LUISS

DIPARTIMENTO DI GIURISPRUDENZA

Cattedra di Economia Politica

BLOCKCHAIN E SMART CONTRACT:

Una panoramica sulle applicazioni, le sfide e le opportunità

RELATORE
Prof. **Cesare Pozzi**

CANDIDATO
Salvatore Bonanno
Matr. **104793**

CORRELATRICE
Prof. ssa. **Maria Federica Izzo**

ANNO ACCADEMICO 2021/2022

BLOCKCHAIN E SMART CONTRACT:
una panoramica sulle applicazioni, le sfide e le opportunità

INDICE

INTRODUZIONE

Mi preme iniziare la tesi rispondendo ad una domanda postami da un ipotetico interlocutore: “perché la scelta di questo argomento?”.

Sono un neofita della materia, lontano dall’essere un esperto informatico, ma l’eco che Bitcoin e le criptovalute in generale, hanno avuto negli ultimi anni è stato talmente forte da aver raggiunto anche “noi non addetti ai lavori”.

La mia curiosità mi ha portato a voler approfondire questa tematica, e dopo aver letto il libro ”Da zero alla luna“ di Gian Luca Comandini, mi si è aperto un mondo, nuovo e sconosciuto, ed ho visto questa tesi come l’espediente per meglio conoscerlo ed approfondirlo.

Bitcoin, uso impropriamente questo termine per riferirmi in generale sia alle criptovalute che alla tecnologia retrostante, è nato molti anni fa nel lontano 2008, ma la maggior parte di noi ne è venuta a conoscenza solo negli ultimi anni. Nasce come argomento di nicchia, non ha avuto subito una rapida diffusione, anzi, durante i primi anni era ritenuto come un qualcosa di inutile, che annoiava, o ancor peggio “la solita truffa informatica”.

Poi però, d’un tratto, è diventato una vera e propria moda e dagli Usa è arrivata, con ritardo, anche qui in Italia: tutti i media hanno iniziato a parlarne, in modo superficiale, non trattando la materia dal punto di vista tecnico ma solo dal punto di vista della speculazione finanziaria, generando in noi una visione distorta di Bitcoin, quasi come fosse un “gratta e vinci” che ci avrebbe reso milionari investendo pochi euro.

Tutti parlavano di Bitcoin, ma in pochi sapevano realmente cosa fosse, alimentando false convinzioni e speranze.

Le conseguenze di questa disinformazione non tardarono ad arrivare ed in molti persero gran parte del loro investimento. Nell’immediato, la “moda bitcoin” sparì ed

anzi, questo fenomeno venne sempre più associato ad una truffa, ad una bolla che sta per scoppiare.

Fortunatamente questo trend negativo passò rapidamente e finalmente ci fu qualcuno che iniziò a chiedersi cosa realmente fosse Bitcoin e si capì che in realtà era solo la punta di un iceberg e che l'aspetto interessante e rivoluzionario era tutto ciò che ne stava alla base: la Blockchain.

Tuttavia, ancora oggi, nonostante la curiosità e la "moda cripto" sia tornata in auge, in pochi sanno che alla base delle criptovalute ci sia proprio la blockchain come tecnologia imprescindibile per la loro esistenza.

Quindi, il fine della mia ricerca sarà quello di concentrarmi su questa tecnologia, analizzarla e comprenderne le sue potenzialità e cercare di descriverne la sua evoluzione nonché le applicazioni pratiche.

CAPITOLO PRIMO

LA BLOCKCHAIN

1.1 STORIA E SVILUPPO DELLA BLOCKCHAIN

1.1.1 Definizione

Nei primi anni di diffusione del bitcoin quasi mai ad esso veniva accostato anche il termine blockchain, la tecnologia che ne sta alla base e che sarà il fulcro del nostro studio.

Solo di recente l'interesse si è concentrato su questa tecnologia per le grandi potenzialità ed applicazioni che può avere nei più disparati settori.

Volendo dare una definizione tecnica di blockchain, la cui traduzione letterale " catena di blocchi", è una struttura di dati decentralizzata, condivisa e crittograficamente immutabile.

Si tratta dunque di un registro che contiene una serie di dati e transazioni che vengono ripartite in una serie di " blocchi" di dati, inseriti e convalidati attraverso un meccanismo di consenso distribuito su tutti i nodi della rete. I nodi sono costituiti a loro volta dai server di ciascun partecipante, usati per prender parte alla decisione. Cercando di semplificare il concetto, la blockchain[1] "*è una sorta di libro mastro ,distribuito e gestito da una rete di computer ,ognuno dei quali ne possiede una copia".*

Per aggiungere poi un nuovo blocco alla catena, è previsto un preciso protocollo basato sul consenso tra questi computer (che rivestono la funzione di nodi). Una volta compiuta questa procedura di autorizzazione, ogni nodo (computer) aggiornerà la propria copia, senza poi più alcuna possibilità di modificare i dati che verranno inseriti e validati in quel blocco.

[1] COMANDINI G., *Da Zero alla Luna. La Blockchain: quando, come, perché sta cambiando il mondo*, Palermo, DarioFlaccovioEditore, marzo 2022, n. 61.

Il blocco non è altro che un file che si divide in due parti :

- *header*: che contiene tutta una serie di dati imprescindibili, come il numero identificativo del blocco, il codice hash sia di questo blocco che di quello precedente, l'ora e la data in cui è stato generato e la sua dimensione in kilobyte

- *body*: il quale contiene tutte le transazioni registrate su quel blocco.

  Ovviamente più transazioni sono contenute nel blocco, maggiore è la sua dimensione.

  Il fatto che all'interno dell'header ci sia l'hash[2] sia di quel blocco che di quello precedente, fa sì che i blocchi siano collegati tra loro e che si crei questa sorta di "catena", collegando quindi ogni blocco sia a quello precedente che a quello successivo.

  Questo ci permette di risalire a qualsiasi transazione contenuta nei blocchi.

  Inoltre ogni transazione che viene compiuta su blockchain è caratterizzata da un input e da un output, che indicano il soggetto da cui parte la criptovaluta che si sta spostando e quello a cui arriva. All'interno del blocco è presente anche un codice alfanumerico, lo script[3], che ci dà ulteriori informazioni sia sull'input che sull'output. Lo script a sua volta si compone di due elementi:

  - *public key*: "chiave pubblica" è la chiave che appartiene all'output della transazione che gli permette di riscattare il contenuto dell'output

  - *signature:* "firma dell'hash" che certifica l'originalità della transazione e che il proprietario era legittimato ad eseguirla.

[2] Un hash (o funzione hash) è una funzione matematica che mappa un input di dati di qualsiasi dimensione in un output di dimensioni fisse. L'output, chiamato hash o digest, è una rappresentazione univoca e codificata dei dati di input.

[3] Lo script non è altro che un particolare programma scritto in uno specifico linguaggio di programmazione che, accompagnando le transazioni, istruisce i nodi su cosa fare con i dati presenti nelle transazioni.

Dunque, lo script contenuto nella transazione può essere risolto solo con una specifica chiave privata o con la chiave pubblica, usata per creare lo script stesso.

Questa è una delle garanzie su cui poggia l'intera tecnologia blockchain.

In conclusione, l'utilizzo della tecnologia blockchain si focalizza su due aspetti: registrare un qualsiasi tipo di evento ed assicurarsi che questa registrazione rimanga in eterno.

La conseguenza pratica è che diviene vantaggioso il suo utilizzo quando due persone vogliono concludere tra loro un accordo, ma non si fidano l'una dell'altra e quindi tramite la blockchain questa transazione viene portata a compimento con successo, senza che ci sia bisogno che questo accordo si fondi sulla fiducia reciproca.

1.1.2 Cenni storici

L'evento storico che ha dato il via al "fenomeno bitcoin" è il paper pubblicato da Satoshi Nakamoto nel 2008 intitolato "*Bitcoin: A Peer-to-Peer Elettronic Cash System*", in cui veniva prefigurato un utilizzo diverso di tecnologie già conosciute al fine di dar vita ad un nuovo sistema di pagamento elettronico.

Ed è proprio in ciò che risiede, secondo Massimiliano Nicotra in "*Smart contract criptovalute e blockchain*", l'aspetto più importante ed innovativo del paper: l'originalità con cui venivano assemblate una serie di tecnologie che erano già note ai tempi e che permisero di risolvere una serie di problematiche legate ai pagamenti a distanza.

I sistemi tradizionali sono incentrati sul concetto della fiducia, la quale viene garantita dalla presenza di enti centrali (banche , istituti di pagamento ecc…) che si occupano di annotare le transazioni operando quindi come terze parti fidate.

Per gli ideatori di Bitcoin questo era un punto debole del sistema, in quanto la presenza della

terza parte fiduciaria, oltre a comportare delle spese, non permetteva l'irreversibilità delle transazioni. Inoltre, per effettuare queste transazioni elettroniche i commercianti richiedono sempre, questo perché alla base manca la fiducia verso il contraente, una serie di informazioni e dati personali al cliente di cui altrimenti non avrebbero bisogno; contrariamente, invece, ciò non accade quando il pagamento è effettuato personalmente tramite moneta fisica.

Pertanto, i creatori della prima blockchain, con questo paper, cercano di superare le criticità dovute alla mancanza di fiducia, adottando un sistema dove la stessa, garantita dagli intermediari, viene sostituita da qualcosa di diverso, capace di rendere le transazioni sicure attraverso la loro irreversibilità e indisponibilità di risorse già utilizzate.

Questo sistema innovativo, capace di sostituire la fiducia, è la prova crittografica che si serve di chiavi asimmetriche di cifratura, marche temporali e funzione di hash, al fine di costruire un database in cui tutte le transazioni che si svolgono tra i partecipanti vengono memorizzate. Nello specifico:

- le chiavi simmetriche hanno la funzione di associare una transazione in modo univoco al mittente ed al destinatario;

- le marche temporali assicurano la conseguenzialità cronologica delle scritture;

- la funzione di hash invece dà un'impronta informatica alle informazioni contenute nella transazione e serve a renderle immodificabili, in quanto un'eventuale loro modifica verrebbe subito rilevata dal sistema e non ci sarebbe più il legame con i contenuti delle transazioni precedenti.

Pertanto, combinando queste tecnologie, si vanno a risolvere tutta una serie di criticità che caratterizzano i sistemi di pagamento elettronici, eliminando completamente la presenza di intermediari e cosa ancor più importante risolvendo il problema del double spending[4].

Volendo andare ancor più indietro nel tempo, possiamo trovare un esempio primordiale di blockchain già nel 1400 d.C. ad opera degli abitanti dell'isola di Yap. Gli indigeni avvertirono il bisogno di avere una moneta per regolare i loro scambi e scelsero il calcare, una roccia che scarseggiava sulla loro isola, che divenne quindi il loro "denaro di pietra".

I primi problemi sorsero quando si resero conto che queste pietre erano troppo grandi per essere trasportate facilmente e lasciandole incustodite c'era il rischio che gli venissero sottratte dagli altri abitanti.

Quindi già allora, come oggi, il problema principale era la fiducia.

Fu così che inventarono una prima forma di blockchain: ogni abitante del luogo aveva un registro in cui annotava la proprietà delle singole pietre; nel momento in cui si faceva una transazione, questa veniva annotata e tutti gli abitanti erano invitati ad aggiornare il proprio registro trascrivendola. Quindi, eliminarono sin da subito la necessità di un'autorità centrale, (l'odierna banca) rimanendone slegati, dunque non pagando alcuna commissione ad essa. Eliminarono di conseguenza anche il problema del double spending perché ogni transazione veniva aggiornata da tutti sul proprio registro; pertanto, tutti sapevano in quel momento chi fosse il legittimo proprietario del bene.

L'impronta di quel sistema decentralizzato è rimasta nella nostra società moderna, la quale ha semplicemente provveduto ad aggiornarlo con l'applicazione di nuove tecnologie ai tempi sconosciute.

[4] Double spending o doppia spesa, potenziale problema o falla di un sistema di pagamenti digitale che consente di spendere una moneta digitale più di una volta in modo illecito. Nel settore delle criptovalute, l'attacco della doppia spesa (double-spending attack), ovvero un attacco posto in essere sfruttando la falla della doppia spesa, è stato portato a termine con successo su alcune altcoin (Comandini G., *Da Zero alla Luna. La Blockchain: quando, come, perché sta cambiando il mondo*, Palermo, DarioFlaccovioEditore, marzo 2022).

1.2 L'EVOLUZIONE DEI REGISTRI DLT E BLOCKCHAIN

"*Sin dalle origini i registri sono nati come una sorta di memoria della società, successivamente sono diventati anche uno strumento per automatizzare le attività degli uomini e, soprattutto, delle macchine. Li usiamo ogni volta che abbiamo bisogno di un consenso sui fatti. Dato che il registro è una delle basi fondamentali della società, perché mappa le relazioni economiche e sociali tra le persone, si deve prestare attenzione a chi ne ha la proprietà e la gestione. Se è una terza parte, allora dobbiamo avere fiducia o firmare un contratto che la obbliga alle responsabilità*" Così Massimo Chiaratti, nella prefazione del libro " Da Zero alla Luna. La Blockchain: quando, come, perché sta cambiando il mondo" di G. Comandini, definisce l'importanza che hanno i registri per la società.

I registri centralizzati sono esistiti per secoli, con lo scopo di mantenere informazioni importanti in un'unica posizione centralizzata per facilitare l'accesso e il controllo.

Tuttavia, la loro evoluzione è stata influenzata dalle tecnologie disponibili, dalle esigenze delle società e dalle preoccupazioni per la privacy e la sicurezza dei dati.

In epoca antica, i registri centralizzati erano spesso tenuti da funzionari governativi o religiosi, come ad esempio i registri dei censimenti e delle proprietà terriere.

Durante il Medioevo, la Chiesa Cattolica manteneva registri centralizzati dei battesimi, dei matrimoni e delle morti, che erano utilizzati per la gestione delle parrocchie e per il pagamento delle tasse.

Con l'avvento della stampa, la tenuta dei registri centralizzati divenne più efficiente e il loro utilizzo si estese a settori come la contabilità, la gestione delle scorte e il controllo degli accessi. Con l'avvento del computer e dell'era digitale, i registri centralizzati sono diventati sempre più sofisticati. Oggi, molte organizzazioni utilizzano database centralizzati per gestire informazioni come: i dati dei clienti, le informazioni sulle transazioni finanziarie e i registri medici. Tuttavia, il crescente uso di questi database centralizzati ha sollevato

preoccupazioni per la privacy e la sicurezza dei dati, portando alla ricerca di soluzioni alternative.

Queste, sono state favorite sia dall'evoluzione tecnologica con l'avvento di Internet, che dall'introduzione di nuove tecniche come la crittografia, il tutto ha permesso di avere una nuova visione dei registri e della loro struttura, capace di superare le criticità dei sistemi centralizzati.

Pertanto, ci si allontana sempre più dalla concezione di un sistema centralizzato, da cui dipendono tutti gli utenti, e dalle conseguenze negative che potrebbero insorgere in caso di malfunzionamento.

Iniziano, quindi, a diffondersi le prime forme di *Distributed Ledger Technology*[5] (DLT).

Le transazioni o le informazioni sono registrate in modo permanente su una rete di nodi, eliminando la necessità di un' entità centralizzata che controlli il database.

"*La distribuzione è una configurazione di rete in cui i partecipanti possono comunicare tra di loro senza passare attraverso un punto centralizzato. Esistono percorsi multipli per la comunicazione e anche se c'è il venir meno di qualsiasi partecipante, ciò non impedisce la comunicazione. Tale meccanismo è conosciuto anche come distribuzione peer-to-peer (P2P) che implica il funzionamento senza un database centrale*".[6]

L'innovativa forma di registro distribuito proposto, si presta ad avere varie strutture, ciascuna con le sue peculiarità. La tecnologia blockchain fa parte di questo ampio gruppo di DLT. I sistemi blockchain a loro volta presentano delle differenze al loro interno: nascono col fine di svolgere delle transazioni che cambiano in base al livello di programmabilità, con cui si intende la capacità del sistema di prevedere alcune condizioni che regolino il trasferimento degli asset all'interno della rete.

[5] la DLT (Distributed Ledger Technology) è un tipo di database distribuito che consente a più parti di avere accesso simultaneo agli stessi dati in modo sicuro e trasparente.

[6] Stralcio estratto dal documento *Technical report FG DLT D4.1,Distributed Ledger Technology regulatory framework*, ITU-T, 2019.

In alcuni sistemi blockchain questa possibilità è assente, in altri come la blockchain Bitcoin è limitata, mentre nella rete Ethereum c'è la possibilità di inserire un linguaggio di programmazione capace di svolgere un qualsiasi programma all'interno del sistema, il cosiddetto *smart contract* è un contratto informatico programmabile che esegue automaticamente e in modo autonomo le clausole del contratto stesso, senza bisogno di intermediari o di autorità centrali per la loro esecuzione (approfondirò la tematica nel prossimo capitolo).

In sintesi, la blockchain è una forma specifica di DLT che utilizza la crittografia per creare una catena di blocchi, mentre la DLT è un concetto più ampio che comprende la blockchain e altre forme di registro distribuito.

1.3 LE TECNOLOGIE ALLA BASE DELLA BLOCKCHAIN

Gli elementi imprescindibili per il funzionamento di una blockchain sono essenzialmente due: la crittografia e la rete internet.

