è al centro di questo ecosistema, utilizzata per pagare transazioni e per partecipare al consenso sulla rete. In sintesi, Polygon è diventato un importante pilastro nell'ecosistema blockchain, offrendo una soluzione efficace per l'escalation di Ethereum, con interoperabilità, sicurezza, e ampio supporto dei progetti. La sua flessibilità e adozione crescente dimostrano come stia contribuendo a plasmare il futuro delle applicazioni decentralizzate e delle criptovalute.

4.5 Sfide legate all'UX: dal WEB2 al WEB3

Nonostante gli sviluppi nel settore, al giorno d'oggi, la blockchain presenta ancora molte sfide dal punto di vista dell'esperienza e dell'usabilità che sono fortemente percepite come degli ostacoli dai principianti e che possono spesso portare a interazioni sgradevoli e intricate, talvolta a errori problematici. La soluzione proposta da Watchain è stata progettata per un utente che potrebbe non avere sempre fiducia

e conoscenza delle complessità di questa tecnologia e su come trarne il massimo vantaggio.

L'obiettivo di Watchain è creare una soluzione che controlli e limiti queste difficoltà al fine di includere il più ampio numero possibile di utenti, anche i meno esperti, senza richiedere una conoscenza particolare della tecnologia e del suo funzionamento: la sensazione dell'utente dovrebbe essere la stessa che si sperimenterebbe utilizzando una piattaforma WEB2, con tutti i vantaggi che una soluzione basata su blockchain porta con sé.

La prima grande sfida da questo punto di vista riguarda l'usabilità dei portafogli (wallet): questo costituisce un'enorme limitazione per gli utenti inesperti che non hanno conoscenza di cosa siano una chiave privata o pubblica. Infatti, nel caso in cui un proprietario dell'orologio non abbia già un wallet su cui indirizzare il NFT, Watchain propone un modello basato su una serie di portafogli "hot" in cui i certificati NFT saranno estratti, memorizzati e successivamente riscattati da utenti più esperti nei loro portafogli. Anche se introduce un po' di centralizzazione nel nostro sistema, questo passo consente un processo di onboarding più agevole per gli utenti meno esperti della nostra piattaforma.

Pertanto, inizieremo adottando un approccio ibrido per la nostra soluzione, in cui costruiremo e distribuiremo una parte del prodotto in un ambiente WEB2. Questa configurazione consentirà un'interazione senza soluzione di continuità con la blockchain, in particolare per la creazione, l'aggiornamento e la visualizzazione dei certificati secondo necessità.

Watchain è creato ponendo l'utente al centro del progetto: solo attraverso la facilità d'uso e la semplificazione dell'esperienza sarà possibile espandere il progetto al di là della nicchia degli appassionati di blockchain.

4.6 Watchain: un marketplace C2C

Viste le problematiche citate nel capitolo precedente, che affliggono il settore del lusso in generale, Watchain mira a creare una soluzione in grado di portare tracciabilità in un mercato complesso come quello degli orologi di lusso. Dopo aver intervistato orologiai, rivenditori e acquirenti di orologi di lusso, abbiamo subito capito che chi è interessato a comprare un orologio di lusso e non ha una grande competenza che gli permetta di capire a fondo tutte le particolarità di un orologio, ha a disposizione un'unica soluzione: affidarsi nelle mani del rivenditore, sperando che il segnatempo che sta per acquistare non sia, totalmente o in parte, contraffatto. Il rischio di poter subire una frode è reale; infatti, Havocscope, fornitore mondiale di informazioni sui diversi mercati neri, prova a dare una dimensione al fenomeno stimando che ogni anno vengano venduti globalmente circa 40[1] milioni di orologi contraffatti, generando un profitto netto di circa 1 miliardo di dollari.

Il bisogno di tracciare e certificare le informazioni riguardo l'orologio che si sta per acquistare diventa ancora più forte nel momento in cui si vogliano utilizzare i canali online per comprare il segnatempo. Durante gli anni della pandemia, secondo BCG, il mercato degli orologi di lusso di secondo polso ha raggiunto il valore di 22 40[2] miliardi nel 2021, risultando quasi un terzo del valore del mercato generale degli orologi, il quale si attesta a 75 milardi per il 2021.

Bisogna dire che la grandezza del mercato di secondo polso degli orologi di lusso è destinata a superare anche la grandezza del mercato primario (ossia quello in cui è un rivenditore autorizzato dalla casa produttrice a vendere l'orologio nuovo), a causa del numero di pezzi limitati prodotti dalle maison e dal crescente interesse suscitato da questo mondo negli appassionati di orologi. La figura 4.12 mostra una fotografia della crescita e delle sue previsioni dei mercati di primo e secondo polso.

[1] https://corsearch.com/content-library/blog/counterfeiting-in-the-watch-industry