La crittografia è la "*tecnica di rappresentazione di un messaggio in una forma tale che l'informazione in esso contenuta possa essere recepita solo dal destinatario; ciò si può ottenere con due diversi metodi: celando l'esistenza stessa del messaggio o sottoponendo il testo del messaggio a trasformazioni che lo rendano incomprensibile*"[7].

La blockchain utilizza algoritmi di crittografia avanzati per garantire la sicurezza e la privacy delle transazioni, mentre la crittografia permette di garantire l'integrità dei dati e di evitare la manipolazione o la falsificazione delle transazioni.

[7] Stralcio estratto da BATTAGLINI. R., GIORDANO M., *Blockchain e smart contract: funzionamento, profili giuridici e internazionali, applicazioni pratiche,* 2019.

La crittografia, dunque, si basa sull'utilizzo di algoritmi matematici complessi per convertire i dati in un formato cifrato, ovvero illeggibile senza una chiave segreta per decifrare il messaggio.

Esistono diversi tipi di algoritmi crittografici, tra cui gli algoritmi di cifratura simmetrica e asimmetrica. Gli algoritmi di cifratura simmetrica utilizzano una singola chiave segreta per cifrare e decifrare i dati, mentre gli algoritmi di cifratura asimmetrica utilizzano una coppia di chiavi, una pubblica e una privata, per proteggere i dati.

Con l'avvento di Internet e l'evoluzione tecnologica, oggi è stato possibile passare da un sistema a cifratura simmetrica, in cui si utilizzava una stessa chiave per criptare e decriptare, ad un sistema asimmetrico con l'inserimento di due chiavi distinte: una pubblica che serve a criptare ed una privata per decriptare. Quella privata è nota, ovviamente, solo al destinatario del messaggio e verrà utilizzata per decifrarlo.

Questo sistema così prospettato però, non risulta invulnerabile. Potrebbe accadere, infatti, che un terzo intercetti il messaggio e riesca a manometterlo utilizzando la chiave pubblica senza che il destinatario se ne accorga, cifrando al termine del procedimento un messaggio diverso rispetto a quello originario.

Per risolvere questa problematica la blockchain si serve di una doppia cifratura combinata con la funzione di hash.

La funzione di hash è una funzione matematica che converte i dati di input in una stringa di output fissa di lunghezza prefissata, chiamata "hash". La funzione di hash è progettata per essere unidirezionale, ovvero, non è possibile ottenere l'input originale a partire dall'hash.

L'utilità di questa funzione è che se il messaggio originario viene modificato, si genera il cosiddetto "effetto valanga", una radicale alterazione di tutto l'hash. Quindi, risulta molto efficace per verificare l'autenticità del messaggio originario. In caso di manomissione, infatti, l'hash finale risulterebbe diverso rispetto a quello precedente.

Ci sono varie tipologie di funzioni di Hash: MD4,MG5,SHA-256 ecc…

Quella che viene utilizzata per il protocollo Bitcoin è la SHA-256, che non è altro che un aggiornamento avvenuto nel 2001 sulla sua forma precedente, la SHA, che era stata sviluppata invece nel 1993 dall'NSA (National Security Agency).

Il risultato di questa funzione è quello di restituirci sempre una stringa alfanumerica di 256 bit, che muta completamente non appena il messaggio originario cambia anche di una semplice virgola.

Un'altra tecnologia su cui si basano le criptovalute in generale ed anche Bitcoin è l'algoritmo chiamato *Proof of Work* (PoW)[8].

Uno degli aspetti rivoluzionari, contenuti nel Paper di Nakamoto è proprio il meccanismo di incentivazione dei partecipanti, che insieme alle tecniche crittografiche, garantisce l'immutabilità del registro distribuito.

Si arriva pertanto a questa immutabilità sia con la funzione di hash, ma soprattutto grazie a questo sistema di "ricompense" che dissuade i partecipanti al network dal compiere comportamenti fraudolenti. Le transazioni vengono convalidate tramite un meccanismo automatico che richiede ai nodi che vogliono operare come miners la risoluzione di un problema matematico.

I problemi matematici sono degli enigmi utilizzati dal sistema Bitcoin, che oltre alla funzione di Hash, ne comprendono altre due tipologie: la scomposizione in numeri primi, che consiste nel rappresentare un numero come moltiplicazione di altri due numeri ed il Guided Tour Puzzle[9] (GTP) protocol.

[8] Proof-of-Work (PoW) indica l'algoritmo di consenso alla base di una rete blockchain. Questo algoritmo viene utilizzato per confermare le transazioni e produrre i nuovi blocchi della catena. PoW incentiva i miner a competere tra loro nell'elaborazione degli scambi, ricevendo in cambio una ricompensa.

[9] Il protocollo Guided Tour Puzzle (GTP) è un protocollo crittografico per mitigare gli attacchi Denial of Service a livello di applicazione . Ha lo scopo di superare il difetto dei protocolli di puzzle basati sul calcolo , in cui i client sono tenuti a elaborare CPU hard o puzzle legati alla memoria che favoriscono i client con abbondanti risorse computazionali.

Il problema nel sistema Bitcoin è definito Hashcash e la difficoltà dell'algoritmo cambia in maniera proporzionale alla potenza computazionale della rete.

Il primo che riesce a risolvere il "problema" è qualificato a validare la transazione, dopo aver ricevuto la conferma sulla soluzione. Il tutto richiede quindi grande capacità computazionale del computer per risolverlo in tempi brevi.

Il meccanismo di risoluzione del problema richiede impiego di risorse e viene chiamato "proof of work" (PoW).

Il primo minatore, quindi, riceve una ricompensa in criptovaluta e il blocco contenente le transazioni appena validate viene aggiunto alla blockchain.

Questo processo viene chiamato "mining" (minaggio) e richiede molta potenza di calcolo. Un ulteriore incentivo è la cosiddetta "fee", che è una tariffa che il mittente paga al minatore per velocizzare la transazione. Questo premio, secondo il paper di Nakamoto, incentiva i nodi a rimanere onesti ma è anche un modo per distribuire inizialmente la moneta, non essendoci un'autorità centrale che la emetta la PoW; inoltre è alla base anche di altre criptovalute come Ethereum e Litecoin.

La sicurezza della PoW si basa sulla difficoltà di risolvere il problema matematico e tale difficoltà viene aumentata automaticamente dalla rete in base alla potenza di calcolo totale degli utenti che partecipano al mining. Questo rende molto difficile modificare i blocchi esistenti, in quanto ciò richiederebbe una quantità enorme di potenza di calcolo.

Tuttavia, la PoW è anche criticata per il suo elevato consumo di energia, e ciò deriva dal fatto che i minatori devono risolvere un gran numero di problemi computazionali complessi per partecipare al mining.

1.4 GLI ATTACCHI ALLA RETE

Nonostante la solidità della tecnologia blockchain, questa non è immune da attacchi. L'eventuale successo di questi attacchi, però, non è dovuto tanto alla bravura degli hacker, ma spesso alla poca esperienza degli utenti.

La crittografia garantisce come abbiamo visto la sicurezza del sistema, ma ci sono alcuni attacchi che potrebbero aver successo nei confronti di alcune tipologie di blockchain.

1.4.1 L'Attack 51%

Il "51% Attack" è un attacco informatico che può essere eseguito contro una blockchain che si basa su un metodo di consenso Proof of Work (come quella di Bitcoin) da un gruppo di miner che detiene il controllo della maggioranza della potenza di calcolo della rete. In pratica, quando i miner di una blockchain competono per la creazione di un nuovo blocco e la sua validazione, il gruppo di miner che controlla il 51% della potenza di calcolo della rete, può creare una versione della blockchain alternativa e rifiutare le transazioni della blockchain originale. Ciò significa che il gruppo di miner potrebbe escludere determinate transazioni, inclusi i trasferimenti di criptovalute, e riscrivere la cronologia delle transazioni, in modo da invalidare le transazioni precedenti e sottrarre fondi a determinati utenti.

Un attacco del genere potrebbe minare la fiducia degli utenti nella sicurezza e l'integrità della blockchain colpita, e causare gravi danni economici. Tuttavia, è importante sottolineare che eseguire un 51% Attack richiede una potenza di calcolo immensa, costosa e difficile da ottenere, per questo la maggior parte delle blockchain decentralizzate sono progettate per resistere a questo tipo di attacco.

In generale però, un soggetto che riuscisse a raggiungere una capacità computazionale pari al 51% dovrebbe trovare economicamente più vantaggioso usarla per estrarre risorse anziché per alterare il sistema.

Infatti, essendo la blockchain immodificabile, una sua alterazione sarebbe evidente e la conseguenza inevitabile sarebbe la sfiducia dei suoi partecipanti con un crollo della criptovaluta associata, ciò provocherebbe, quindi, un danno economico proprio al soggetto che ha provato a frodare il sistema con un crollo del valore delle sue risorse.

1.4.2 Il Distributed Denial of Service (DDoS)

Il Distributed Denial of Service (DDoS) è un tipo di attacco che mira a saturare la rete di una blockchain con una grande quantità di transazioni o richieste, rendendo il sistema inutilizzabile o rallentandone notevolmente le prestazioni. In questo tipo di attacco, gli aggressori utilizzano una grande quantità di computer o dispositivi connessi in rete per inviare una grande quantità di transazioni o richieste alla rete della blockchain. L'obiettivo è quello di occupare tutta la capacità della rete e impedire l'elaborazione delle transazioni legittime, causando così la congestione della rete e la sua paralisi. L'attacco DDoS su blockchain può essere particolarmente pericoloso perché la blockchain è stata progettata per essere decentralizzata e resistente agli attacchi informatici, ma un attacco DDoS può sovraccaricare la rete e causare problemi di prestazioni o addirittura la sua interruzione. Gli sviluppatori delle blockchain stanno lavorando costantemente per migliorare la sicurezza delle loro reti e prevenire gli attacchi DDoS utilizzando metodi come la limitazione della quantità di transazioni accettate in un determinato periodo di tempo o l'implementazione di meccanismi di consenso resistenti agli attacchi DDoS.

1.4.2 L'ignoranza

Ebbene sì, il pericolo più grande per una blockchain sono gli esseri umani.

Infatti, gli hacker non cercano di attaccare direttamente la blockchain o i wallet[10], i quali sono sicuri grazie alla crittografia, ma il loro bersaglio principale siamo noi.

Molto spesso per negligenza o paura di dimenticarci le password dei wallet, affidiamo i nostri fondi a siti terzi che non hanno standard di sicurezza elevati e sono facilmente hackerabili oppure, ancora peggio, veniamo truffati dalle consuete email di phishing[11] che riceviamo quotidianamente.

Quindi per rendere la tecnologia realmente invulnerabile, non ci sarà solo bisogno di un quasi naturale avanzamento tecnologico, ma questo, deve essere accompagnato da una formazione degli utenti della rete che devono essere informati su ciò che devono fare per salvaguardare le proprie risorse.

1.5 LE DIVERSE TIPOLOGIE DI BLOCKHAIN

Esistono diversi tipi di blockchain che differiscono per il loro grado di accessibilità, trasparenza, gestione e controllo. Le scelte di progettazione dipendono dalle esigenze specifiche delle organizzazioni e dalle finalità per cui la blockchain viene utilizzata.

Possono essere:

- *permissionless*; le blockchain pubbliche sono accessibili da chiunque e le transazioni vengono verificate e registrate da una rete decentralizzata di nodi. Le blockchain

[10] Il wallet o portafoglio digitale, noto anche come portafoglio elettronico, è un dispositivo elettronico, un servizio online o un programma software che consente a una parte di effettuare transazioni elettroniche con un'altra parte barattando unità di valuta digitale per beni e servizi.

[11] Un'email o un SMS di phishing (nel caso dei messaggi di testo si parla di SMiShing) è un messaggio fraudolento creato in modo da sembrare autentico, che in genere richiede di fornire informazioni personali sensibili in vari modi.

pubbliche sono trasparenti e immutabili, il che significa che tutte le transazioni registrate sulla blockchain sono permanenti e non possono essere modificate o eliminate. Gli esempi più noti sono le blockchain di Bitcoin ed Ethereum.

- *permissioned;* le blockchain private sono utilizzate da organizzazioni o gruppi ristretti di partecipanti. Le transazioni vengono verificate e registrate da un gruppo selezionato di nodi che hanno l'autorizzazione per accedere alla blockchain. Le blockchain private sono meno trasparenti e possono essere gestite in modo centralizzato.

A loro volta quest'ultime si suddividono in:

- *permissioned privata* (la possibilità di leggere il registro e l'invio di transazioni è soggetta ad autorizzazione);

- *permissioned pubblica* (tutti i nodi possono leggere dati e sottoporre transazioni).

Alcuni esempi di blockchain private sono:

- *Chain*, che appartiene ad una società tecnologica che collabora con diverse organizzazioni per creare blockchain private;

- *Multichain* , che è una piattaforma aperta per la creazione di nuove blockchain, R3, Hyperledge ecc…

1.6 LA FUNZIONE DEI FORK

Nel contesto delle blockchain con il termine "fork" si intende una situazione in cui la cronologia delle transazioni registrate sulla catena di blocchi si divide in due o più diramazioni separate. Questo può accadere quando gli utenti della blockchain non sono d'accordo sulla direzione futura della rete e decidono di apportare delle modifiche al software che gestisce la blockchain.

Ci sono due tipi di fork:

- *hard fork*

  Un "hard fork" comporta la creazione di una nuova blockchain separata dalla blockchain originale, con regole e protocolli di consenso differenti. Ciò significa che tutti i nodi della vecchia blockchain devono aggiornare il loro software per supportare la nuova versione della blockchain, altrimenti verranno esclusi dalla nuova rete. In pratica, ciò significa che gli utenti della vecchia blockchain dovranno adottare la nuova blockchain, o rimanere sulla vecchia blockchain che potrebbe diventare obsoleta;

- *soft fork*

  Un "soft fork", implica una modifica al protocollo della blockchain che è retrocompatibile con la versione precedente del software, il che significa che i nodi della vecchia versione della blockchain possono ancora comunicare con i nodi della nuova versione. Ciò significa che gli utenti non sono costretti ad aggiornare il loro software, ma solo quelli che adottano la nuova versione del software potranno beneficiare delle nuove funzionalità e degli aggiornamenti del protocollo.

Per capire come funziona un fork, prendiamo ad esempio il fork di Bitcoin

Si chiama Bitcoin Cash ed è nato nel 2017, mentre Bitcoin nasce tra il 2008 ed il 2009.

Uno dei principali problemi di Bitcoin è la scalabilità, nonostante essa rimane la criptovaluta più preziosa ed affidabile che ci sia sul mercato.

La scalabilità in Bitcoin si riferisce alla capacità del sistema Bitcoin di gestire un aumento del numero di transazioni in modo efficiente e affidabile. In altre parole, la scalabilità si riferisce alla capacità di elaborare un numero crescente di transazioni senza che ciò comporti un aumento dei tempi di elaborazione delle transazioni o un aumento dei costi.

Poiché Bitcoin utilizza un registro contabile pubblico (la blockchain) per registrare tutte le transazioni, il numero di transazioni che il sistema può gestire è limitato dalla dimensione massima dei blocchi della blockchain.

In origine, la dimensione massima dei blocchi di Bitcoin era di 1 MB, il che significa che il sistema era in grado di elaborare solo un certo numero di transazioni per blocco.

Nel 2017 si era arrivati ad attendere anche diversi giorni per la conferma di una transazione e questo era un grave problema, visto che bitcoin nasce con l'obiettivo di effettuare dei pagamenti.

Il primo tentativo di risolvere il problema fu l'adozione del protocollo SegWit2x[12] che tra le altre migliorie, aumentò la grandezza dei blocchi da 1MB a 2MB e venne approvato ai voti dal 95% dei miner.

Nonostante i miglioramenti, il problema non si risolse e per questo motivo si ricorse ad un altro protocollo, Bitcoin Cash, che avrebbe portato i blocchi da 2MB a 8MB.

Questa modifica così radicale richiese però una separazione dalla rete originale e quindi l'adozione di un hard fork, dunque, una separazione con la catena dei blocchi precedente.

[12] SegWit2x (Segregated Witness) il termine si riferisce a un cambiamento (soft fork) avvenuto nel formato delle transazioni di Bitcoin. Scopo del miglioramento era risolvere il problema della malleabilità (in senso crittografico) e aumentare la capienza dei blocchi. Definizione estratta da COMANDINI G., *Da Zero alla Luna. La Blockchain: quando, come, perché sta cambiando il mondo*, Palermo, DarioFlaccovioEditore, marzo 2022, n. 214.

Le conseguenze di un hard fork sono l'aumento di valore della criptovaluta nella fase che precede la separazione, in quanto il possessore di quella criptovaluta prima del fork dopo si ritroverà la stessa quantità della nuova criptovaluta "forkata", senza aver speso denaro. Quindi, se prima del fork si avevano 10BTC, dopo il fork si avranno 10BTC+10BCH(Bitcoin Cash) senza aver investito ulteriore denaro, il che , come è facile immaginare, porta con se grossi interessi speculativi dietro a molti fork.

Subito dopo, però, inevitabilmente il prezzo della criptovaluta crolla, in quanto gli speculatori avranno interesse nella sua vendita rapida.

In ogni caso, un fork nella blockchain è una decisione importante che deve essere presa con cautela, poiché può influenzare significativamente la sicurezza, la stabilità e la direzione futura della rete. Tuttavia, i fork possono anche essere utili per risolvere problemi di scalabilità, migliorare le prestazioni e l'efficienza della blockchain, e introdurre nuove funzionalità.

CAPITOLO SECONDO

GLI SMART CONTACT: I CONTRATTI INTELLIGENTI

2.1 L'ORIGINE DEL FENOMENO

La progressiva affermazione ed il crescente utilizzo dei Distributed Ledger Technology[13], e in particolare della blockchain, hanno favorito l'approfondimento della disciplina e la parallela diffusione dei cosiddetti "smart contract".

Con l'espressione smart contract, letteralmente "contratti intelligenti", si fa oggi comunemente riferimento all'incorporazione del software di clausole contrattuali con esecuzione automatica ed indipendente dall'intervento di terzi.

Più propriamente con il termine smart contract si fa riferimento ad un processo negoziale giuridicamente vincolante in cui alcuni, o tutti i termini dello stesso, sono attestati o eseguiti automaticamente da un programma informatico su un registro distribuito.

Interessante la descrizione proposta nelle "Questioni di Economia e Finanza (Occasional Papers)" della Banca d'Italia per cui lo smart contract è un algoritmo che si caratterizza per la presenza di determinate caratteristiche:

1) un accordo che definisce una serie di promesse che si declinano in un insieme di clausole;

2) l'accordo è scritto in forma digitale, attraverso un programma o software che incorpora tali clausole;

3) l'accordo è formalizzato da un protocollo che stabilisce come le parti debbano processare le informazioni qualitative e quantitative del contratto, permettendo alle stesse di soddisfare i

[13] Database di operazioni distribuito su una rete di numerosi computer, anziché custodito presso un nodo centrale

termini concordati.

L'algoritmo prevede un insieme di regole o triggers (condizioni logiche e sequenze temporali) che modulano, in modo dinamico, l'esecuzione dell'accordo.

Si anticipa che la nozione giuridica di smart contract non può ritenersi ancora univocamente intesa, sia perché si tratta di un fenomeno relativamente nuovo, sia perché ricomprende una vasta gamma di ipotesi che, per varietà ed eterogeneità, difficilmente si prestano ad una trattazione unitaria, se non in termini generici.

Nel corso degli ultimi 25 anni, da quando l'informatico ungherese Nick Szabo ne ha coniato l'espressione, la stessa ha assunto accezioni sempre più articolate e contaminate dai settori all'interno dei quali si sono registrate le principali applicazioni.

Secondo Szabo "nel commercio elettronico, i criteri di progettazione per automatizzare l'esecuzione dei contratti sono venuti da campi disparati come l'economia e la crittografia, con poca comunicazione incrociata: poca consapevolezza della tecnologia, da un lato, e poca consapevolezza dei suoi migliori usi commerciali dall'altro. Questi sforzi sono alla ricerca di obiettivi comuni, e convergono proprio nel concetto di smart contract".

Modelli anticipatori degli odierni smart contract si possono anche rinvenire nei "contratti in forma informatica" come, per esempio, il sistema EDI (Electronic Data Interchanges) utilizzato già agli inizi degli anni '70 da alcune aziende per regolare automaticamente le forniture di materiali.

Ma a contribuire in modo rilevante alla informatizzazione dei contratti sono stati, indubbiamente, lo sviluppo dell'e-commerce e la diffusione di applicazioni informatiche per l'effettuazione di operazioni su un mercato finanziario.

Tuttavia, tali tipologie di accordo, possono essere considerati testi contrattuali tradizionali semplicemente trasposti in espressione informatica e la cui esecuzione dipende, in ogni caso, da un'azione aggiuntiva non automatizzata.

Se si vogliono però ricercare i veri predecessori degli attuali smart contract nel contesto DLT-blockchain, occorre far riferimento ai “Ricardian Contracts” introdotti nel 1995 dal programmatore Ian Grigg, ossia contratti espressi in forma di documenti digitali che fungono da accordo tra le parti su termini e condizioni previamente concordati tra le stesse. Si tratta di documenti legali unici leggibili, sia dalle macchine che dall'uomo.

Concludendo questa veloce disamina sulle origini degli smart contract, si può dire che la principale discriminante tra le forme di automatizzazione di accordi contrattuali e i contratti intelligenti come li ha concepiti Szabo, risiede nel fatto che, in questi ultimi, l'intera disciplina dell'accordo, compresa la sua esecuzione, è automatizzata, dunque, non solo non è necessario ma neppure possibile un intervento attivo ulteriore delle parti. Una volta, infatti, che le condizioni concordate si avverano, l'hardware ed il software si occupano dell'interpretazione ed esecuzione del contratto, senza che quest'ultima possa essere interrotta.

Tale meccanismo, inoltre, se attestato su una blockchain, non può più essere disatteso al verificarsi delle condizioni in esso previste e, una volta eseguito, la transazione che ne consegue diviene irrevocabile.

2.2 SMART CONTRACT NEL CONTESTO DELLA BLOCKCHAIN

Gli smart contract nascono molti anni prima della blockchain, ma è solo grazie a quest'ultima ed alle sue caratteristiche di fiducia e sicurezza che possono esprimere tutte le loro potenzialità.

In pratica, gli smart contract vengono scritti in un linguaggio di programmazione specifico e caricati sulla blockchain. Una volta immessi nella rete possono essere eseguiti in modo automatico ogni volta che vengono soddisfatte le condizioni stabilite al loro interno. Questo significa che le transazioni avvengono in modo automatico, sicuro e senza bisogno di intermediari, riducendo i costi e aumentando l'efficienza del processo.

In sintesi, gli smart contract e la blockchain lavorano insieme per creare un ambiente sicuro e decentralizzato in cui è possibile eseguire transazioni in modo automatico e senza intermediari.

È facile comprendere il ruolo fondamentale della blockchain in questo contesto: se il codice dello smart contract, le condizioni prestabilite del contratto ed i dati che determinano le conseguenti azioni non fossero immutabili e trasparenti, non ci si potrebbe fidare di questo strumento.

La svolta avviene nel 2014 con la pubblicazione del white paper di Ethereum, che divenne, in poco tempo, la piattaforma di riferimento per la diffusione degli smart contract su blockchain. consegue diviene irrevocabile.

2.3 ETHEREUM & SMART CONTRACT

Ethereum è una piattaforma decentralizzata, basata su blockchain, che consente lo sviluppo e l'esecuzione di applicazioni decentralizzate (dApps)[14] e smart contract.

[14] Dapps acronimo di "Decentralized Applications Apps", sono applicazioni informatiche operanti nel contesto di una blockchain decentralizzata.

In pratica funziona come una rete di computer interconnessi che utilizzano la stessa blockchain per archiviare e condividere informazioni. Ogni nodo della rete esegue una copia della blockchain e contribuisce alla validazione delle transazioni e alla sicurezza della rete.

Quindi Ethereum non mira a proporre un sistema alternativo di pagamento online, ma un "sistema operativo distribuito" con un linguaggio di programmazione chiamato Solidity[15] ed una Ethereum virtual Machine (EVM) che elabora i programmi software,gli smart contract.

La caratteristica distintiva di Ethereum rispetto ad altre blockchain è la sua capacità di eseguire un codice autonomamente attraverso gli smart contract.

Ciò significa che è possibile creare applicazioni decentralizzate, come giochi, mercati e applicazioni finanziarie, che eseguono automaticamente il codice scritto in un contratto intelligente.

Ethereum è stato progettato per essere altamente scalabile e flessibile, con la capacità di adattarsi a nuove esigenze e di essere aggiornato in modo regolare attraverso i cosiddetti hard fork.

La natura decentralizzata della piattaforma significa che qualsiasi modifica alla blockchain, deve essere approvata dalla maggioranza dei nodi della rete.

Ogni utente di Ethereum lavora su una rete peer to peer e può creare nuovi smart contract che verranno poi eseguiti sfruttando la forza computazionale della rete, la quale viene retribuita attraverso la criptovaluta Ether.

Invece, il costo delle transazioni su Ethereum è determinato dallo stato attuale della rete e dalla domanda di utilizzo della blockchain in un determinato momento.

Il costo delle transazioni viene espresso in "gas", un'unità di misura, che rappresenta l'energia computazionale necessaria per eseguire una particolare operazione sulla blockchain.

[15] Solidity è un linguaggio di programmazione Turing Complete ibrido che garantisce la programmabilità degli smart contract.

Il costo del gas può variare a seconda della congestione della rete e della priorità della transazione. Quando la rete è congestionata e ci sono molte transazioni in attesa di essere elaborate, il costo del gas aumenta. Viceversa, quando la rete è meno congestionata, il costo del gas tende a diminuire.

Quindi nell'eseguire le transazioni i miner devo attenersi scrupolosamente alle istruzioni date ai fini della buona riuscita dell'operazione.

Ad ogni istruzione che eseguono assegnano un costo in un'unità di gas.

Anche Ethereum come Bitcoin si serve di un processo di mining, il cui termine richiama il processo di estrazione dell'oro, per la creazione della criptovaluta che non potrà superare l'emissione annuale di 18 milioni di ether.

Il tempo necessario per la creazione di un nuovo blocco è di 12 secondi (a differenza del Bitcoin che è di 10 minuti) e per validare le transazioni e per produrre nuovi blocchi si serve di algoritmi informatici.

Dal 2022 è passata dalla Proof of Work alla Proof of Stake.

La Proof of Stake (PoS) è un algoritmo di consenso utilizzato dalle blockchain per validare le transazioni e creare nuovi blocchi nella catena. A differenza della Proof of Work (PoW), che richiede che i partecipanti alla rete risolvano complessi problemi crittografici per creare nuovi blocchi, la PoS seleziona in modo casuale un nodo all'interno della rete per creare un blocco sulla base della quantità di criptovaluta che detiene.

In pratica, la PoS funziona come una lotteria, in cui i nodi con maggiori quantità di criptovaluta hanno una maggiore probabilità di essere selezionati per creare un nuovo blocco e ricevere una ricompensa in cambio. In questo modo, la PoS incoraggia i partecipanti alla rete a "giocare" in modo onesto e ad accumulare maggiori quantità di criptovaluta per aumentare le loro possibilità di essere selezionati per la creazione dei blocchi.

Il soggetto (nodo) che viene scelto si chiama validator ed una volta completata l'operazione, con l'aggiunta del blocco alla catena, riceve una ricompensa determinata dalle fee delle

transazioni contenute in quel blocco. La PoS ha diversi vantaggi rispetto alla PoW, tra cui una maggiore efficienza energetica, in quanto non richiede l'utilizzo di risorse informatiche per risolvere complessi problemi matematici, e una maggiore sicurezza, in quanto rende più difficile un attacco del 51% contro la rete.

2.4 VERIFICA DELLE CONDIZIONI DELLO SMART CONTRACT ED IL RUOLO DEGLI ORACOLI

Uno dei caratteri distintivi degli smart contract è che questi, una volta caricati sulla blockchain con l'apposito linguaggio e verificatesi le condizioni poste dalle parti, entrano in esecuzione senza alcuna possibilità da parte degli utenti di interrompere o sospendere questo processo, a meno che questa possibilità non sia stata prevista ed inserita in origine dai suoi programmatori.

Può accadere, però, nelle sue molteplici applicazioni, che la verifica delle condizioni che attivano lo smart contract non sia sempre semplice.

Infatti, è possibile che le condizioni che attivino lo smart contract siano esterne alla blockchain. Ed è qui che entra in gioco la figura dell'oracolo.

Gli oracoli sono agenti esterni alla blockchain che forniscono informazioni e dati all'interno di uno smart contract. Essi agiscono come intermediari tra la blockchain e il mondo esterno, fornendo dati esterni che possono essere utilizzati dallo smart contract per prendere decisioni.

Ad esempio, uno smart contract che si occupa di scommesse su eventi sportivi, può utilizzare un'API fornita da un oracolo per ricevere i risultati dell'evento. In questo caso, l'oracolo funge da ponte tra la blockchain e il mondo esterno, fornendo dati affidabili che lo smart contract può utilizzare per verificare l'esito della scommessa.

Gli oracoli possono essere programmati per monitorare fonti di dati specifiche e fornire

informazioni in modo autonomo, oppure, possono essere gestiti manualmente da operatori umani che forniscono dati a richiesta. In ogni caso, gli oracoli sono fondamentali per consentire agli smart contract di interagire con il mondo esterno e di eseguire le loro funzioni in modo affidabile.

Tuttavia, è importante notare che gli oracoli presentano anche alcune sfide per la sicurezza degli smart contract.

Gli oracoli possono essere soggetti a manipolazione o attacchi informatici che potrebbero compromettere la sicurezza e l'affidabilità degli smart contract che dipendono da essi.

Inoltre, gli oracoli possono anche presentare problemi di latenza e di disponibilità. Se un oracolo non fornisce informazioni in modo tempestivo o non è disponibile, lo smart contract potrebbe non essere in grado di eseguire la sua funzione correttamente, il che potrebbe causare perdite finanziarie o altri problemi.

Per risolvere questi problemi, gli sviluppatori di smart contract spesso utilizzano più oracoli per ottenere dati da fonti multiple e quindi eseguire una verifica incrociata dei dati. In questo modo, se un oracolo non è disponibile o fornisce informazioni inaffidabili, gli smart contract possono ancora funzionare correttamente utilizzando dati da altre fonti.

In sintesi, gli oracoli sono imprescindibili per consentire agli smart contract di interagire con il mondo esterno, ma la loro sicurezza e affidabilità è fondamentale per garantire la sicurezza delle transazioni sulla blockchain.

Pertanto, la scelta di un oracolo affidabile e la progettazione di uno smart contract che gestisca correttamente le informazioni fornite dall'oracolo sono importanti per garantire la sicurezza degli smart contract.

Gli oracoli possono essere basati su :

- *Software*, quando l’oracolo trova le informazioni necessarie online o su altre blockchain.

- *Hardware*, gli oracoli basati su hardware possono funzionare in modo simile agli oracoli basati su software, ma con un livello aggiuntivo di sicurezza.

I dispositivi hardware possono essere progettati per essere resistenti alle intrusioni e possono utilizzare tecniche di crittografia avanzate per garantire la privacy e la sicurezza dei dati. Uno degli esempi più comuni di oracoli basati su hardware è rappresentato dai Trusted Execution Environments (TEE), che sono spazi sicuri all'interno di un processore in cui i dati sensibili possono essere elaborati in modo sicuro. I TEE possono essere utilizzati per eseguire i calcoli degli oracoli all'interno di un ambiente sicuro e poi fornire i risultati allo smart contract.

- *Intermediari umani*, gli oracoli intermediari umani sono un tipo di oracolo in cui una persona o un gruppo di persone viene utilizzato come fonte di informazioni per un contratto intelligente. In questo caso, invece di affidarsi a dati provenienti da una fonte di dati esterna o a dispositivi hardware, il contratto intelligente si basa su informazioni fornite da un oracolo umano.

Questi possono essere utilizzati in situazioni in cui i dati necessari per il contratto sono difficili da ottenere tramite mezzi automatizzati, o dove è richiesta una discrezionalità o un giudizio umano.

Ad esempio, un contratto che richiede una valutazione dell'idoneità di un richiedente per un prestito, potrebbe utilizzare un oracolo umano per eseguire tale valutazione. Gli oracoli intermediari umani possono offrire flessibilità e adattabilità alle esigenze del contratto intelligente, tuttavia ci sono anche alcune sfide. Ad esempio, l'affidabilità e l'obiettività dell'oracolo umano possono essere difficili da garantire, in quanto possono essere influenzate da fattori come la conoscenza e l'esperienza dell'oracolo, la sua oggettività e la sua etica professionale. Inoltre, l'uso di oracoli intermediari umani può aumentare i costi e il tempo necessario per eseguire il contratto.

Un impulso importante al problema della veridicità dei dati "esterni" è stato dato con l'avvento di Chainlink.

Chainlink è stato creato nel 2017 da un team di sviluppatori guidati da Sergey Nazarov e Steve Ellis. La piattaforma utilizza una criptovaluta chiamata LINK per incentivare i nodi oracolari a fornire dati accurati e affidabili.

Una delle principali caratteristiche di Chainlink è la sua flessibilità e la sua capacità di connettersi a una vasta gamma di fonti di dati. Ciò include dati finanziari, di mercato e di trading, ma anche dati meteorologici, di traffico e di eventi sportivi.

Chainlink ha già integrato la sua piattaforma con diverse blockchain, tra cui Ethereum, Polkadot e Binance Smart Chain, e sta lavorando per espandere la sua presenza su altre blockchain.

L'utilizzo di Chainlink ha il potenziale di risolvere alcune delle sfide che i contratti intelligenti hanno incontrato finora, in particolare, l'accesso a dati affidabili e verificabili da fonti esterne.

Ciò apre la strada a nuove applicazioni decentralizzate, che possono utilizzare dati esterni in modo sicuro e affidabile, aprendo nuove opportunità per l'adozione della tecnologia blockchain.

2.5 CONCLUSIONI SUGLI SMART CONTRACT

In conclusione, prima di addentrarci nel prossimo capitolo sui profili giuridici degli smart contract, cerchiamo di analizzare sinteticamente gli elementi che li caratterizzano in rapporto ai contratti tradizionali.

I contratti tradizionali e gli smart contract sono entrambi strumenti legali utilizzati per definire e regolare accordi tra le parti, ma differiscono in diversi aspetti chiave.