[2] https://www.bcg.com/publications/2023/luxury-watch-market-trends

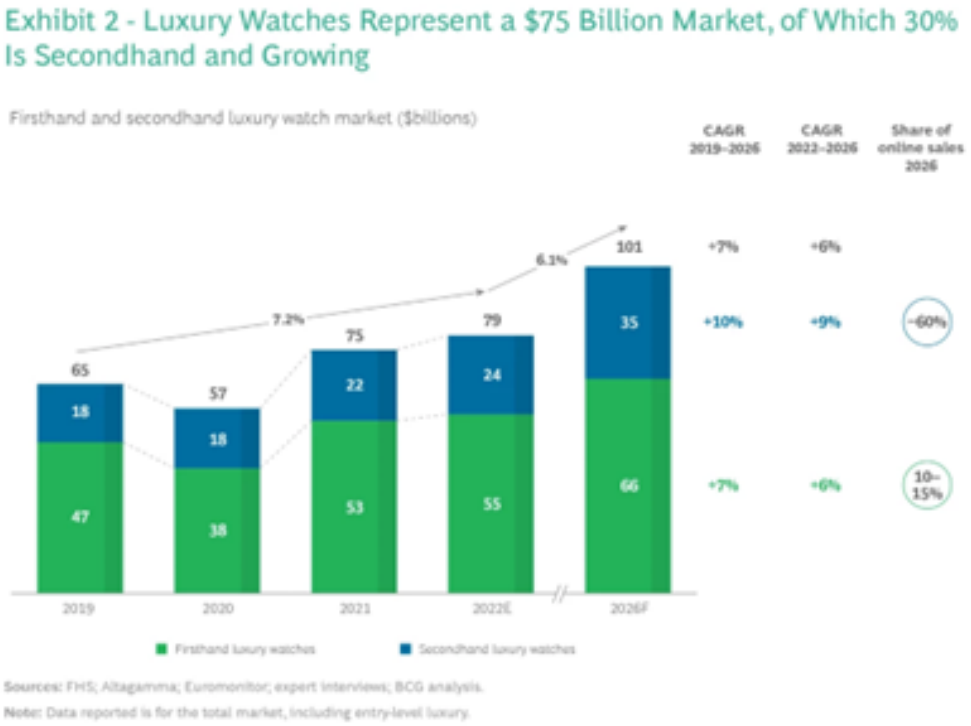

Figura 4.12: Proiezione della grandezza del mercato di prima e seconda mano per gli orologi di lusso

È inutile dire che, se questo mercato ha potuto vedere negli ultimi un così forte fermento, è stato soprattutto grazie allo sviluppo dei canali di vendita online, come ad esempio vari marketplace, ma anche banalmente grazie al proliferare di gruppi Facebook in cui avvengono regolarmente compravendite di orologi. Analizzando le dinamiche che si presentano nel contesto dei marketplace di orologi di lusso odierni abbiamo capito che queste piattaforme tendono a mettere in contatto maggiormente rivenditori di orologi (aziende) con i privati. Infatti, anche se ad esempio su Chrono24 sono presenti anche privati, attraverso l'utilizzo di forum di appassionati, abbiamo capito che un compratore di orologi tende ad evitare di comprare da privati, poiché sia la piattaforma sia il privato stesso offrono meno garanzie per l'acquisto di un orologio da un privato rispetto che da un'azienda.

Alla luce delle problematiche appena evidenziate, l'obiettivo del progetto Watchain è quello di offrire la possibilità di comprare segnatempo anche da privati, con la stessa affidabilità che si ha quando si compra da una gioielleria riconosciuta. Per raggiungere tale obiettivo, ovvero certificare e tracciare orologi di lusso, Watchain ha pensato bene di avvalersi della tecnologia blockchain, in particolare mintando i

NFT associati agli orologi. In sostanza, quando un utente conferma l'acquisto di un orologio, attraverso il marketplace C2C propietario, effettuerà un pagamento verso Watchain, la quale custodirà il denaro fino a quando l'orologio non sarà certificato dal nostro orologiaio partner. Nel momento in cui il NFT è mintato, Watchain procederà con il pagamento del venditore, trattenendo la quota che gli spetta e pagando l'orologiaio che ha periziato il segnatempo. Infine, il compratore riceverà da noi sia l'orologio certificato che la card di watchain con sopra un codice QR che rimanda ad un sito in cui sono rappresentate tutte le caratteristiche del NFT.

Le entità che interagiranno con la piattaforma Watchain saranno di due tipi: i certificatori e i privati; questi ultimi si dividono a loro volta in acquirenti e venditori. I maestri orologiai appartengono alla prima categoria: nel sistema di Watchain hanno il ruolo di certificatori e possiedono la capacità di creare e convalidare ogni certificato attraverso un processo suddiviso in due fasi, le quali garantiranno un livello più elevato di decentralizzazione a un processo che è centralizzato per design (è inevitabile che l'attore in grado di verificare fisicamente l'autenticità di un orologio, quindi i maestri orologiai ed esperti di orologi, debba essere anche colui che inserisce i dati dell'orologio nella blockchain). Il processo a due fasi funziona nel seguente modo: innanzitutto, il maestro orologiaio o l'esperto di orologi incaricato di certificare un orologio compilerà il modulo sulla dashboard di Watchain e allegherà tutte le foto, la documentazione relativa e tutte le informazioni riguardanti il proprietario. Tale ispettore/valutatore esprimerà un giudizio sull'autenticità e la contemporaneità dell'orologio. A questo punto, viene impiegato un secondo processo di verifica di queste informazioni: un secondo certificatore presente sulla nostra piattaforma verrà scelto casualmente e gli verrà chiesto di convalidare il certificato appena creato. Tutte le informazioni sul proprietario e sul maestro orologiaio che ha effettuato la prima perizia verranno omesse per garantire che non ci siano accordi malevoli tra i validatori. Una volta superata questa fase, il NFT verrà creato e coniato nel nostro sistema.

Nel caso in cui un produttore di orologi decidesse di tokenizzare i propri prodotti all'interno della nostra piattaforma, si comporterebbe esattamente come un maestro orologiaio e sarà in grado di creare i propri certificati, ma non potrà convalidare i certificati di altri partner. Infatti, la soluzione pensata da Watchain potrebbe essere destinata anche ad aziende produttrici di orologi medio/piccole che vogliano immettere i loro nuovi orologi sul mercato primario con già il NFT associato al segnatempo. Con questa ulteriore linea di business, si soddisferebbero i bisogni dei microbrand che vorrebbero già implementare questa soluzione ma che non hanno a disposizione le risorse e le competenze per farlo. Inoltre, immettendo i loro prodotti sul marketplace godrebbero della pubblicità che una piattaforma di questo tipo può offrire.