In primo luogo, mentre i contratti tradizionali sono spesso scritti in linguaggio naturale e richiedono la presenza di un intermediario (ad esempio un notaio o un avvocato) per verificare e far rispettare le condizioni dell'accordo, i contratti intelligenti sono programmati in linguaggio di programmazione e sono auto eseguibili.

In altre parole, i contratti intelligenti sono eseguiti automaticamente sulla blockchain, in modo che le condizioni dell'accordo vengano rispettate automaticamente senza la necessità di un intermediario.

Inoltre, mentre i contratti tradizionali possono richiedere diversi giorni o settimane per essere finalizzati, i contratti intelligenti possono essere eseguiti istantaneamente, poiché tutte le informazioni pertinenti sono già memorizzate sulla blockchain.

I contratti intelligenti offrono anche un maggiore livello di trasparenza e immutabilità rispetto ai contratti tradizionali, poiché tutte le informazioni relative all'accordo sono registrate sulla blockchain e non possono essere modificate senza il consenso delle parti coinvolte.

Infine, i contratti intelligenti possono ridurre i costi e l'inefficienza associati ai processi tradizionali di elaborazione dei contratti, poiché sono auto eseguibili e non richiedono la presenza di intermediari o il pagamento di commissioni per la gestione del processo.

CAPITOLO TERZO

PROFILI GIURIDICI

3.1 OSSERVAZIONI INTRODUTTIVE

Nel seguente capitolo cercherò di fare chiarezza sulle recenti riforme, nazionali ed internazionali, incentrate sulla blockchain e gli smart contract.

L'introduzione di una nuova tecnologia mette sempre il legislatore nelle condizioni di porsi delle domande su quale possa essere l'approccio più corretto per disciplinarla.

Infatti, da una parte c'è sempre la preoccupazione che il nuovo fenomeno possa consentire di svolgere nuove attività che la legge corrente non permette;

dall'altra invece bisogna valutare e comprendere la portata innovativa di queste nuove tecnologie che potrebbero portare ad una crescita sia economica sia di ottimizzazione dei processi e, pertanto, cercare di incentivarle anziché "soffocarle" e limitarle con un irrigidimento normativo che potrebbe rivelarsi un freno all'introduzione di eventuali benefici che queste novità potrebbero apportare.

Con riguardo alla blockchain, bisogna tener conto delle sue specificità e delle diverse relazioni giuridiche che potrebbero instaurarsi considerando il loro duplice aspetto, pubblico e privato.

Infatti, per le *blockchain permissionless* (pubbliche) il codice sorgente è open source e la catena di blocchi si modifica autonomamente.

Nelle *blockchain permissioned* (private), invece, il codice non è open source ma insieme al database è di proprietà del suo autore.

Tuttavia, la tecnologia blockchain solleva anche alcune questioni giuridiche e regolamentari.

In primo luogo, la decentralizzazione e l'anonimato della blockchain possono rendere difficile l'individuazione di responsabili in caso di attività illecite.

Inoltre, l'uso di criptovalute e ICO[16] potrebbe essere soggetto a regolamentazioni finanziarie e tributarie.

Infine, la blockchain potrebbe avere implicazioni per la protezione dei dati personali e la privacy. A tal proposito, un aspetto fondamentale da trattare è la privacy dei dati e la sicurezza delle transazioni, diventate una grande preoccupazione per le persone e le imprese che utilizzano blockchain.

Di conseguenza, ci sono stati sviluppi nella tecnologia della crittografia e dell'anonimizzazione dei dati per proteggere le informazioni sensibili.

Per affrontare queste questioni, molti paesi stanno cercando di sviluppare una legislazione che si adatti alla blockchain e alle tecnologie correlate.

In sintesi, le riforme su blockchain e smart contract stanno cercando di creare un ambiente normativo più chiaro e sicuro, di promuovere l'interoperabilità tra le diverse reti blockchain e di migliorare la privacy e la sicurezza delle transazioni.

3.2 QUADRO GIURIDICO DELLA BLOCKCHAIN

Come anticipato, nell'analisi che ci accingiamo a compiere dobbiamo tenere in considerazioni le due tipologie di blockchain: quella pubblica e quella privata.

Pur tenendo in grande considerazione le blockchain private, di solito, quelle che vengono prese da riferimento per le loro caratteristiche peculiari, tali da creare una rottura col passato, sono quelle pubbliche.

[16] ICO acronimo di "Initial Coin Offering", il termine si riferisce a un metodo di raccolta fondi per un'azienda, un ente o un progetto che preveda la cessione di token o altri asset digitali in cambio di denaro fiat o altre criptovalute. In molti casi, l'investitore partecipa a una ICO per ottenere un profitto sull'eventuale futura vendita a un prezzo maggiorato dei token (o degli altri asset digitali) ottenuti.

Infatti, la blockchain pubblica è un registro distribuito e immutabile, il che significa che le transazioni registrate sulla blockchain sono quasi impossibili da modificare o cancellare.

Ciò rende le parti coinvolte in una transazione responsabili per le loro azioni, poiché ogni transazione è permanentemente registrata e tracciabile.

In secondo luogo, la blockchain pubblica utilizza un sistema decentralizzato di consenso per validare le transazioni, eliminando la necessità di intermediari di fiducia come le banche. Ciò significa che le parti coinvolte in una transazione sono responsabili per il mantenimento dell'integrità del sistema, poiché non ci sono intermediari a cui affidarsi.

Infine, la blockchain pubblica utilizza la crittografia per garantire la sicurezza e la privacy delle transazioni. Ciò significa che le parti coinvolte in una transazione sono responsabili per la gestione delle loro chiavi private, poiché queste chiavi sono l'unica cosa che gli garantisce l'accesso ai loro fondi sulla blockchain.

In sintesi, la blockchain pubblica cambia il paradigma della responsabilità spostando la responsabilità dalle autorità centralizzate a tutti i partecipanti del sistema distribuito.

Ciò garantisce che ogni parte[17] sia responsabile delle proprie azioni e che il sistema sia affidabile, sicuro e trasparente per tutti i partecipanti.

Tuttavia, ci sono anche sfide e rischi associati all'adozione della blockchain pubblica, tra cui la gestione della privacy, la sicurezza e la scalabilità del sistema.

Parte di queste problematiche ed incertezze giuridiche su chi attribuire la responsabilità di eventuali malfunzionamenti o errori, vengono meno in caso di blockchain permissioned (private).

Infatti, nelle blockchain private le responsabilità giuridiche sono generalmente meno problematiche rispetto alle blockchain pubbliche, poiché le private sono gestite da entità centralizzate e regolate da accordi contrattuali.

[17] Parte, le parti a cui ci riferiamo sono: gli utenti, i nodi ed i miners.

Ciò significa che le responsabilità delle parti coinvolte nella rete possono essere definite in modo più chiaro e preciso rispetto alle blockchain pubbliche.

Tuttavia, ci sono comunque alcune questioni giuridiche che potrebbero sorgere, come la questione della conformità normativa, poiché le normative applicabili possono variare a seconda del settore in cui viene utilizzata la blockchain e del paese in cui le parti coinvolte nella rete operano.

In generale, sebbene le blockchain private possano presentare meno dubbi sulle responsabilità giuridiche rispetto alle blockchain pubbliche, ci sono ancora alcune sfide che devono essere affrontate per garantire la conformità normativa e definire in modo chiaro le responsabilità delle parti coinvolte nella rete.

Su questa nuova tecnologia si è esposta anche l'ESMA[18] che ha espresso una posizione favorevole alla blockchain e alle tecnologie distribuite in generale, riconoscendo il loro potenziale di trasformare il settore finanziario e migliorare l'efficienza, la trasparenza e la sicurezza delle transazioni finanziarie.

Proprio in virtù del grande potenziale rilevato, ritiene controproducente assoggettare fin da subito ad una disciplina le applicazioni delle blockchain per evitare di limitarne o arrestarne il processo evolutivo e che dunque, bisognerebbe applicare la normativa generale che salvaguarda il buon funzionamento del mercato[19].

Per questo motivo, l'ESMA ha invitato gli operatori del mercato a considerare attentamente i rischi e le opportunità della blockchain e ad adottare un approccio collaborativo e regolamentare per affrontare le sfide e massimizzare i vantaggi della tecnologia.

Nonostante ciò, gli stati nazionali hanno percorso un'altra strada e con una serie di interventi normativi hanno cercato di disciplinare alcune applicazioni di questa nuova tecnologia.

[18] L'ESMA è l'autorità europea degli strumenti finanziari e dei mercati.

[19] Disciplina del buon funzionamento del mercato, inteso come una serie di norme nazionali poste a tutela della concorrenza, pubblicità, sicurezza dei prodotti, protezione dei dati, etichettatura dei prodotti, trasparenza dei prezzi ecc…

3.3 BLOCKCHAIN E PROTEZIONE DEI DATI PERSONALI

Come preannunciato nell'introduzione, un argomento di cui moltissimi autori si sono occupati è il rapporto tra la tecnologia blockchain e la normativa in materia di protezione dei dati personali.

Il testo normativo a cui facciamo riferimento è il Regolamento (UE)2016/679 sulla protezione dei dati personali[20], approvato il 14 aprile 2016 dal Parlamento europeo ed oggi in vigore in tutti gli stati membri dell'Unione (senza necessità di leggi nazionali di recepimento) dal 25 maggio 2018.

Il Regolamento, meglio conosciuto come GDPR[21], ha il fine sia di rafforzare la protezione dei dati personali[22], sia di render la disciplina omogenea tra i cittadini residenti in UE, superando le legislazioni dei singoli stati membri che avevano recepito nei rispettivi stati in modo disomogeneo la precedente direttiva 95/46/CE.

I principi cardine della tecnologia blockchain, come abbiamo visto in precedenza, sono la trasparenza, l'immutabilità e la decentralizzazione, e la visione del GDPR, che si basa su un sistema di intermediari centralizzati, i c.d. titolari e responsabili del trattamento, si scontra con queste caratteristiche innovative.

I lavori preparatori del GDPR sono iniziati alcuni anni prima, già nel 2012, quando ancora la tecnologia blockchain non era molto conosciuta.

[20] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio dal 27 aprile 2016 relativo alla protezione dei dati delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46CE Regolamento europeo sulla protezione dei dati.

[21] GDPR, acronimo di "General Data Protection Officer", esso è relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

[22] Dati personali, l'art 4 del GDPR definisce dati personali "qualsiasi informazione riguardante una persona fisica identificata o identificabile".

Pertanto, il sistema "centrico" prospettato con al centro la figura di un ente capace di determinare finalità e strumenti del trattamento nonché capace di identificare e monitorare i responsabili è la logica conseguenza del contesto storico in cui nasce.

Dunque, un primo punto di discussione è capire come la disciplina contenuta nel GDPR possa effettivamente esser applicata a questa tecnologia.

Lo stesso Parlamento Europeo espressamente sottolineava "*che è della massima importanza che gli usi della DLT siano conformi alla legislazione dell'UE sulla protezione dei dati ,in particolare al regolamento generale sulla protezione dei dati (GDPR); invita la Commissione e il Garante europeo della protezione dei dati (GEPD) a fornire ulteriori orientamenti su questo punto*"[23].

Da ciò si evince che, vista la natura decentralizzata delle più importanti blockchain pubbliche (Bitcoin ed Ethereum) impedirne il loro utilizzo, e quindi bloccare questo processo tecnologico che può portare grandi benefici all'attività degli utenti, non sembra essere la soluzione ottimale.

Il GDPR in linea di massima è astrattamente applicabile alla tecnologia blockchain, in questo senso non ci sono divieti assoluti, ma i soggetti che l'utilizzano devono porsi il problema su come adattare la disciplina alle peculiarità di questa tecnologia.

Il GDPR riconosce agli utenti una serie di diritti nei confronti del "titolare del trattamento[24]:

- Diritti di natura informativa[25], art. 12,13 e 14, su come vengono usati i propri dati personali e sull' accesso agli stessi (art.15);

- Diritto alla rettifica art.16;

[23] Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772(RSP)),P8_TA-PROV(2018)0373).

[24] Titolare del trattamento, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento (art 3,numero 7 , del GDPR).

[25] Diritti di natura informativa, origine e categorie dei dati trattati, destinatari degli stessi, finalità del trattamento, periodo di conservazione, esistenza di un processo decisionale automatizzato, compresa la profilazione ecc…

- Diritto alla cancellazione dei propri dati art.17;

- Diritto alla limitazione del trattamento art. 18;

- Diritto alla portabilità art.20;

- Diritto di opposizione al trattamento in determinate circostanze art.21.

In un sistema " centralizzato" questi diritti possono essere esercitati rivolgendosi al titolare del trattamento.

In un sistema "decentralizzato" e "distribuito" manca questa figura e quindi bisogna capire chi svolgerà le sue funzioni e se e come questi diritti verranno tutelati.

Si riscontrano varie problematiche:

1) come esercitare il diritto alla cancellazione dei propri dati, art.17, vista la caratteristica dell'immutabilità della blockchain;

2) il principio della "minimizzazione dei dati" prevede che i dati vengano utilizzati solo nei limiti dello scopo per il quale sono raccolti, ma una volta immessi nella blockchain questi sono registrati su ogni nodo della rete, che è pubblica ed accessibile a tutti;

3) il principio della limitazione della conservazione dei dati, che prevede che i dati vengano conservati in modo tale che, per un periodo limitato di tempo non superiore al conseguimento delle finalità, sia possibile l'identificazione degli interessati;

Ulteriori strumenti che saranno utili per l'esame della compatibilità della blockchain con la normativa corrente, possono essere le osservazioni espresse dall'EU Blockchain Observatory and Forum[26] e dal servizio di ricerca del Parlamento europeo.

[26] EU Blockchain Observatory and Forum è un'iniziativa dell'Unione Europea volta a sostenere l'innovazione della tecnologia blockchain e facilitare la condivisione di conoscenze e buone pratiche tra gli stakeholder dell'ecosistema blockchain. L'Osservatorio è stato lanciato nel 2018 e viene gestito dalla Commissione Europea. La sua missione è accelerare lo sviluppo della tecnologia blockchain in Europa.

Il primo tema da analizzare riguarda l'ambito di applicazione territoriale del GDPR.

L'art. 3 del Regolamento prevede che questo si applichi quando il trattamento è posto in essere "*nel contesto delle attività di uno stabilimento di un responsabile o di un incaricato del trattamento nell'Unione, indipendentemente dal fatto che il trattamento avvenga o meno nell'Unione*" e quando i dati personali oggetto del trattamento si riferiscano ad interessati che si trovano nell'UE, anche se il titolare del trattamento non è stabilito nell'UE, purché abbia ad oggetto l'offerta di beni o servizi o sia rivolto al monitoraggio del comportamento degli interessati.

Da ciò si evince che il titolare del trattamento, sia che sia stabilito all'interno dell'UE e tratti dati personali attraverso la blockchain, sia che si trovi all'estero e tratti dati personali con riguardo l'offerta di beni/servizi o per monitorare comportamenti, sempre attraverso blockchain, in entrambi i casi trova applicazione la disciplina del Regolamento.

Bisogna anche verificare se la registrazione dei dati su blockchain rientri nella definizione di "trattamento" come è intesa dall'art.2 del Regolamento.

La risposta è affermativa in virtù dell'ampia concezione di trattamento dei dati contenuta nel suddetto articolo.

Un caso particolare invece riguarda l'art. 2, paragrafo 2, lettera c, che afferma che la normativa non si applica quando la registrazione dei dati sulla blockchain non avviene nel contesto di un'attività commerciale o professionale, ma solo a scopo personale nell'ambito "di un'attività puramente personale o domestica", come può essere ad esempio l'utente che compra e vende Bitcoin per conto proprio.

Ulteriore questione è quella di stabilire se i dati immessi su blockchain debbano essere considerati o meno nella categoria di dati personali, e nel caso, se sono dati anonimizzati o pseudonimizzati.

Nel Regolamento è ritenuto "dato personale" tutto ciò che si riferisce a persona identificata o identificabile.

Anche i dati pseudonimizzati rientrano in questa categoria, perché la "pseudonimizzazione" viene vista come una modalità di trattamento dei dati, per cui questi vengono condotti alla persona interessata solo con l'aiuto di ulteriori informazioni.

A questa conclusione è giunto il Gruppo di lavoro dell'art.29 secondo cui la pseudonimizzazione non è un metodo di anonimizzazione "*essa si limita a ridurre la collegabilità di una serie di dati con l'identità originale di una persona interessata ed è una misura di sicurezza utile*".

Nel contesto della blockchain la coppia di chiavi pubbliche deve essere considerata un dato personale perché cela l'identità dell'individuo in quanto, con l'aggiunta di ulteriori informazioni come un nome, un indirizzo o altro, è possibile risalire all'identificazione di un soggetto.

In considerazione di ciò, molti illustri autori che hanno esaminato la questione, come Sarzana-Nicotra ,Gambino-Bomprezzi, ritengono che le chiavi pubbliche debbano essere trattate alla stregua di dati personali ai sensi della normativa vigente, anche se sono dati pseudonimizzati.

Altra tipologia di dati oggetto di studio sono i "dati transazionali" che si riferiscono alla transazione e l'orientamento comune è quello di analizzarli caso per caso per capire se possono essere qualificati come dati personali.

A seconda dell'uso specifico della blockchain può accadere che, anche per ragioni di economicità, non tutti i dati necessitino della registrazione su blockchain e possano essere memorizzati su un database "off-chain", collegato alla blockchain attraverso un hash.

Questa potrebbe essere una soluzione al problema della conformità della disciplina del GDPR con applicazione sulla blockchain, poichè memorizzando i dati off chain, questo permetterebbe di effettuare operazioni di rettifica e cancellazione dei dati personali,

venendo, quindi, incontro ai diritti riconosciuti dagli artt. 16 e 17 del GDPR.

Quindi, anche se attraverso questo metodo si potrebbero risolvere alcune problematiche di compatibilità con la normativa, resta ancora irrisolto un aspetto fondamentale che riguarda l'individuazione del titolare, che, secondo la normativa è colui che decide i mezzi e gli scopi del trattamento.

Come accennato in precedenza, assume notevole rilievo la differenza tra blockchain pubbliche e private.

Infatti, in quelle "chiuse" è facile individuare i ruoli dei vari soggetti che partecipano al network, i quali assumeranno il ruolo di co-titolari del trattamento, potendo anche stipulare contratti ad hoc circa le ripartizioni delle responsabilità come previsto dall'art.26 del Regolamento.

Nelle pubbliche invece, tutto è molto più complesso sia per la diversità di ruoli, che per le varie tipologie di soggetti che vi partecipano.

Procediamo dunque ad analizzare i soggetti che interagiscono con la piattaforma per comprenderne il loro inquadramento.

Uno studio approfondito è stato condotto dalla CNIL[27], autorità francese per la protezione dei dati, pubblicando nel Settembre 2018 una Guida intitolata "Blockchain.

Premiers elements d'analyse de CNIL[28]" in cui analizzava i ruoli dei vari soggetti che ruotano attorno alla blockchain al fine di individuarne il titolare del trattamento.

I soggetti sono:

- *Sviluppatori di software*: loro sviluppano il software e non decidono se gli eventuali aggiornamenti verranno poi adottati. Difficilmente sono loro i titolari del trattamento, visto il ruolo marginale che ricoprono, fornendo soltanto ad altri un'infrastruttura per realizzare le

[27] CNIL acronimo di "Commission Nationale de l'informatique et des Libertes".

[28] Blockchain.Premiers elements d'analyse de CNIL al link :https//www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

finalità.

- *Miners*: sono coloro che raggruppano le transazioni in nuovi blocchi, eseguono il software e possono aggiungere dati alla blockchain. Anche loro non possono essere qualificati come controllori non determinando gli scopi di una transazione e limitandosi semplicemente a convalidare quelle presentate dai partecipanti.

- *Nodi*: sono i computer che memorizzano il registro e verificano la correttezza dei calcoli del meccanismo del consenso ed anche se le transazioni hanno le firme digitali e tutti gli altri dati corretti. Visto il loro ruolo prioritario è possibile considerarli come titolari o co-titolari del trattamento.

- *Utenti*: sono coloro che usano la blockchain ed inviano transazioni. Per il CNIL, che li chiama "partecipanti", sono loro che determinano le decisioni sulle finalità e sui mezzi impiegati nel trattamento.
Nella Guida si fa l'esempio di un notaio che scrive un rogito sulla blockchain e di una banca che vi scrive i dati dei suoi clienti: sono loro ad essere i Titolari del trattamento.

Infine, sottolinea che non sono Titolari del trattamento coloro che inseriscono nella blockchain dati a fini esclusivamente personali, come ad esempio chi compra e vende criptovalute per conto proprio, mentre lo sono coloro che vendono per conto di propri clienti, questo è il caso degli exchanger.
Quindi, in base agli studi effettuati, si può concludere che gli utenti siano i contitolari del trattamento e che, ai sensi dell'art 82,paragrafo 4 del GDPR, "*ciascun responsabile del trattamento congiunto è ritenuto responsabile dell'intero danno al fine di garantire l'effettivo risarcimento dell'interessato*", sebbene poi possa richiedere la restituzione di parte

dei fondi agli altri responsabili del trattamento ai sensi dell'art 82 , paragrafo 5 del GDPR.

È innegabile quindi che, seppur con difficoltà, questa disciplina possa essere adattata alla nuova tecnologia, anche se le norme contenute nel Regolamento sono concepite per tecnologie molto diverse dalla blockchain.

Il problema, invece, che riguarda l'art.17, il diritto all'oblio, ad oggi non ha trovato una soluzione soddisfacente.

La soluzione avanzata da alcuni autori, come Finck, è condivisibile e potrebbe ritenersi corretta per quanto concerne i dati eventualmente conservati off-chain, con la loro cancellazione logica, e quindi non fisica, rendendo questi dati non più accessibili al pubblico.

Per le blockchain pubbliche, invece, essendo i dati registrati onchain, non è possibile allo stato attuale della tecnologia procedere alla loro cancellazione se non tramite un fork a costi non sostenibili.

Dall'analisi svolta emerge dunque che il rapporto tra blockchain e regolamentazione in materia di protezione dei dati personali non è ancora molto chiaro.

C'è molta incertezza giuridica su come diversi elementi del Regolamento possano essere applicati a questa tecnologia e quindi non resta che sperare in un tempestivo intervento normativo, al fine di fornire una maggiore certezza del diritto.

3.4 LA STRATEGIA ITALIANA SULLA BLOCKCHAIN

La strategia italiana sulla blockchain è stata presentata nel marzo 2019 dal Ministero dello Sviluppo Economico (MISE)[29].

La strategia prevede l'adozione della tecnologia blockchain per promuovere l'innovazione e la competitività del Paese.

Tra le principali azioni previste dalla strategia italiana sulla blockchain, ci sono:

1. *Promuovere la ricerca e lo sviluppo*: il Governo italiano intende incentivare la ricerca e lo sviluppo nel settore della blockchain attraverso il finanziamento di progetti di ricerca, il supporto alle start-up e l'organizzazione di eventi di formazione.

2. *Sostenere l'adozione della tecnologia blockchain*: il Governo italiano vuole promuovere l'adozione della blockchain da parte delle aziende, delle pubbliche amministrazioni e delle istituzioni attraverso l'elaborazione di piani strategici e l'organizzazione di tavoli di lavoro.

3. *Migliorare la regolamentazione*: il Governo italiano intende migliorare la regolamentazione della blockchain e delle criptovalute per garantire la protezione dei consumatori e prevenire l'uso illegale della tecnologia.

4. *Favorire l'integrazione della blockchain con altre tecnologie*: il Governo italiano vuole promuovere l'integrazione della blockchain con altre tecnologie, come l'Internet delle Cose (IoT) e l'intelligenza artificiale (AI), per creare soluzioni innovative e sostenibili.

[29] MISE è l'acronimo del "Ministero dello Sviluppo Economico", un dicastero del governo italiano che si occupa di promuovere lo sviluppo economico del Paese, sostenere l'innovazione e la competitività delle imprese italiane, nonché di regolamentare e controllare i settori economici strategici.

5. *Migliorare la collaborazione internazionale*: il Governo italiano vuole collaborare con altri paesi e organizzazioni internazionali per promuovere l'uso della blockchain a livello globale.

È prevista anche l'istituzione di un osservatorio sulla blockchain, che ha il compito di monitorare lo sviluppo della tecnologia blockchain e promuoverne l'adozione in Italia. L'osservatorio è composto da rappresentanti del Governo, dell'industria e del mondo accademico.

Infine, la strategia italiana sulla blockchain prevede anche l'organizzazione di eventi e di iniziative di formazione per diffondere la conoscenza sulla tecnologia blockchain e promuoverne l'adozione a livello nazionale al fine di sfruttarne le potenzialità per l'innovazione e la competitività del Paese.

3.5 PROFILI GIURIDICI DEGLI SMART CONTRACT

Il diritto, e in particolare il diritto commerciale, è stato intensamente coinvolto nel processo di tecnologizzazione cui si assiste da anni, ma con grande difficoltà, trovandosi ad inseguire una realtà in rapidissima evoluzione, è riuscito nell'intento di qualificare e disciplinare fenomeni sconosciuti e non riconducibili agli schemi tradizionali.

Così l'analisi degli smart contract, in concomitanza con quella della blockchain, non poteva che alimentare un acceso dibattito tra legislatori ed interpreti che devono affrontare diversi aspetti giuridici, a partire dalla criticità terminologica della locuzione, alla configurabilità o meno di un ordinamento giuridico autonomo, alla riconducibilità degli stessi a categorie di diritto tradizionali fino alla applicabilità delle norme di diritto internazionale.

Un confronto aperto tra gli operatori del diritto è tuttora "la questione lessicale" e se sia giusto attribuire al termine "contract" il significato di contratto nel senso classico del termine o se tale termine si riferisce al solo aspetto funzionale, quale mezzo di espressione ed esecuzione di un accordo tra le parti. Tale ultimo orientamento muove le ragioni dall'assunto che lo smart contract non può essere assimilato ad un modello di regolazione di rapporti giuridici patrimoniali, in quanto non afferisce alla fase di formazione del contratto, costituita sempre dall'accordo fra le parti, ma alla sola fase dell'adempimento, con la conseguenza che non può per questo ravvisarsi neanche una fattispecie di contratto atipico.

Sarebbe, invece, più corretto inquadrare lo smart contract come strumento di esercizio dell'attività negoziale tra le parti.

Ma ancor prima della questione "lessicale" la dottrina si è interrogata sulla possibilità che il sistema degli smart contract trascritti in blockchain, potesse configurare un vero e proprio ordinamento autonomo. Partendo dal presupposto che gli smart contract assolvono, attraverso un meccanismo di tipo *"if this- then that"* [30], alla funzione di eseguire determinate azioni al verificarsi di specifiche condizioni senza l'ausilio di un intervento umano, la blockchain sarebbe così una tecnologia "regolatoria" in quanto le regole codificate all'interno del software di uno smart contract assurgerebbero al rango di regole normative, per la caratteristica intrinseca di essere automaticamente eseguite e non modificabili.

Dunque, la blockchain "può essere utilizzata sia per definire che per incorporare disposizioni legali o contrattuali nel codice e di farle rispettare indipendentemente dalla sussistenza di una regola legale sottostante"[31].

In questa prospettiva il sistema di smart contract, con regole proprie e modalità di esecuzione, potrebbe configurarsi come ordinamento autonomo perché ricorrerebbero gli elementi tipici di quest'ultimo:

30 . Secondo quanto ideato dal creatore della piattaforma Ethereum, la prima che ha consentito allo *smart contract* di funzionare sulla *blockchain*, V. BUTERN, *A Next – Generation Smart Contract and Decentralized Application Platform*, White Paper, 1, 2014.

31 . De Filippi - Hassan

- *plurisoggettività* (più soggetti utilizzano la blockchain);

- *normazione propria* (regole tecniche di utilizzo della stessa);

- *forza coercitiva* (automatica esecuzione degli stessi).

In questo modo le parti sarebbero tutelate ex ante ma non ex post, dovendo ricorrere agli strumenti già previsti dall'ordinamento statale su eventuali modifiche o momenti successivi all'esecuzione del contratto.

Pertanto, alla luce di queste considerazioni, il sistema smart contract non può essere considerato ordinamento giuridico autonomo poichè il meccanismo di esecuzione automatica è solo uno strumento per agevolare l'esecuzione del contratto in determinate ipotesi.

3.5.1 Il parallelismo con la disciplina contrattualistica tradizionale

Il dispositivo dell'art. 1321 Codice Civile, così recita:

" *Il contratto è l'accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale*".

Il contratto tradizionale prevede un'autonomia contrattuale che legittima le parti a concludere contratti diretti a perseguire interessi meritevoli di tutela secondo l'Ordinamento.

Tra gli elementi "essenziali" del contratto tradizionale c'è l'*accordo*, definito come l'incontro delle manifestazioni di volontà dei contraenti:

1) Quella di chi propone il contratto (Proposta);

2) Quella di chi accetta (Accettazione).

Proposta e accettazione rappresentano le fasi tipiche attraverso le quali si giunge alla conclusione del contratto.

Altro elemento essenziale è la *causa* o funzione economica-sociale del contratto (quale effetto si vuole produrre con il contratto), come ad esempio nella compravendita è il trasferimento di proprietà.

L'*oggetto* è altro elemento essenziale del contratto, ovvero è necessario individuare cosa ci si scambia.

Importante è anche la *forma,* intesa come mezzo con cui si manifesta la volontà (mediante parole, scritti...).

La *conclusione* prevede che il contratto è concluso nel momento in cui chi ha fatto la proposta ha conoscenza dell'accettazione dell'altra parte, tramite quindi l'incontro delle rispettive manifestazioni di volontà.

Dopo aver visto rapidamente gli elementi essenziali del contratto tradizionale, vediamo come lo smart contract si differenzia o si identifica con questi.

"*Secondo parte della dottrina, uno smart contract sarebbe composto da una parte informatica , la quale prende il nome di smart contract code e corrisponde al software e da una parte giuridica chiamata smart legal contract che corrisponderebbe ad un contratto dal punto di vista legale*".[32]

In riferimento all'*oggetto,* lo smart contract, **"***può classificarsi un contratto ad oggetto virtuale, mentre in riferimento alla forma, potrebbe essere inserito nella categoria dei contratti cibernetici, dove un agente software interferisce autonomamente nella fase della formazione del contratto*"[33]

"*Al contrario, nel caso degli smart contact che non utilizzano l'intelligenza artificiale, il grado di autonomia è sicuramente ridotto: per questo motivo essi potrebbero essere ritenuti una mera manifestazione della volontà delle parti contraenti*".[34]

[32] Mateja Durovic,Andrè Jassen,The formation of blockchain –based smart contracts in the light of contract law, in European Rewiew of Private Law(6-2019)

[33] Emilio Tosi, Contratti informatici, telematici e virtuali. Nuove forme e procedimenti formativi. Giuffrè Editore, Milano 2010.

[34] G. Rinaldi, Smart contract: meccanizzazione del contratto nel paradigma della blockchain, in G. Alpa (cur.), Diritto e intelligenza artificiale, Pisa 2020

Per quanto riguarda la conclusione, lo smart contract esegue in modo automatico quanto si è programmato. L'esecuzione automatica dello smart contract non bisogna confonderla con l'autonomia della conclusione.

Quando i due contraenti scelgono uno smart contract per regolare i propri interessi, semplicemente proiettano verso il futuro le loro aspettative, cioè quando lo smart contract sarà eseguito. Tali aspettative manifestate verranno successivamente trasportate in codice in sede di programmazione .

La proposta e l'accettazione che manifestano l'accordo delle parti è dichiarazione recettizia che produce effetti giuridici solo dal momento della sua ricezione, intesa come conoscibilità da parte del soggetto cui è destinata.

La conoscenza potrebbe realizzarsi nel momento in cui una delle parti attiva lo smart contract.

"*In poche parole, gli smart contract sono simili ai contratti tradizionali in quanto sono costituiti da clausole, ma si differenziano da questi ultimi in quanto caratterizzati dalla peculiarità di essere programmati elettronicamente e di essere inseriti su registri distribuiti. La registrazione dei contratti intelligenti permette infatti di attivare automaticamente le azioni ad esse riconnesse non appena si verificano le condizioni concordate, senza , peraltro, che le parti debbano porre in essere verifiche o attivare procedure cartacee o manuali*"[35].

Ad oggi, però, permangono diversi punti irrisolti che non permettono o rendono complessa l'estensione delle norme del contratto tradizione allo smart contract, che quindi ne necessita di proprie.

[35] Duilia Delfino –Smart Contract: un contratto ad << alta tensione>>
https://www.filodiritto.com/blockchain-e-smart-contract

Innanzitutto, un primo punto critico si rinviene sull'idoneità dello smart contract di rappresentare la volontà delle due parti, seppur non redatto dalle stesse ma da un terzo.

Nei contratti tradizionali, il tutto è superato attraverso la sottoscrizione che fa acquisire alle parti la paternalità del documento.

Nello smart contract, invece, non sono contemplate ad oggi forme di sottoscrizione; quindi, questa problematica potrebbe essere superata attraverso l'identificazione informatica delle parti interessate.

Pertanto, si richiamano gli artt. 20 e 21 del d.lgs. n. 82/2005 del CAD[36] che affermano "*un documento informatico soddisfa il requisito della forma scritta ed ha l'efficacia prevista dall'art 2702 c.c. quando vi è apposta una firma digitale o comunque è formato previa identificazione digitale del suo autore,con modalità che ne garantiscano la sicurezza,l'integrità e l'immodificabilità del documento*".

Per quanto riguarda la forma del contratto, lo smart contract è scritto in codice software e viene poi trascritto sulla blockchain in vista della sua esecuzione.

Altre criticità possono insorgere proprio in relazione all'interpretazione del contratto e ad eventuali errori nella trascrizione del codice sulla blockchain che potrebbero quindi stravolgerne il contenuto.

Secondo Nicotra-Sarzana in questi casi si ritiene applicabile la disciplina dell'annullabilità del contratto per errore , art. 1428-1433 c.c. in quanto lo smart contract è solo il risultato finale di un processo logico che avviene prima della scrittura dello stesso sulla blockchain.

Altra situazione delicata riguarda l'automatica esecuzione dello smart contract una volta trascritto sulla blockchain senza possibilità di esser revocato.

Secondo una prima visione sembrerebbe inapplicabile, viste le caratteristiche di immutabilità della blockchain, l'eccezione di inadempimento.

[36] CAD è l'acronimo di "*Codice dell'Amministrazione Digitale*", un insieme di norme e principi che disciplinano l'utilizzo delle tecnologie digitali nell'amministrazione pubblica italiana. Il CAD è stato introdotto nel 2005 e successivamente aggiornato nel 2017, con l'obiettivo di favorire l'efficienza, la trasparenza e la semplificazione dei processi amministrativi grazie all'utilizzo delle tecnologie digitali.