Sia i proprietari di orologi che gli acquirenti appartengono alla categoria degli utenti. Questi soggetti saranno in grado di interagire con la piattaforma attraverso la dashboard dei proprietari, nella quale, una volta registrati, sarà possibile richiedere la certificazione dei loro orologi, gli aggiornamenti dei certificati (ad esempio, in caso di vendita o manutenzione) e segnalare il furto o la scomparsa di uno degli orologi posseduti tokenizzati sulla nostra piattaforma (che successivamente verrà inserito in una lista nera dal nostro sistema). La decisione di consentire la creazione di NFT degli orologi solo a soggetti autorizzati è un elemento di centralizzazione della piattaforma. Tuttavia, è fortemente necessario, poiché i maestri orologiai ed esperti di orologi sono gli unici soggetti in grado di rilasciare un certificato di valutazione di questo tipo. Inoltre, pensiamo che sia fondamentale garantire l'autorevolezza della fonte dei dati da immettere sulla blockchain e inoltre, potrebbe essere sfruttato a nostro favore associare il brand Watchain all'esperienza riconosciuta di alcuni maestri orologiai, visti come dei guru dal settore. Un sistema di autocertificazione in cui ciascun utente è libero di tokenizzare il proprio orologio è già presente (con alcuni sistemi centralizzati), ma il valore di questo tipo di certificazione è estremamente limitato data la sua natura. Dal punto di vista architettonico, la soluzione di Watchain è divisa in 3 segmenti principali: il sito web, l'area dei proprietari e la dashboard dei maestri orologiai.

Il sito web permetterà l'accesso all'area dei proprietari e la compilazione della richiesta di certificato, nonché la scoperta della soluzione Watchain, delle sue funzionalità e dei partner.

L'area dei proprietari sarà dedicata esclusivamente ai possessori di orologi: in questa sezione sarà possibile richiedere nuovi certificati, chiedere aggiornamenti dei propri certificati, segnalare un furto e esplorare tutti i certificati presenti sulla blockchain, nonché la propria collezione di orologi registrati nel sistema di Watchain.

La dashboard dei maestri orologiai non sarà accessibile tramite il sito web e verrà fornita a ciascun maestro orologiaio partner o esperto di orologi sulla piattaforma in seguito a un processo di selezione. All'interno di questa sezione, sarà possibile esplorare tutti gli orologi certificati, creare nuovi certificati e aggiornare i certificati esistenti seguendo le richieste dei proprietari. Allo stesso tempo, attraverso questa dashboard, ai partner verrà chiesto di convalidare i certificati inseriti nel nostro sistema da altri esperti o maestri orologiai.

Figura 4.13: Architettura del sito web di Watchain

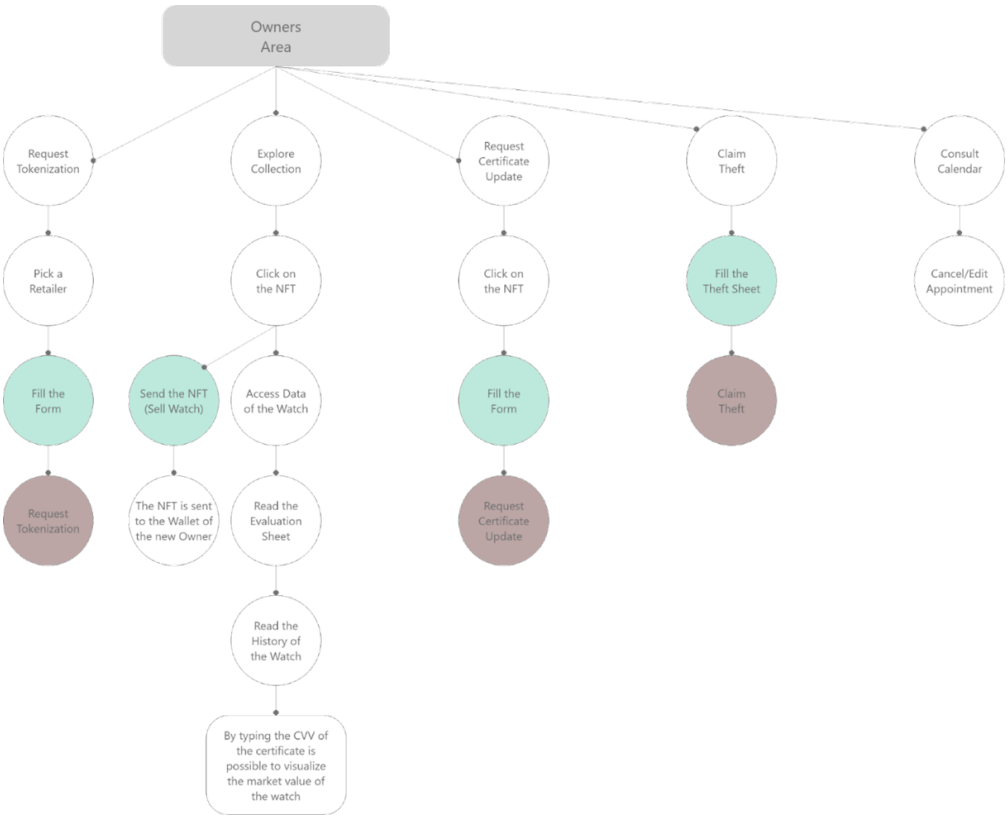

Figura 4.14: Architettura della sezione “Owners” sul sito web Watchain

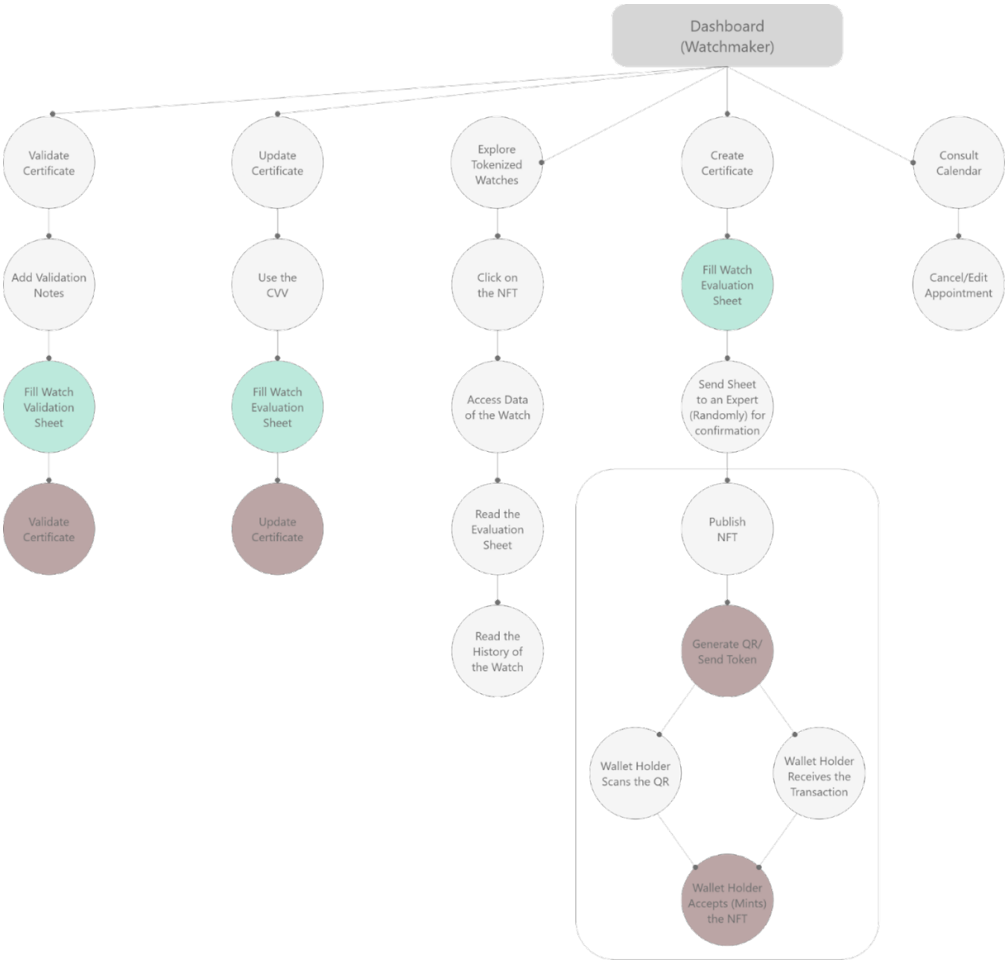

Figura 4.15: Architettura della dashboard per gli orologiai affiliati a Watchain

Capitolo 5

Valutazioni

In questo capitolo sarà descritta l'analisi condotta da me al fine di individuare la blockchain che ci permetta di spendere il meno possibile quando si interagisce con lo smart contract e che garantisca allo stesso scalabilità e affidabilità in linea con la portata del progetto che si vuole sviluppare.

È importante dire che nel caso di sola 'lettura' del contratto non si sostengono costi. I casi di lettura del contratto, ad esempio, sono quelli riguardanti la verifica di quanti token possieda un determinato wallet, la richiesta del link IPFS in cui sono conservati i metadati oppure l'identificazione dell'address che detenga un determinato token. Questi sono tutti i casi in cui non avviene una vera propria modifica e quindi una transazione sulla blockchain, ma solamente una lettura dello stato della blockchain in quel momento. Invece, è diversa la situazione quando si va 'scrivere' sulla blockchain attraverso il contratto. Infatti, in questi casi si sostengono dei costi da parte di chi invoca la determinata funzione, in quanto si sta andando a modificare lo stato della blockchain. Una parte dei costi sostenuti servono ad invogliare i miner o i validatori ad approvare la transazione e ad inserirla in un blocco. Esempi di 'scrittura' attraverso lo smart contract sono: il minting del NFT, l'updating del NFT, il transferring del NFT, il burning del NFT e il deployment dello smart contract stesso. Il mio lavoro è stato quello di testare, per ognuna di queste ultime funzioni elencate, il costo che dovrebbe sostenere Watchain su diverse blockchain. Per fare ciò, ho innanzitutto creato un nuovo wallet su Metamask. Per deployare il contratto sulla rete di test Sepolia, è necessario ottenere i token attraverso un faucet di Sepolia, il quale li distribuisce agli sviluppatori che intendono testare duramente il contratto in una modalità demo prima di deployarlo sulla blockchain reale. È importante testare il codice in un ambiente di questo tipo perché anche dei piccoli bug presenti nel software, una volta deployato il contratto, potrebbero compromettere tutta la soluzione proposta e quindi far fallire la missione aziendale.