Però questo ostacolo può essere superato in alcune tipologie più evolute di blockchain che prevedono una funziona particolare, la c.d. "*kill*", la quale, attivabile soltanto da colui che ha trascritto lo smart contract su blockchain, permette l'autodistruzione dello stesso.

Ciò consente, in caso di inadempimento del contratto, alla parte adempiente di richiederne la cancellazione dalla blockchain dello smart contract.

Possiamo sin da subito notare la differenza con la disciplina tradizionale dei contratti, in quanto qui, per l'eventuale pronuncia giudiziale di risoluzione, annullabilità o nullità del contratto è necessario un "obbligo di facere" della parte che lo aveva generato.

Negli altri casi, invece, dove la blockchain non contempla la funzione di "*kill*", gli unici rimedi percorribili secondo Werbach-Cornell sono quelli restitutori, sia in forma specifica o per equivalente, della prestazione resa in precedenza.

Concludendo possiamo affermare che queste nuove tipologie contrattuali ,oltre a richiedere un intervento normativo , richiedono agli operatori del diritto una serie di nuove competenze in quanto avranno a che fare con aspetti tecnologici nuovi che andranno coniugati con le competenze tradizionali del giurista.

3.6 IL CONTESTO EUROPEO ED INTERNAZIONALE IN MATERIA DI SMART CONTRACT

L'approccio tradizionale basato sul diritto contrattuale potrebbe risultare inadeguato, poiché gli smart contract possono essere difficili da interpretare in base alle norme esistenti.

Per questo motivo, si sta sviluppando un nuovo approccio giuridico che tiene conto della natura tecnologica degli smart contract e che mira a fornire un quadro giuridico chiaro ed adeguato per le transazioni basate su questi strumenti.

Nonostante si tratti di un istituto non ancora completamente definito, tanto da limitarne al momento gli usi, tuttavia la ricerca "*tecnologica sta ampliando notevolmente l'operatività dello stesso, dall'ambito finanziario a quello assicurativo. Si stanno modificando i rapporti umani, divenuti oggi anche interconnessi grazie all'ausilio di Internet, e conseguentemente questa trasformazione colpisce anche il mondo del diritto, facendo sì che questi contratti siano impiegati tanto nell'ambito del commercio business to consumer che in quello dei rapporti business to business*"[37].

Per loro natura, hanno una vocazione transfrontaliera e pertanto è doveroso analizzare il coordinamento tra gli smart contract e le norme di diritto internazionale privato.

Intatti, potrebbero sorgere problemi se dovessero esserci delle controversie tra i contraenti di uno smart contract sulla legge applicabile e la giurisdizione competente.

Secondo alcune ricostruzioni compiute da illustri giuristi, tra i quali Ruhl, la disciplina compatibile, in attesa di una più specifica, è quella conosciuta come Regolamento Roma I, ovvero quella relativa al sistema europeo dal Regolamento (CE) n.593/2008 ove vi sia un accordo tra le parti concluso nel mondo virtuale tramite un software.

[37] Duilia Delfino –Smart Contract: un contratto ad << alta tensione>>
https://www.filodiritto.com/blockchain-e-smart-contract

Secondo il Regolamento, viene data priorità all'applicazione della legge scelta di comune accordo tra le parti, e la scelta deve risultare espressamente dalle disposizioni del contratto.

Tradurre questa scelta in linguaggio informatico non è sempre un'operazione agevole, pertanto, è possibile che emerga da un accordo separato fra le parti.

Se le parti non hanno effettuato alcuna scelta, allora la disciplina applicabile sarà quella che presenterà un collegamento più "stretto" in rapporto al contenuto della prestazione del contratto.

Altra questione rilevante è quella dell'individuazione del foro competente in caso di controversie relative all'esecuzione del contratto. In mancanza di un'apposita scelta dei contraenti che emerga dal contratto, le caratteristiche della blockchain "decentralizzata" e quindi "a-territoriale" rendono difficile l'estensione della disciplina del Regolamento UE n.1215/2012, essendo la blockchain una sorta di "non luogo".

Tra le ipotesi avanzate, quella più attinente con la natura dello smart contract sembra essere l'arbitrato, che risolverebbe il conflitto tra leggi di diversi Paesi.

Prima di addentrarci nello studio della disciplina italiana è molto importante delineare il quadro europeo ed internazionale che si è sviluppato attorno al tema smart contract.

Ciò che risulta subito evidente è il diverso approccio avuto dai giuristi di civil law rispetto a quelli di common law.

Nei paesi di civil law il tema è trattato in modo molto prudente, limitando in qualche modo la portata rivoluzionaria di questa nuova tecnologia, inquadrando lo smart contract semplicemente come uno strumento di esecuzione automatica del contratto.

I giuristi di common law invece vedono lo smart contract come un vero e proprio negozio giuridico, a patto che venga rispettato l'elemento della "consideration".

Infatti, parte della dottrina ritiene di riscontrare nello smart contract gli elementi essenziali del contratto tradizionale, quindi, lo scambio di promesse e obblighi è tale da produrre effetti tra le parti.

A conferma di questa tendenza sono stati elaborati molti documenti, tra cui lo *Uniform Commercial Code* (UCC)[38], il quale non richiedendo la forma scritta come condizione di validità del contratto, permette allo smart contract, col suo linguaggio informatico, di rientrare nella categoria dei contratti.

Altre conferme le abbiamo con *l'Uniform Eletronic Transaction Act* (UETA)[39] e nell'*Eletronic Signature in Global and National Commerce* (ESIGN)[40], che equiparano l'efficacia dei contratti elettronici a quelli in formato cartaceo.

Trovarono quindi, in questo contesto, terreno fertile le prime normative specifiche sulla blockchain da parte dei singoli Stati.

"*Nel 2018 il Tennessee, attraverso il Senate Bill N.1662, ha sancito la validità legale degli smart contract con la seguente motivazione: ' non è possibile negare efficacia giuridica a un contratto solo perché è eseguito tramite uno snart contract*" [41].

Anche lo Stato dell'Arizona con l'emendamento al Titolo 44, Capitolo 26 dell'Arizona Revised Statutes, equipara gli smart contract ai contratti tradizionali, aggiungendo nel nuovo art. 5 che "*smart contract may exist in commerce. A contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract terms*".

[38] UCC, acronimo di *Uniform Commercial Code (UCC)*, è un insieme di regole commerciali uniformi sviluppate negli Stati Uniti per standardizzare e semplificare le transazioni commerciali tra gli Stati. Il codice, che è stato adottato da tutti i 50 stati degli Stati Uniti, definisce le regole per le transazioni commerciali, tra cui vendite, garanzie, pagamenti e contratti.

[39] L'UETA, acronimo di *Uniform Electronic Transactions Act*, è una legge degli Stati Uniti che stabilisce regole uniformi per le transazioni commerciali elettroniche. La legge è stata introdotta nel 1999 e adottata da molti stati degli Stati Uniti.

[40] ESIGN, acronimo di *Electronic Signatures in Global and National Commerce Act,* è una legge federale degli Stati Uniti, adottata nel 2000, che riconosce l'efficacia giuridica delle firme digitali e delle transazioni commerciali elettroniche.

[41] Davide Calderone in Smart Contract:la situazione normativa in UE e Usa.
https://www.chainon.it/la-valenza-giuridica-degli-smart-contract/
Davide Calderone

Anche altri Stati seguono questo esempio, e così anche New York con la Senate Bill n.4142 del 1° marzo 2019 e il North Dakota con la House Bill n. 1045 del 24 Aprile del 2019.

Anche l'Unione Europea ha mostrato interesse verso lo sviluppo delle tecnologie blockchain e smart contract, destinando ad esse ingenti risorse economiche.

"Il Parlamento Europeo ha approvato una risoluzione denominata Blockchain Strategy per indirizzare l'operato della Commissione. L'obiettivo è quello di creare un quadro giuridico paneuropeo condiviso e che conferisca una certezza legale degli smart contract in tutti gli Stati europei. Le caratteristiche transazionali della blockchain, e quindi anche degli smart contract, necessitano di norme condivise per promuovere l'utilizzo di questi strumenti.

La risoluzione dichiara apertamente che il fine dell'operato della Commissione Europea dovrà essere quello di evitare la frammentazione del quadro normativo.

L'European Blockchain Services Institute (EBSI)[42], introdotto nel 2021, dovrà essere l'ente che, con consapevolezza tecnica e giuridica, avrà il compito di costruire una propria blockchain che connetta gli Stati, incentivando l'interpolarità tra gli attori business del Continente"[43].

In Europa solo Malta ha dato una definizione giuridica degli Smart contract, contenuta nel framework normativo approvato nel 2018 con *l'Innovative Tecnology Arrangements and Services Act* (ITAS)[44] che disciplina sia smart contract che le altre tecnologie che si basano sul registro distribuito.

[42] L'European Blockchain Services Infrastructure (EBSI) è un'iniziativa dell'Unione Europea che mira a fornire un'infrastruttura di servizi basata sulla tecnologia blockchain per la gestione di servizi pubblici transfrontalieri in modo sicuro e affidabile.

[43] Davide Calderone in Smart Contract:la situazione normativa in UE e Usa.
https://www.chainon.it/la-valenza-giuridica-degli-smart-contract/
Davide Calderone

[44] L'Innovative Technology Arrangements and Services Act (ITAS) è una legge maltese che mira a regolamentare l'uso delle tecnologie emergenti come la blockchain, l'intelligenza artificiale e l'Internet delle cose (IoT).

Negli altri Stati invece non si segnalano interventi legislativi, ma solo accesi dibattiti in dottrina. Nonostante ciò, sono diversi i documenti che devono essere tenuti in considerazione.

Cominciamo dalla Direttiva UE 2018/843-AML/CFT.

Questa Direttiva (UE) del Parlamento Europeo e del Consiglio del 30 maggio 2018, modifica la precedente Direttiva (UE)2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo. La Direttiva non disciplina direttamente l'utilizzo dello smart contract, ma fornisce una utile definizione di valuta virtuale e tratta gli obblighi dei soggetti che operano in ambito di cambio con valute legali.

Altro documento utile è il Regolamento (UE) n°910/2014 eIDAS (electronic Identification Autenticatio and Signature)[45].

Tale documento fornisce una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni ed è finalizzato ad incrementare la sicurezza e l'efficacia dei servizi elettronici nell'Unione Europea.

Fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato d'identificazione elettronica di un altro Stato membro; stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche; istituisce un quadro giuridico per le firme elettroniche, sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web.

Rispetto ai sistemi di identificazione elettronica, eIDAS prevede che ciascun Stato membro possa notificare i sistemi di identificazione elettronici forniti ai cittadini e alle aziende per consentire un reciproco riconoscimento.

[45] EIDAS è l'acronimo di "*Electronic Identification, Authentication and Trust Services*". EIDAS è un regolamento dell'Unione Europea (UE) adottato nel 2014, che stabilisce un quadro normativo per l'identificazione e l'autenticazione elettronica transfrontaliera e per i servizi di fiducia elettronici all'interno dell'UE.

Il Regolamento eIDAS svolge un ruolo importante nel contesto dello smart contract in quanto si sofferma sull'identificazione elettronica.

La volontà manifestata da una delle due parti contraenti deve essere riconducibile ad uno specifico soggetto, cioè ad una indicazione univoca che permetta di distinguere quella da qualsiasi altra. Pertanto, in mancanza di linee guida da parte dell'AGID[46], oggi si po' fare solo affidamento su tale Regolamento per l'identificazione elettronica.

Altro documento da tenere in considerazione è ovviamente il Regolamento(UE) 2016/679-GDPR (General DataProtetion Regulation), di cui abbiamo discusso ampiamente nel paragrafo precedente.

Anche se permangono interrogativi irrisolti, sono sempre più gli Stati in Europa che vogliono arrivare ad una soluzione e, pertanto, possiamo sperare in futuro in una normativa chiara per lo smart contract, che ad oggi ancora non esiste.

3.7 LA DISCIPLINA ITALIANA INTRODOTTA DALLA L. 12/2019, DI CONVERSIONE DEL D.L. 135/2018

Il legislatore italiano con la Legge dell'11 Febbraio 2019, n° 12 (Conversione in legge, con modificazioni, del decreto-legge 14 dicembre 2018, n.135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione) sulla scia della Risoluzione del Parlamento europeo del 3 ottobre 2018, ha voluto compiere un primo passo verso la disciplina in materia di "Tecnologie Distributed Ledger" (DLT) e di Smart Contract, tra i primi Paesi a farlo dopo Malta.

[46] L'AGID è l'acronimo di "Agenzia per l'Italia Digitale", un'agenzia governativa italiana istituita nel 2016 per promuovere la diffusione e lo sviluppo delle tecnologie digitali nell'amministrazione pubblica italiana e nella società in generale. L'AGID ha il compito di coordinare le politiche digitali del governo italiano e di promuovere l'accesso ai servizi pubblici digitali per tutti i cittadini e le imprese. Inoltre, l'AGID svolge anche attività di ricerca e sviluppo in materia di tecnologie digitali e si occupa della promozione dell'innovazione digitale nel settore privato.

Si tratta di un tentativo meritevole per volontà ma che contiene nel suo interno qualche contraddizione e qualche manchevolezza .

L'art. 8-ter, comma 2, qualifica lo smart contract come programma per elaboratore che opera su tecnologie DLT, che una volta attivato, vincola automaticamente le parti agli effetti che avevano precedentemente concordato.

Inoltre, aggiunge che lo smart contract soddisfa il requisito della forma scritta, a patto che avvenga l'identificazione informatica dei contraenti, secondo dei criteri fissati dall'Agenzia per l'Italia Digitale.

Uno degli aspetti innovativi portati da questa norma è senza dubbio quello di riconoscere a dei programmi per elaboratore, quali lo smart contract, che usano un proprio linguaggio, una piena valenza probatoria, a patto che però operino su tecnologie basate su registri distribuiti, le cui caratteristiche vengono definite al primo comma dell'art. 8 ter.

Viene fatta chiarezza anche sul termine "esecuzione" del contratto, che aveva destato incertezza in dottrina su quale fosse il significato da attribuirgli.

Ciò che destava incertezza è che molti associavano il termine esecuzione al fatto che lo smart contract, essendo un programma per elaboratore, veniva eseguito, azionato.

Mentre, altri, riconducevano il termine esecuzione alle obbligazioni e prestazioni oggetto del contratto.

Sono due momenti distinti che non necessariamente coincidono, dato che l'esecuzione (attivazione), in senso informatico, dello smart contract non comporta necessariamente l'esecuzione delle obbligazioni e prestazioni in esso contenute, se ad esempio non si avverano le condizioni del contratto.

Far coincidere la nascita dello smart contract all'esecuzione delle prestazioni in esso contenute renderebbe, nella prima fase, lo smart contract una sorta di non contratto, o un contratto non ancora perfezionato, quindi estraneo al mondo giuridico.

Quindi, come è stato correttamente qui chiarito, l'esecuzione del contratto si riferisce al

momento in cui il programma viene registrato su blockchain, in quanto è questo il momento in cui le parti decidono di vincolarsi ad una serie di previsioni concordate precedentemente.

Assume anche importanza il fatto che le parti possano prendere visioni di tali disposizioni concordate, tradotte poi in linguaggio informatico, con le difficoltà che ne comporta la comprensione di tale linguaggio.

Per quanto riguarda il requisito della forma, come abbiamo già anticipato, questo è soddisfatto a patto che sia possibile identificare i contraenti a livello informatico attraverso un processo, i cui requisiti, diversamente dal termine previsto, ancora oggi non sono stati resi noti dall'Agenzia per l'Italia Digitale.

È un compito molto importante per far sì che queste tecnologie basate sui registri garantiscano criteri di sicurezza, immodificabilità ed integrità tali da assicurare l'efficacia dell'art. 41 del Regolamento eIDAS.

Questo processo evolutivo della componente informatica ha già dato qualche frutto con la nascita di strumenti capaci di imputare la paternità di documenti informatici come: le firme elettroniche ed i sigilli elettronici ed il Sistema Pubblico di Identità Digitale (SPID), la Carta Nazionale dei Servizi (CNS) e la Carta d'identità elettronica (CIE).

Questi strumenti possono essere, pertanto, utilizzati anche dagli operatori che si occupano della formazione di uno smart contract in quanto riconosciuti sia in UE che nel nostro Paese.

Concludendo, nonostante questi apprezzabili interventi, ad oggi ci sono molte questioni aperte che frenano il diffondere di questa nuova tecnologia.

Infatti, la mancanza di un quadro legislativo chiaro e completo, unita alla complessità di questa tecnologia, frena indubbiamente gli operatori di mercato divenendo una barriera in vista di un utilizzo all'interno di attività imprenditoriali.

Servirebbero delle regole capaci di incentivarne l'utilizzo, e cosa ancora più importante, eliminare le incertezze degli operatori non lasciando spazio a conflitti interpretativi.

Il tutto ovviamente non può rimanere circoscritto all'ambito nazionale, ma occorre, come

evidenziato dal Parlamento Europeo, che ci sia una diffusione in tutta l'UE ed anche a livello internazionale.

La vera sfida sarà trovare una soluzione ad eventuali conflitti che potrebbero sorgere tra i diversi principi che sono alla base degli ordinamenti di ciascuno Stato, cercando anche di trovare un linguaggio informatico universale per la stesura dei contratti, al fine di agevolarne l'interpretazione.