Sepolia è una blockchain parallela di Ethereum con lo scopo di replicarla fedelmente; l'unica differenza sta nel fatto che i token utilizzati per portare a termine tutte le operazioni sono fittizi e non hanno un valore reale, ma la quantità richiesta per ogni operazione è esattamente la stessa. Quindi, una volta deployato il contratto, ho potuto portare a termine anche le operazioni di minting, transferring, updating e infine burning del NFT. Dopodichè, utilizzando Etherscan, ho trovato per ognuna di queste operazioni la quantità di gas che il contratto ha utilizzato. La quantità di gas dipende solamente dal contratto chiamato in causa; quindi, sarà la stessa anche per altre tipologie di blockchain. Le quantità di gas di cui si necessitano sono rappresentate nella tabella 5.1:

Contract	**Method**	**Gas needs [GAS]**
Watchain	burn	30919
Watchain	mint	117592
Watchain	safeTransformFrom	57856
Watchain	updateCertificate	31312
Watchain	Deployment	1282496

Tabella 5.1: Quantità di gas necessaria per ogni funzione

Ciò che cambia per ogni blockchain che si utilizza è il costo di ogni unità di gas, il quale dipende principalmente dalla congestione della rete, ossia da quante transazioni devono essere processate in quel preciso momento. Infatti, se si vuole che la propria transazione venga approvata e inserita in un blocco prima rispetto alle altre, è possibile pagare di più affinché tale transazione venga processata prima dai validatori, ottenendo la precedenza rispetto a quelle transazioni che pagano meno fee. Un'altra determinante del costo complessivo della transazione è il prezzo del token nativo della blockchain; quindi, più sarà elevato e più costerà effettuare la transazione su quella determinata blockchain. Quindi, una volta che ho tracciato la quantità di gas necessaria per chiamare ogni funzione di scrittura sulla blockchain, ho ricercato il prezzo del gas contemporaneamente sulle blockchain prese in esame attraverso i 'gas tracker' di ognuna di esse. Le blockchain prese in considerazione per tale analisi sono: Ethereum, Avalanche, Binance Smart Chain, Polygon, Moonriver e Fantom. Logicamente, su tutte queste blockchain appena citate è possibile deployare smart contract e mintare NFT. Dopodichè, moltiplicado la quantità di gas necessaria per il prezzo del gas si è ottenuto il costo della transazione in gwei o in formati equivalenti. In particolare, il gwei equivale a 10^{-9} ETH o nella currency corrispondente, nel caso diverso da Ethereum. Pertanto, si

ottiene così il prezzo della transazione nel formato del token nativo della blockchain. Infine, moltiplicando tale valore per il prezzo di cambio in euro in quel momento, si è ottenuto il prezzo in euro per ogni transazione in quel preciso momento. È importante dire che sarebbe stato possibile deployare realmente lo smart contract, simulare le transazioni su ogni rete di test per tutte le blockchain e notare il costo per ogni blockchain. Tuttavia, il limite è stato che per ottenere i token fittizi per operare sulle reti di test di blockchain meno note come quelle prese in esame, era necessario detenere una quantità minima di token reali sulle reti principali delle blockchain in questione.
I risultati dei test effettuati da me per ognuna delle blockchain prese in considerazione sono riassunti nelle tabelle: 5.2, 5.3, 5.4, 5.5, 5.6 e 5.7.

5.1 Ethereum

Al momento dell'analisi, il prezzo di una singola unità di gas equivaleva a 28,6 gwei. Allo stesso tempo, 1 ETH costava 1693€.

Contract	**Method**	**Gas needs [GAS]**	**Gas needs [gwei]**	**ETH**	**€**
Watchain	burn	30919	884283,4	0,000884	1,50
Watchain	mint	117592	3363131,2	0,003363	5,69
Watchain	safeTransformFrom	57856	1654681,6	0,001655	2,80
Watchain	updateCertificate	31312	895523,2	0,000896	1,52
Watchain	Deployment	1282496	36679385,6	0,036679	62,10

Tabella 5.2: Costo per ogni funzione su Ethereum

5.2 Polygon

Al momento dell'analisi, il prezzo di una singola unità di gas equivaleva a 67,6 gwei. Allo stesso tempo, 1 MATIC costava 0,61€.

Contract	**Method**	**Gas needs [GAS]**	**Gas needs [gwei]**	**MATIC**	**€**
Watchain	burn	30919	2090124,4	0,002090	0,00
Watchain	mint	117592	7949219,2	0,007949	0,00
Watchain	safeTransformFrom	57856	3911065,6	0,003911	0,00
Watchain	updateCertificate	31312	2116691,2	0,002117	0,00
Watchain	Deployment	1282496	86696729,6	0,086697	0,05

Tabella 5.3: Costo per ogni funzione su Polygon

5.3 Binance Smart Chain

Al momento dell'analisi, il prezzo di una singola unità di gas equivaleva a 3 gwei. Allo stesso tempo, 1 BNB costava 215,2€.

Contract	Method	Gas needs [GAS]	Gas needs [gwei]	BNB	€
Watchain	burn	30919	92757	0,000093	0,02
Watchain	mint	117592	352776	0,000353	0,08
Watchain	safeTransformFrom	57856	173568	0,000174	0,04
Watchain	updateCertificate	31312	93936	0,000094	0,02
Watchain	Deployment	1282496	3847488	0,003847	0,83

Tabella 5.4: Costo per ogni funzione su Binance Smart Chain

5.4 Avalanche

Al momento dell'analisi, il prezzo di una singola unità di gas equivaleva a 25,3 nAVAX. Allo stesso tempo, 1 AVAX costava 10,85€.