Nonostante qualche risultato sia già stato raggiunto, questo è un processo abbastanza complesso che potrà dare risultati concreti solo nel medio-lungo termine.

CAPITOLO QUARTO

PRINCIPALI APPLICAZIONI DELLA TECNOLOGIA BLOCKCHAIN

4.1 CENNI INTRODUTTIVI

La tecnologia blockchain, che nasce nel 2008 come infrastruttura per supportare la criptovaluta Bitcoin, negli ultimi anni è stata adottata in molti altri contesti grazie alle sue caratteristiche distintive di sicurezza, trasparenza ed immutabilità.

Quando parliamo di blockchain siamo abituati ad associarla solo ad investimenti, ovvero alle criptovalute, ma la maggior parte delle innovazioni che arriveranno nei prossimi anni sono legate ad altri settori.

Sta rivoluzionando il mondo della finanza, della logistica e della gestione delle informazioni e continua a trovare nuove applicazioni in molti altri settori.

In questo capitolo, esploreremo alcune delle principali applicazioni della tecnologia blockchain e come queste stanno cambiando il modo in cui le aziende operano.

Inizieremo discutendo le applicazioni della blockchain nel settore finanziario, dove ha dato vita a una nuova era di criptovalute e di pagamenti digitali sicuri ed efficienti. Si è diffusa una nuova generazione di criptovalute, come Ethereum, Ripple e Litecoin, che stanno diventando sempre più popolari come alternative ai tradizionali metodi di pagamento e trasferimento di denaro.

La blockchain è anche utilizzata per creare nuovi strumenti finanziari, come i contratti intelligenti (smart contract), che consentono di automatizzare le transazioni in modo sicuro ed efficiente.

Successivamente, analizzeremo come la blockchain possa essere utilizzata per migliorare la sicurezza della gestione dei dati.

Ad esempio, la blockchain può essere utilizzata per creare registri immutabili delle transazioni e dei dati sensibili, consentendo una maggiore tracciabilità e riducendo il rischio di frodi e manipolazioni.

La blockchain è inoltre utile nella gestione delle catene di fornitura, dove può aiutare a migliorare la tracciabilità dei prodotti e a prevenire la contraffazione.

Grazie alla tecnologia blockchain, i consumatori possono verificare l'origine e la qualità dei prodotti che acquistano, mentre le aziende possono gestire in modo più efficiente le loro attività di logistica e di produzione.

Esamineremo poi come la tecnologia blockchain stia trovando applicazione in settori come la salute, l'energia rinnovabile e l'immobiliare, dove sta consentendo di creare soluzioni innovative e trasparenti.

In conclusione, ci concentreremo sui vantaggi e sugli svantaggi dell'adozione della blockchain e su come le aziende possono valutare se questa tecnologia sia adatta alle loro esigenze specifiche.

4.2 SETTORE BANCARIO

Il settore bancario e finanziario è uno dei principali campi di applicazione della tecnologia blockchain. La blockchain ha introdotto una nuova era di criptovalute e pagamenti digitali sicuri ed efficienti, offrendo al contempo la possibilità di creare nuovi strumenti finanziari e di gestire i dati sensibili in modo sicuro e trasparente.

Un settore, quello bancario, che si basa sulla mancanza di fiducia tra gli utenti, i quali necessitano di una terza parte che faccia da intermediario e permetta il buon esito della transazione scongiurando il pericolo di truffe.

Con l’avvento della tecnologia blockchain queste problematiche possono esser facilmente

superate, proprio per questo, oggi sono proprio le banche che stanno intensificando gli investimenti, di milioni e milioni di euro, su questa tecnologia.

Questi investimenti ingenti sono finalizzati allo sfruttamento di questa tecnologia per risolvere tutta una serie di punti deboli dell'attuale sistema bancario, oltre che alla risoluzione di alcuni problemi interni.

Infatti, oltre all'utilità che la blockchain potrebbe avere nei loro processi, abbattendo i costi ed aumentando la velocità e sicurezza delle transazioni, le banche temono che questa tecnologia possa tagliarle fuori e sostituirle totalmente in futuro, rendendo quindi superflua la loro esistenza.

La Cina, ad esempio, sta cercando di risolvere un problema interno, quello della "finanza ombra"[47] ed a creare la propria criptovaluta centrale.

Altri Paesi come la Svezia, invece, stanno abbandonando il contante a vantaggio dei pagamenti digitali, mentre India e Senegal cercano di sfruttare questa tecnologia per permettere transazioni semplici e sicure ai milioni di africani ed indiani che sono situati in tutto il mondo, sprovvisti di un proprio conto bancario.

Le banche di tutto il mondo fanno fronte comune per l'implementazione e lo sviluppo della tecnologia nei loro processi, infatti oltre 200 di esse hanno aderito ad un consorzio chiamato R3.

Il consorzio R3 (R3 Consortium) è un'organizzazione che si concentra sulla tecnologia blockchain e sullo sviluppo di soluzioni basate su blockchain per le imprese. È stato fondato nel 2014 da un gruppo di imprese finanziarie, tra cui Barclays, Credit Suisse, HSBC e RBS, per sperimentare l'uso della tecnologia blockchain in ambito finanziario.

R3 si concentra sulla creazione di una piattaforma blockchain chiamata Corda, che è stata sviluppata specificamente per le imprese.

[47] La finanza ombra (o shadow banking in inglese) si riferisce ad un insieme di attività finanziarie che si svolgono al di fuori del sistema bancario tradizionale, spesso caratterizzate da un basso livello di regolamentazione e di trasparenza.

Corda si distingue dalle altre piattaforme blockchain per la sua architettura che consente alle imprese di condividere i dati solo con le controparti necessarie, senza dover rendere pubblico l'intero registro delle transazioni come avviene invece su altre blockchain, come quella di Bitcoin.

Il consorzio R3 continua a crescere e conta oggi centinaia di membri, tra cui imprese finanziarie, istituzioni governative, fornitori di tecnologie e organizzazioni no profit. Oltre alla piattaforma Corda, R3 lavora anche su altri progetti blockchain e collabora con altri consorzi e organizzazioni per promuovere l'uso della tecnologia blockchain nelle imprese.

Rimanendo invece in ambito italiano, uno dei progetti senza dubbio più importanti è quello della “spunta interbancaria”.

Il progetto della Spunta Interbancaria è un'iniziativa promossa dalla Banca d'Italia e dalle principali banche italiane per modernizzare il processo di conciliazione delle transazioni interbancarie.

Il processo di conciliazione della spunta interbancaria riguarda la verifica e l'approvazione delle transazioni tra banche diverse.

In passato, questo processo era spesso manuale e richiedeva molto tempo e risorse per essere completato. Con il progetto della Spunta Interbancaria, l'obiettivo è di automatizzare e semplificare questo processo utilizzando la tecnologia blockchain.

Il progetto prevede la creazione di una rete blockchain privata, basata sulla piattaforma Corda del consorzio R3, che consente alle banche di condividere i dati delle transazioni in modo sicuro e in tempo reale. Ciò elimina la necessità di scambiare informazioni tramite email o fax e consente di risolvere le eventuali discrepanze o errori in modo più efficiente.

Il progetto della Spunta Interbancaria è stato lanciato nel 2019 e nel corso degli anni ha visto un'ampia adesione da parte delle banche italiane. L'obiettivo finale è di rendere il processo di conciliazione più efficiente, riducendo i tempi e i costi per le banche e migliorando l'esperienza per i clienti.

Dopo questa breve analisi, quel che è certo è che la tecnologia blockchain sta invadendo sempre più questo settore e non ci sono dubbi che nei prossimi anni diventerà elemento imprescindibile.

Ciò che invece ad oggi non possiamo prevedere è se in futuro prevarrà un sistema innovativo, con una blockchain pubblica senza la presenza di intermediari, oppure se la paura per l'innovazione farà sì che il consumatore continuerà ad affidarsi a banche e sistemi centralizzati, i quali avranno fatto propria questa nuova tecnologia creando loro valute digitali.

4.3 BLCKCHAIN NEI PROCEDIMENTI GIURIDICI

La tecnologia blockchain può essere applicata in diversi settori, tra cui anche quello giuridico. In particolare, può essere utilizzata per creare registri digitali immutabili e trasparenti, che consentono di mantenere la tracciabilità e l'affidabilità dei dati.

Una volta registrato su blockchain il documento avrà data certa.

Bisogna altresì dire che già prima dell'avvento di questa tecnologia i Paesi si erano dotati di sistemi di certificazioni digitale.

In Italia, ad esempio, era stato introdotto uno strumento che riconoscesse la validità giuridica a strumenti e mezzi di comunicazione digitale con il Codice dell'Amministrazione Digitale.

La sfida odierna è quella di cercare di adattare questa normativa alla nuova tecnologia.

Inoltre, la blockchain può essere utilizzata per creare una piattaforma di gestione delle dispute, che consenta alle parti di registrare le loro posizioni e di discutere e negoziare in modo trasparente e sicuro. In questo modo, le parti possono raggiungere una soluzione efficace e giusta per entrambi senza l'intervento di un tribunale.

Infine, la blockchain può essere utilizzata per creare un registro pubblico dei giudizi e delle

sentenze emesse dai tribunali, consentendo di avere un sistema trasparente e accessibile a tutti per verificare la validità di un giudizio.

4.4 BLCKCHAIN NEL SETTORE DEI TRASPORTI

La tecnologia blockchain può essere utilizzata anche nel settore dei trasporti per migliorare l'efficienza, la trasparenza e la sicurezza delle operazioni di trasporto di merci e persone.

4.4.1 Trasporto merci

Nel settore del trasporto merci, la blockchain può essere utilizzata per tracciare e monitorare le spedizioni, migliorando la sicurezza, l'efficienza e la trasparenza delle operazioni.

Grazie alla blockchain, tutte le informazioni relative alla spedizione (ad esempio: data, luogo di partenza e di arrivo, modalità di trasporto, documenti di trasporto, data di consegna, eventuali incidenti o ritardi) possono essere registrate in modo immutabile e condivise in tempo reale con tutti i soggetti coinvolti nella catena di distribuzione, come fornitori, spedizionieri, corrieri e clienti.

Ciò consente di ridurre il rischio di frodi o errori, di migliorare la tracciabilità delle merci e di ridurre i tempi di consegna, migliorando la gestione delle spedizioni e la soddisfazione dei clienti.

Alcune aziende del settore trasporti stanno già utilizzando la blockchain per tracciare e gestire le spedizioni, ad esempio utilizzando smart contract per automatizzare i pagamenti e garantire la consegna dei beni.

In generale, l'applicazione della blockchain nel trasporto merci potrebbe avere importanti

benefici in termini di efficienza, sicurezza e trasparenza delle operazioni, favorendo la crescita e l'innovazione del settore.

4.4.2 Trasporto persone

La blockchain potrebbe avere molteplici applicazioni nel settore del trasporto di persone. Ecco alcuni esempi:

1. *Gestione dei dati dei passeggeri*: La blockchain potrebbe essere utilizzata per creare un registro digitale di tutti i dati dei passeggeri (nome, cognome, documento di identità, informazioni sulla prenotazione, ecc…). Ciò potrebbe aiutare a semplificare il processo di prenotazione e di controllo del biglietto, riducendo il rischio di frodi.

2. *Pagamenti*: La blockchain potrebbe anche essere utilizzata per gestire i pagamenti delle corse. Questo potrebbe consentire di eliminare le commissioni delle banche o di altri intermediari, ridurre il rischio di frodi e accelerare i tempi di transazione.

3. *Monitoraggio della sicurezza*: La blockchain potrebbe essere utilizzata per creare un registro immutabile delle verifiche sulla sicurezza dei veicoli e dei conducenti. Ciò potrebbe contribuire a garantire un livello più elevato di sicurezza per i passeggeri.

4. *Gestione della logistica*: La blockchain potrebbe essere utilizzata per migliorare la gestione della logistica del trasporto di persone. Ad esempio, potrebbe essere utilizzata per monitorare il movimento dei veicoli e per coordinare le attività di manutenzione.

5. *Gestione delle recensioni*: La blockchain potrebbe anche essere utilizzata per gestire le

recensioni dei passeggeri sui conducenti e sui veicoli. Ciò potrebbe contribuire a garantire una maggiore trasparenza e affidabilità del servizio.

In generale, l'utilizzo della blockchain nel trasporto di persone potrebbe portare a una maggiore efficienza, trasparenza e sicurezza del servizio. Tuttavia, sarebbe necessario sviluppare apposite applicazioni e infrastrutture per supportare l'adozione di questa tecnologia nel settore.

4.5 BLCKCHAIN NEL SETTORE DELLA MODA

La tecnologia blockchain può essere utilizzata nel mondo della moda per migliorare la trasparenza, la sostenibilità e la tracciabilità dei prodotti.

Uno dei principali problemi nel settore della moda è l'impossibilità di tracciare la catena di approvvigionamento delle materie prime, il processo di produzione e la distribuzione dei prodotti.

Ciò rende difficile per i consumatori conoscere l'origine e la qualità dei prodotti e per le aziende garantire la sostenibilità e l'etica nella produzione.

Utilizzando la tecnologia blockchain, è possibile creare un sistema di tracciabilità che registra ogni fase della produzione dei prodotti, dal raccolto delle materie prime fino alla vendita al consumatore finale. Questo sistema consente ai consumatori di verificare l'autenticità dei prodotti e la loro provenienza, e alle aziende di garantire la sostenibilità e l'etica nella produzione.

La tecnologia va ad inserirsi in un contesto dove gli interessi economici sono molto elevati ed il problema delle merci contraffatte è all’ordine del giorno.

A livello legislativo, la tutela della provenienza dei beni è affidata al Regolamento UE n.

952/2013, il cui art. 60 dispone "*Le merci alla cui produzione hanno contribuito due o più paesi o territori sono considerate originarie del paese o territorio in cui hanno subito l'ultima trasformazione o lavorazione sostanziale ed economicamente giustificata, effettuata presso un'impresa attrezzata a tale scopo, che si sia conclusa con la fabbricazione di un prodotto nuovo o abbia rappresentato una fase importante del processo di fabbricazione*".

Dunque, i produttori per non incorrere nelle sanzioni previste dall'art. 4 comma 49 della legge n. 350 del 2003, devono essere in grado di dimostrare sia la provenienza delle materie prime che il luogo in cui avviene la produzione finale del bene.

Introdurre questa tecnologia in questo settore, quindi, permetterebbe al consumatore di effettuare scelte consapevoli, essendo a conoscenza dell'origine del prodotto.

Inoltre, la tecnologia blockchain può essere utilizzata per creare un sistema di proprietà intellettuale che consente ai designer di proteggere le proprie creazioni e di ricevere una giusta remunerazione per il loro lavoro. Utilizzando la blockchain, i designer possono registrare la proprietà delle loro creazioni in modo sicuro e trasparente, riducendo il rischio di frodi e di violazioni del diritto d'autore.

La blockchain può anche essere utilizzata per creare un sistema di gestione degli stock che consente alle aziende di ridurre lo spreco di prodotti invenduti.

Utilizzando la blockchain, le aziende possono tracciare il movimento dei prodotti nel loro magazzino e identificare le opportunità per ottimizzare l'inventario.

In sintesi, l'utilizzo della tecnologia blockchain nel settore della moda può offrire importanti vantaggi in termini di trasparenza, sostenibilità e tracciabilità dei prodotti e rendere consapevoli i consumatori di ciò che realmente acquistano. Tuttavia, l'adozione di questa tecnologia richiede una cooperazione tra le diverse parti coinvolte nel settore e una regolamentazione adeguata per garantire la sicurezza dei dati e delle transazioni.

4.6 APPLICAZIONI DELLA BLCKCHAIN IN AMBITO SANITARIO

La blockchain, grazie alla sua natura decentralizzata e sicura, può trovare molteplici applicazioni nell'ambito sanitario. Ecco alcune delle possibili applicazioni:

1. *Gestione dei dati sanitari*: la blockchain può essere utilizzata per creare un registro distribuito e immutabile dei dati sanitari dei pazienti. In questo modo, i dati possono essere condivisi tra diversi operatori sanitari in modo sicuro e trasparente, garantendo la privacy dei pazienti e riducendo il rischio di errori.

2. *Tracciamento dei farmaci*: la blockchain può essere utilizzata per tracciare la catena di approvvigionamento dei farmaci, dalla produzione alla distribuzione. In questo modo, si può garantire l'autenticità dei farmaci e prevenire la contraffazione.

3. *Autenticazione delle prescrizioni*: la blockchain può essere utilizzata per autenticare le prescrizioni dei medici, garantendo la loro autenticità e riducendo il rischio di frodi.

4. *Pagamenti in sanità*: la blockchain può essere utilizzata per gestire i pagamenti in sanità, rendendoli più sicuri e trasparenti. Inoltre, può aiutare a ridurre i costi delle transazioni e migliorare l'efficienza dei processi di fatturazione.

5. *Ricerca clinica*: la blockchain può essere utilizzata per creare registri distribuiti e immutabili dei risultati delle ricerche cliniche. In questo modo, i dati possono essere condivisi tra diversi ricercatori in modo sicuro e trasparente, migliorando l'efficienza della ricerca clinica e accelerando lo sviluppo di nuovi farmaci.

6. *Consentire il monitoraggio e la prevenzione delle epidemie*: la blockchain può essere utilizzata per monitorare la diffusione di malattie infettive e prevenire epidemie attraverso la creazione di registri decentralizzati che tracciano i dati sanitari della popolazione e dei viaggiatori.

7. *Facilitare la donazione di organi*: la blockchain può essere utilizzata per creare un sistema di tracciamento immutabile per la donazione di organi, in modo da garantire che gli organi siano distribuiti in modo equo e che non ci siano frodi o abusi.

Ci sono già alcune applicazioni della blockchain nell'ambito sanitario, come ad esempio *MedicalChain*, che consente ai pazienti di controllare i propri dati medici e condividerli con i professionisti sanitari autorizzati, o *Guardtime*, che utilizza la blockchain per proteggere le forniture mediche durante la catena di distribuzione.

Queste sono solo alcune delle possibili applicazioni della blockchain nell'ambito sanitario. L'uso della blockchain può migliorare l'efficienza e la sicurezza dei processi sanitari, portando benefici sia ai pazienti che agli operatori sanitari.

4.7 BLOCKCHAIN IN AMBITO ASSICURATIVO

Gli esperti sono pronti a scommettere che uno dei settori che maggiormente sarà rivoluzionato dalla tecnologia blockchain sarà proprio quello assicurativo.

Infatti, le caratteristiche della blockchain, che permettono di avere transazioni veloci e sicure, andranno a risolvere tutta una serie di problematiche che caratterizzano questo settore.

Uno dei problemi più importanti è sicuramente quello delle truffe e dei molti dati che

un’assicurazione deve gestire, che, se gestiti in maniera decentralizzata in tempo reale permetterebbero sicuramente di avere enormi benefici sia per la compagnia in termini di efficienza, sia anche nei confronti dei clienti con polizze ridotte.

In tempo reale si potrebbe avere una scheda con la situazione di ogni cliente migliorando la sua esperienza ed implementandola con ulteriori servizi.

Alcune delle multinazionali più importanti del settore, come Swiss Re, Zurich, Allianz, Munich Re ed Aegon si sono già mosse costituendo B3i (Blockchain Insurance Industry Initiative) che ha come obiettivo lo studio della tecnologia blockchain applicata a questo settore.

Gli aspetti principali che andranno ad essere trattati riguarderanno l’assistenza del cliente con gestione dei reclami ed automatizzazione dei processi, riducendo i costi.

Poi si cercherà di ampliare anche l’offerta, implementandola con ulteriori servizi.

Sono state sviluppate già alcune startup, tra queste Poleecy[48], di origine italiana, che permette l’attivazione istantanea e personalizzata di alcune polizze assicurative, il tutto sfruttando la tecnologia blockchain tramite un’app.

In sintesi, la blockchain offre molte opportunità per l'ambito assicurativo, consentendo alle compagnie assicurative di ridurre i costi, migliorare l'efficienza e la trasparenza e offrire prodotti personalizzati ai loro clienti.

[48] Poleecy è una startup italiana fondata nel 2019 che opera nel settore assicurativo digitale. La missione di Poleecy è quella di offrire soluzioni innovative per semplificare l'esperienza di acquisto di prodotti assicurativi online, migliorando la trasparenza e la personalizzazione delle polizze assicurative.

4.8 LA BLOCKCHAIN NELLA PUBBLICA AMMINISTRAZIONE

Negli ultimi anni la PA ha iniziato un processo di innovazione tecnologica, introducendo nuove tecnologie in vari settori.

Ovviamente la blockchain, in virtù delle sue proprietà, è stata protagonista di questa innovazione con la nascita di progetti, europei ed italiani, finalizzati a sfruttare le sue potenzialità valorizzando i servizi erogati dalle Pubbliche Amministrazioni.

I più importanti progetti sono EBSI (*European Blockchain Service Infrastructure)* ed IBSI*(Italian Blockchain Service Infrastructure).*

- EBSI (*European Blockchain Services Infrastructure*) è un'iniziativa dell'Unione Europea che mira a creare un'infrastruttura comune per la gestione di servizi basati su blockchain tra i vari paesi membri dell'Unione.

L'obiettivo principale di EBSI è quello di accelerare l'adozione della tecnologia blockchain nella pubblica amministrazione e nei servizi pubblici europei, migliorando l'efficienza e la trasparenza delle operazioni e riducendo i costi.

L'infrastruttura fornirà servizi di autenticazione, di firma digitale, di condivisione di dati e di tracciabilità delle transazioni basati su blockchain, garantendo al contempo la conformità alle normative sulla protezione dei dati.

L'iniziativa EBSI è stata avviata nel 2019 e coinvolge diversi paesi membri dell'Unione Europea, insieme a diverse organizzazioni pubbliche e private. Il progetto è in fase di sviluppo e implementazione, ma si prevede che potrebbe avere un impatto significativo sulla modernizzazione della pubblica amministrazione europea.

- IBSI (*Italian Blockchain Service Infrastructure*) è un'iniziativa del governo italiano per sviluppare un'infrastruttura comune per la gestione di servizi basati su blockchain tra le varie organizzazioni pubbliche e private in Italia.

L'iniziativa IBSI coinvolge diverse organizzazioni pubbliche e private in Italia, tra cui il Ministero dell'Economia e delle Finanze, l'Agenzia delle Entrate, l'Agenzia per l'Italia Digitale, l'Istituto Nazionale di Previdenza Sociale (INPS) e il Consiglio Nazionale del Notariato.

IBSI mira a creare un'infrastruttura tecnologica comune per le organizzazioni coinvolte, consentendo loro di condividere dati e informazioni in modo sicuro, veloce ed efficiente attraverso la tecnologia blockchain.

L'iniziativa IBSI è stata lanciata nel 2019 e si prevede che potrebbe avere un impatto significativo sulla modernizzazione delle organizzazioni pubbliche e private in Italia.

Quindi le caratteristiche di immodificabilità e tracciabilità della blockchain permettono di avere una gestione dei dati sempre chiara e trasparente nei confronti sia dei cittadini che degli altri Enti interessati, favorendo, quindi, una collaborazione che sfocia in servizi sempre più efficienti.

In sintesi, la blockchain può offrire molte opportunità per la pubblica amministrazione, migliorando l'efficienza, la trasparenza e la sicurezza dei processi e dei servizi offerti ai cittadini. Tuttavia, è importante considerare anche le sfide e le criticità legate all'adozione della tecnologia blockchain, come la complessità della gestione della blockchain stessa, la necessità di standard interoperabili e la protezione della privacy dei dati personali dei cittadini.

4.9 CHARITY

La tecnologia blockchain può essere utilizzata nel mondo della beneficienza in diversi modi per aumentare la trasparenza, la sicurezza e l'efficacia delle donazioni.

Uno dei principali vantaggi della blockchain è la possibilità di creare registri digitali immutabili e trasparenti, che possono essere utilizzati per tracciare le donazioni e garantire che i fondi vengano utilizzati per gli scopi previsti.

Inoltre, la blockchain può essere utilizzata per automatizzare i processi di donazione e distribuzione dei fondi, riducendo i costi amministrativi e migliorando l'efficienza delle operazioni.

Ad esempio, alcune organizzazioni no profit stanno utilizzando la tecnologia blockchain per creare piattaforme di crowdfunding decentralizzate, in cui i donatori possono visualizzare in tempo reale come vengono utilizzati i loro fondi. In questo modo, i donatori possono avere una maggiore fiducia nell'efficacia delle loro donazioni e le organizzazioni no profit possono dimostrare la loro trasparenza e responsabilità.

Inoltre, la blockchain può essere utilizzata per creare programmi di incentivazione basati sulla tokenizzazione, in cui i donatori ricevono token che possono essere utilizzati per acquistare beni o servizi specifici, come ad esempio una donazione per la ricerca di una malattia o per la costruzione di un ospedale. In questo modo, i donatori possono avere una maggiore influenza sulle attività delle organizzazioni no profit e sentirsi più coinvolti nelle loro attività.

Uno dei progetti più interessanti è sicuramente quello di Binance “la crypto-filantropia”.

Attraverso la costituzione di un’organizzazione no profit, la *Blockchain Charity Foundation* (BCF) garantisce che una somma donata arrivi al 100% al suo destinatario senza commissioni.

Questa organizzazione sta avendo molto successo ed ha stretto partnership con gli enti più

importanti del settore.

Altri progetti “blockcharity” sono *Aidcoin*, che si occupa di render tracciabili le donazioni ed *Helperbit* che raccoglie fondi in bitcoin indirizzandoli ad ONG ed associazioni di beneficenza che aiutano coloro che sono stati colpiti da calamità naturali.

Secondo molti esperti questo sarà il settore che trarrà maggiori benefici dall’adozione della tecnologia blockchain vista la crescente sfiducia nei confronti dei mezzi di beneficenza tradizionali.

In generale, la tecnologia blockchain offre molte opportunità per migliorare il mondo della beneficienza, ma ci sono anche problematiche da affrontare, come la regolamentazione e la sicurezza dei dati. Tuttavia, molte organizzazioni no profit stanno già esplorando le potenzialità della blockchain e ci si aspetta che la sua adozione continui a crescere nel tempo.

CONCLUSIONI: luci ed ombre legate all'applicazione della tecnologia Blockchain

La tecnologia Blockchain e gli Smart Contract rappresentano un'innovazione significativa nel campo della gestione e della sicurezza dei dati.

Nessuno anni fa, alla nascita di Bitcoin, si sarebbe aspettato uno sviluppo di questa tecnologia di tale portata da interessare diversi settori dell'economia.

La loro capacità di creare registri distribuiti e di eseguire codici autoeseguibili ha il potenziale di trasformare numerose industrie e settori, dalla finanza alle forniture, dall'energia alle assicurazioni.

La tracciabilità è un'altra caratteristica che rende Blockchain e Smart Contract unici. Grazie alla natura immutabile dei registri distribuiti, è possibile tenere traccia di tutte le transazioni e di tutte le modifiche apportate ai dati registrati. Questo aumenta la trasparenza dei processi e la fiducia tra le parti coinvolte.

Queste caratteristiche oggi vengono sfruttate in ambito industriale, contrastando la problematica della contraffazione e garantendo un monitoraggio su tutta la supply chain e la veridicità delle informazioni documentali fornite. Il veloce adattamento e l'utilità che questa tecnologia ha dimostrato nei confronti dei vari settori dell'industria, fanno ben sperare per il futuro, in quanto secondo gli esperti ancora oggi non viene sfruttata al massimo del suo potenziale.

Inoltre, grazie alla natura decentralizzata e alla crittografia avanzata, la blockchain consente di effettuare transazioni finanziarie sicure e senza intermediari, eliminando la necessità di dover fare affidamento su banche o altri intermediari di fiducia.

La blockchain può essere utilizzata per creare sistemi di autenticazione e identità digitale. Questi sistemi consentono di eliminare la necessità di dover fare affidamento su intermediari di fiducia per la verifica dell'identità, rendendo il processo più

efficiente e sicuro.

Infine, la blockchain può essere utilizzata per creare sistemi di votazione e democrazia digitale. Grazie alla sua natura decentralizzata e alla crittografia avanzata, la blockchain può garantire l'integrità e la trasparenza del processo elettorale, aiutando a prevenire eventuali tentativi di manipolazione o frode.

Tuttavia, l'adozione di queste tecnologie presenta ancora alcune criticità, tra cui la scarsa interoperabilità tra diverse piattaforme Blockchain, la complessità di sviluppare Smart Contract sicuri e affidabili e la necessità di standardizzazioni e normative più chiare.

L'aspetto normativo rappresenta una delle principali sfide per l'adozione di Blockchain e Smart Contract.

Attualmente, come trattato in questo studio, la regolamentazione di queste tecnologie è ancora in fase di evoluzione, poiché i legislatori, sia a livello nazionale che internazionale, cercano di comprendere e regolare gli aspetti legali e fiscali delle applicazioni Blockchain e non hanno ancora trovato la giusta chiave per far convivere diritto e tecnologia al fine di avere un quadro normativo chiaro e favorevole allo sviluppo di queste tecnologie.

In molti paesi la regolamentazione è ancora limitata e varia notevolmente da una giurisdizione all'altra.

Ad esempio, alcuni paesi hanno promosso la tecnologia Blockchain e la creazione di criptovalute attraverso incentivi fiscali e normative favorevoli, mentre altri hanno adottato una posizione più restrittiva.

Una delle principali questioni normative riguarda la definizione giuridica degli Smart Contract e la loro applicabilità nel diritto contrattuale. In molti casi, gli Smart Contract sono considerati legalmente vincolanti solo se soddisfano determinati requisiti di validità, come la capacità delle parti di contrarre e la mancanza di vizi del consenso.

Inoltre, la questione della privacy e della protezione dei dati personali rappresenta un'altra sfida normativa per l'adozione di Blockchain e Smart Contract.

La natura immutabile e permanente della tecnologia Blockchain può creare difficoltà nel rispettare le normative sulla privacy e sulla protezione dei dati personali, come il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea.

Oltre all'aspetto normativo, però, permangono anche altre problematiche, altrettanto importanti.

La maggior parte delle blockchain richiedono un enorme consumo di energia per la verifica delle transazioni e il mantenimento del registro. Ciò potrebbe avere un impatto ambientale negativo e può essere costoso in termini di costi energetici.

Ad esempio, il Bitcoin, la criptovaluta più famosa che utilizza la blockchain, consuma più energia di alcune nazioni intere.

L'implementazione di una soluzione blockchain richiede spesso una significativa quantità di risorse finanziarie, umane e tecnologiche. Ciò potrebbe limitare l'adozione della tecnologia blockchain da parte delle organizzazioni più piccole o meno finanziariamente solide. La manutenzione richiede una costante attenzione e risorse, il che può essere costoso per le organizzazioni a lungo termine. Inoltre, eventuali errori o bug nell'applicazione blockchain potrebbero essere difficili da correggere senza dover interrompere l'intera rete blockchain.

Anche se la blockchain è una tecnologia decentralizzata, esiste la possibilità che alcuni attori dominino la maggior parte del potere di calcolo, rendendo la blockchain meno democratica e più centralizzata.

Le blockchain attuali hanno limitazioni in termini di scalabilità, poiché richiedono una grande quantità di risorse computazionali per l'elaborazione delle transazioni. Ciò potrebbe limitare l'utilizzo della blockchain in ambienti ad alta frequenza di transazioni o in situazioni in cui sono necessari tempi di elaborazione rapidi.

Anche se la blockchain è generalmente considerata sicura, esistono alcune vulnerabilità potenziali che potrebbero essere sfruttate dagli attaccanti per compromettere la sicurezza del sistema. Ad esempio, i sistemi di smart contract sulla blockchain potrebbero essere soggetti a bug o a violazioni di sicurezza, mettendo a rischio i fondi degli utenti.

In conclusione, la blockchain e gli smart contract rappresentano una grande opportunità per l'innovazione e la trasformazione digitale.

Tuttavia, come con qualsiasi tecnologia emergente, ci sono sfide e problemi da risolvere, ma con la giusta attenzione alle questioni di sicurezza, regolamentazione e adozione di massa, la blockchain e gli smart contract potrebbero diventare parte integrante del nostro futuro digitale e della nostra economia.

BIBLIOGRAFIA

- COMANDINI G.L., *Da zero alla Luna. Quando, come e perché la Blockchain sta cambiando il mondo,* Palermo, Dario Flaccovio Editore, Marzo 2022.

- BASSOLI E., *Smart Contract, criptovalute e blockchain,* Pisa, Industrie Grafiche della Pacini Editore S.r.l., 2021.

- COMELLINI S., VASAPOLLO M., *Blockchain, criptovalute, I.C.O. e Smart Contract,* Rimini, Maggioli Editore S.r.l., 2019.

- DUROVIC M., JASSEN A., *The formation of blockchain - based smart contracts in the light of contract law, in European Rewiew of Private Law,* Giugno, 2019.

- TOSI. E., *Contratti informatici, telematici e virtuali. Nuove forme e procedimenti formativi*, Giuffrè Editore, Milano, 2010.

- COMELLINI S., VASAPOLLO M., Blockchain, criptovalute, I.C.O. e Smart Contract, Rimini, Maggioli Editore S.r.l., 2019.

- RINALDI G., *Smart contract: meccanizzazione del contratto nel paradigma della blockchain*, in G. Alpa (cur.), Diritto e intelligenza artificiale, Pisa, 2020.

- DE FILIPPI V.P., *The interplay between decentralization and privacy: the case of blockchain technologies*.

SITOGRAFIA

- https://www.altalex.com/documents/news/2021/06/29/smart-contract-profili-di-qualificazione-giuridica

  Marco Nigro

- https://blog.osservatori.net/it_it/smart-contract-in-blockchain

  Andrea Reghelin

- https://www.filodiritto.com/blockchain-e-smart-contract

  Duilia Delfino

- https://www.dirittodelrisparmio.it/wp-content/uploads/2022/04/A.-Albanese_Smart-contract.pdf

  Alessia Albanese

- https://www.chainon.it/la-valenza-giuridica-degli-smart-contract/

  Davide Calderone

- https:// www.legaltech-smartcontract.it/quadro-normativo

- https://www.agendadigitale.eu/documenti/litalia-prova-a-normare-gli-smart-contract-ecco-come-pro-e-contro/

  Massimiliano Nicotra

- https://www.altalex.com/documents/news/2019/10/01/blockchain-e-smart-contracts-report-forum-europeo

  Massimiliano Nicotra