Contract	Method	Gas needs [GAS]	Gas needs [gwei]	AVAX	€
Watchain	burn	30919	782250,7	0,000782	0,01
Watchain	mint	117592	2975077,6	0,002975	0,03
Watchain	safeTransformFrom	57856	1463756,8	0,001464	0,02
Watchain	updateCertificate	31312	792193,6	0,000792	0,01
Watchain	Deployment	1282496	32447148,8	0,032447	0,35

Tabella 5.5: Costo per ogni funzione su Avalanche

5.5 Moonriver

Al momento dell'analisi, il prezzo di una singola unità di gas equivaleva a 1,3 gwei. Allo stesso tempo, 1 MOVR costava 4,12€.

Contract	Method	Gas needs [GAS]	Gas needs [gwei]	MOVR	€
Watchain	burn	30919	40194,7	0,000040	0,00
Watchain	mint	117592	7949219,2	0,007949	0,03
Watchain	safeTransformFrom	57856	3911065,6	0,003911	0,02
Watchain	updateCertificate	31312	2116691,2	0,002117	0,01
Watchain	Deployment	1282496	86696729,6	0,086697	0,36

Tabella 5.6: Costo per ogni funzione su Moonriver

5.6 Fantom

Al momento dell'analisi, il prezzo di una singola unità di gas equivaleva a 36 gwei. Allo stesso tempo, 1 FTM costava 0,23€.

Contract	Method	Gas needs [GAS]	Gas needs [gwei]	FTM	€
Watchain	burn	30919	1113084	0,001113	0,00
Watchain	mint	117592	4233312	0,004233	0,00
Watchain	safeTransformFrom	57856	2082816	0,002083	0,00
Watchain	updateCertificate	31312	1127232	0,001127	0,00
Watchain	Deployment	1282496	46169856	0,046170	0,01

Tabella 5.7: Costo per ogni funzione su Fantom

5.7 Considerazioni finali

Dallo studio condotto su queste differenti blockchain, il costo totale è risultato essere pari a quanto riportato nella tabella 5.8. Il costo totale è stato ottenuto sommando i costi di deployment, minting, transferring, burning and updating. Tuttavia, è importante notare che il costo per il deployment dello smart contract è il costo maggiore da sostenere su qualsiasi blockchain, ma allo stesso tempo è quella spesa da effettuare solo una volta. Invece, gli altri costi dovranno essere sostenuti ogni volta che, attraverso lo smart contract, si compie quella determinata azione sul NFT.

Blockchain	**Totale**
Ethereum	73,61€
Avalanche	0,42€
Polygon	0,06€
Binance Smart Chain	0,98€
Moonriver	0,41€
Fantom	0,01€

Tabella 5.8: Totale dei costi per ogni blockchain

Si nota come le blockchain Avalanche, Fantom, Polygon e Moonriver siano le più convenienti dal punto dei visti dei costi, in quanto hanno registrato un costo complessivo inferiore a 0,5€.

Ciononostante, reputo che sia importante analizzare anche altre caratteristiche di una blockchain oltre ai costi, nel caso si voglia sceglierne una di queste per applicarle in un contesto aziendale. A tal fine, le altre caratteristiche prese in considerazione sono state: scalabilità, storia, ecosistema, diffusione e interoperabilità.

Per quanto riguarda la scalabilità, un buon indicatore può essere il valore massimo di TPS registrato per ogni blockchain. Il TPS (Transactions per second) si riferisce al numero di transazioni che un sistema o una rete può elaborare entro un determinato periodo di tempo. È una misura della capacità ed efficienza del sistema nel gestire le transazioni. Valori più alti di TPS indicano che il sistema può elaborare un volume maggiore di transazioni in un periodo di tempo più breve. Raggiungere un alto TPS è spesso una sfida per le reti blockchain a causa delle limitazioni dei loro meccanismi di consenso e dell'infrastruttura di rete.

Per avere un'indicazione sulla storia della blockchain, ho considerato l'anno in cui è avvenuto il lancio. Una blockchain più datata, è più probabile che abbia già affrontato diversi problemi, come attacchi al meccanismo di consenso ed altri; quindi, se è sopravvissuta a tali problematiche, significa che può essere considerata una rete robusta in termini di sicurezza. Inoltre, in tal caso anche il codice dovrebbe essere più consolidato e meno soggetto a presentare dei bug. La differenza di anche pochi anni di vita tra una blockchain e un'altra, almeno in questo periodo, non può essere sottovalutata perché bisogna considerare che tutta la tecnologia Blockchain ha avviato la sua diffusione solo nel 2008.

Un'altra caratteristica che si è cercata di misurare è stato l'ecosistema, valutato attraverso il numero di dApp attualmente presente su ognuna di queste blockchain. Avere tante dApp sulla blockchain che si sta per scegliere potrebbe risultare utile in futuro per collaborare con un numero più ampio e diversificato di altre organizzazioni, o banalmente provando a intercettare gli utenti che già utilizzano quella determinata blockchain utilizzando altre dApp, in modo da sfruttare le esternalità positive che la rete può offrire.

Inoltre, per valutare l'adozione e la diffusione della blockchain la metrica di riferimento è stata il TVL, ossia Total Value Locked, il quale indica il valore totale di asset bloccati o vincolati nel protocollo della blockchain di riferimento. Tale parametro è di solito espresso in dollari o in un'altra valuta fiat. Poiché tutte le blockchain considerate nell'analisi utilizzano come algoritmo di consenso il Proof of Stake o qualche sua variante, il TVL è una buona rappresentazione del valore messo in staking dai nodi validatori. Quindi, più è alto il TVL e più dovrebbe essere affidabile e diffusa la blockchain, in quanto è considerata sicura dai nodi validatori.

Infine, un'ultima caratteristica che è stata valutata è l'interoperabilità tra le varie blockchain. Questa caratteristica è valutabile attraverso l'analisi di quali e quanti bridge una blockchain detiene con altre blockchain. La funzione dei bridge è quella di permettere di comunicare e scambiare asset con altre blockchain. Nel caso in questione, tutte le blockchain sono EVM compatibili, ciò significa che è possibile eseguire lo smart contract sulla macchina virtuale della rete Ethereum. Questo si traduce nella possibilità di utilizzare il codice dello smart contract senza modifiche sostanziali anche sulle altre blockchain EVM compatibili.

Nella tabella 5.9 sono riportati i valori trovati per le altre caratteristiche analizzate, al fine di compiere una valutazione più completa possibile.

Blockchain	**Max TPS**	**Lancio**	**dApp**	**TVL [M$]**
Avalanche	21,2	2020	400	568,48
Fantom	24,35	2018	245	54,7
Ethereum	57,91	2015	2800	24469
Polygon	63,36	2017	19000	820,3
Binance Smart Chain	318,5	2020	83	3000
Moonriver	0,4	2022	27	5,13

Tabella 5.9: Altre caratteristiche delle blockchain analizzate

A valle delle considerazioni fatte sulle caratteristiche sopra elencate, l'analisi condotta da me ha riscontrato che la blockchain con prestazioni migliori e più adatta al nostro scopo è Polygon. Infatti, tale blockchain è risultata sempre tra le prime posizioni per costi, scalabilità, storia e diffusione. Inoltre, è la blockchain che ospita più dApp nella propria rete, risultando così quella che possiede di gran lunga l'ecosistema più sviluppato.

Capitolo 6

Conclusioni

Nel corso di questa tesi, abbiamo intrapreso un viaggio nel mondo complesso e in continua evoluzione della tecnologia blockchain. Attraverso cinque capitoli distinti, abbiamo esplorato la tecnologia blockchain in generale, le sue applicazioni nei settori industriali chiave, la creazione di un marketplace di orologi di seconda mano basato su NFT e smart contract, e l'analisi dettagliata delle diverse blockchain disponibili. Inoltre, siamo giunti a una conclusione significativa: Polygon si è rivelata la soluzione ideale per la nostra piattaforma di orologi di seconda mano.

Il secondo capitolo ci ha fornito le basi teoriche per comprendere l'ecosistema blockchain, esaminando algoritmi di consenso, NFT e smart contract. Abbiamo acquisito familiarità con i concetti fondamentali e le caratteristiche chiave di questa tecnologia rivoluzionaria, preparandoci così all'analisi pratica che segue.

Il terzo capitolo ci ha condotto attraverso un'indagine approfondita sulle applicazioni attuali della blockchain in settori cruciali, quali l'agroalimentare, l'energetico, le costruzioni edili e il lusso. Abbiamo esaminato attentamente i vantaggi e gli svantaggi dell'implementazione della blockchain in ognuno di questi contesti, rivelando come questa tecnologia stia rivoluzionando processi e transazioni.

Il quarto capitolo ci ha permesso di mettere in pratica la nostra comprensione della blockchain, sviluppando con successo uno smart contract che permetterà di testare l'idea imprenditoriale del marketplace per orologi di seconda mano basato su NFT. Abbiamo dimostrato l'efficacia di questa soluzione, mostrando in modo pratico come i NFT e gli smart contract possano rivoluzionare il mercato di beni di lusso come gli orologi.

Il quinto capitolo ci ha condotti in un'analisi dettagliata delle diverse blockchain disponibili per lo sviluppo di smart contract. Abbiamo valutato criteri come il costo,

la scalabilità, l'ecosistema e l'interoperabilità, e abbiamo concluso affermando che Polygon è la scelta migliore per la nostra piattaforma.

Uno degli obiettivi futuri di Watchain sarebbe la creazione di una dApp, che abbia quindi il backend che lavori sulla blockchain, e che permetta di andare a recuperare tutte le transazioni (ad esempio come il 'transfer', 'update', e altre) e che li mostri all'utente, senza che quest'ultimo debba andare a ricostruire tutta la storia dell'orologio da sé attraverso l'explorer. Tale dApp si sposa bene con il concetto di mettere l'utente al centro del progetto, facendo in modo che il Web3 diventi più accessibile anche ai meno esperti.

Penso che sia importante affermare che, a valle di tutte le analisi condotte in questa tesi, sia fondamentale concepire la blockchain non come una tecnologia a sé stante; in quanto considerare la collaborazione con altre tecnologie come IoT e Intelligenza Artificiale possa far sì che il risultato finale crei un impatto più disruptive nel settore economico di collazione della tecnolgia. A proposito di quanto appena detto, nel nostro progetto sarebbe interessante in futuro allenare un algoritmo di IA che sia in grado di rilevare criticità e originalità di alcuni orologi, in modo da automatizzare ancora di più la soluzione e renderla scalabile al massimo.

Questa tesi non è stata solo un esercizio accademico, ma un'esplorazione che ha coniugato la passione per la tecnologia blockchain con la volontà di intraprendere un percorso imprenditoriale. Questo lavoro ha dimostrato che la blockchain non è solo una tecnologia futuristica, ma una realtà che sta trasformando industrie e apre nuove opportunità. Il futuro è promettente per chi abbraccia questa innovazione e la sfrutta in modo creativo.

In sintesi, questa tesi costituisce un'analisi esaustiva e pratica della tecnologia blockchain e delle sue varie applicazioni. È un punto di partenza essenziale per ricerche future e un invito a esplorare le innumerevoli possibilità offerte da questa rivoluzionaria tecnologia. La blockchain si è rivelata ben più di una mera innovazione tecnologica: è una forza trasformatrice destinata a plasmare il nostro avvenire in modi che oggi appena intravediamo. È giunto il momento di abbracciare questa rivoluzione e, con fervida creatività e impegno instancabile, dare forma a un mondo migliore.

Bibliografia

[1] David Chaum, Ronald L Rivest e Alan T Sherman. «CRYPTO'82». In: *Advances in Cryptology 1981–1997: Electronic Proceedings and Index of the CRYPTO and EUROCRYPT Conferences 1981–1997*. Springer. 1998, pp. 13–19 (cit. a p. 3).

[2] Daniel Burkhardt, Maximilian Werling e Heiner Lasi. «Distributed ledger». In: *2018 IEEE international conference on engineering, technology and innovation (ICE/ITMC)*. IEEE. 2018, pp. 1–9 (cit. a p. 5).

[3] Aisha Zahid Junejo, Manzoor Ahmed Hashmani e Abdullah Abdulrehman Alabdulatif. «A survey on privacy vulnerabilities in permissionless blockchains». In: *International Journal of Advanced Computer Science and Applications (IJACSA)* 11.9 (2020), pp. 130–139 (cit. a p. 8).

[4] Satoshi Nakamoto. «Bitcoin: A Peer-to-Peer Electronic Cash System». In: (mag. 2009). URL: http://www.bitcoin.org/bitcoin.pdf (cit. a p. 9).

[5] Artur Meynkhard. «Fair market value of bitcoin: Halving effect». In: *Investment Management & Financial Innovations* 16.4 (2019), p. 72 (cit. a p. 9).

[6] Vitalik Buterin et al. «A next-generation smart contract and decentralized application platform». In: *white paper* 3.37 (2014), pp. 2–1 (cit. a p. 17).

[7] Sumit K Rana, Arun K Rana, Sanjeev K Rana, Vishnu Sharma, Umesh Kumar Lilhore, Osamah Ibrahim Khalaf e Antonino Galletta. «Decentralized model to protect digital evidence via smart contracts using layer 2 polygon blockchain». In: *IEEE Access* (2023) (cit. a p. 22).

[8] Xiaofeng Chen, Xiangjuan Jia, Lu Zhang e Liang Cai. «Optimization of Blockchain Storage Architecture Based on Voronoi Diagram». In: *2022 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS)*. IEEE. 2022, pp. 1223–1227 (cit. a p. 23).

[9] Qian Li e Yingli Wang. «Blockchain's role in supporting circular supply chains in the built environment». In: (2021), pp. 578–583. DOI: 10.1109/Blockchain53845.2021.00087 (cit. a p. 29).

[10] Roberta De Angelis, Mickey Howard e Joe Miemczyk. «Supply chain management and the circular economy: towards the circular supply chain». In: *Production Planning & Control* 29.6 (2018), pp. 425–437 (cit. a p. 33).

[11] Denis J Scott, Tim Broyd e Ling Ma. «Exploratory literature review of blockchain in the construction industry». In: *Automation in construction* 132 (2021), p. 103914 (cit. a p. 33).

[12] Abderahman Rejeb, John G Keogh, Suhaiza Zailani, Horst Treiblmaier e Karim Rejeb. «Blockchain technology in the food industry: A review of potentials, challenges and future research directions». In: *Logistics* 4.4 (2020), p. 27 (cit. a p. 34).

[13] Bowen Tan, Jiaqi Yan, Si Chen e Xingchen Liu. «The impact of blockchain on food supply chain: The case of walmart». In: *Smart Blockchain: First International Conference, SmartBlock 2018, Tokyo, Japan, December 10–12, 2018, Proceedings 1*. Springer. 2018, pp. 167–177 (cit. a p. 35).

[14] Petter Olsen, Melania Borit e Shaheen Syed. «Applications, limitations, costs, and benefits related to the use of blockchain technology in the food industry». In: *Nofima rapportserie* (2019) (cit. a p. 38).

[15] Julija Golosova, Andrejs Romanovs e Nadezhda Kunicina. «Review of the blockchain technology in the energy sector». In: *2019 IEEE 7th IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*. IEEE. 2019, pp. 1–7 (cit. a p. 39).

[16] Qiang Wang e Min Su. «Integrating blockchain technology into the energy sector—from theory of blockchain to research and application of energy blockchain». In: *Computer Science Review* 37 (2020), p. 100275 (cit. a p. 41).

[17] Asma Khatoon, Piyush Verma, Jo Southernwood, Beth Massey e Peter Corcoran. «Blockchain in energy efficiency: Potential applications and benefits». In: *Energies* 12.17 (2019), p. 3317 (cit. a p. 43).

[18] Mehmet Parlak, Nurkan Fatih Altunel, Utku Ayaz Akkaş e Emir Tarık Arici. «Tamper-Proof Evidence via Blockchain for Autonomous Vehicle Accident Monitoring». In: *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)*. IEEE. 2022, pp. 1–6 (cit. a p. 46).

[19] Arpan Kumar Kar e L Navin. «Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature». In: *Telematics and Informatics* 58 (2021), p. 101532 (cit. a p. 47).

[20] Shakil Ahmad e Charu Saxena. «Internet of Things and Blockchain technologies in the insurance sector». In: *2022 3rd International Conference on Computing, Analytics and Networks (ICAN)*. IEEE. 2022, pp. 1–6 (cit. a p. 47).

[21] Juliette Herinckx e Rosalie Ghislain. «The Use of Blockchain to Fight Counterfeiting in the Second-Hand Luxury Fashion Market». In: () (cit. a p. 48).

[22] AL-Issa Nermain, Marsela Thanasi-Boçe e Omar Ali. «Boosting Luxury Sustainability Through Blockchain Technology». In: *Blockchain Technologies in the Textile and Fashion Industry* (2022), p. 17 (cit. a p. 51).