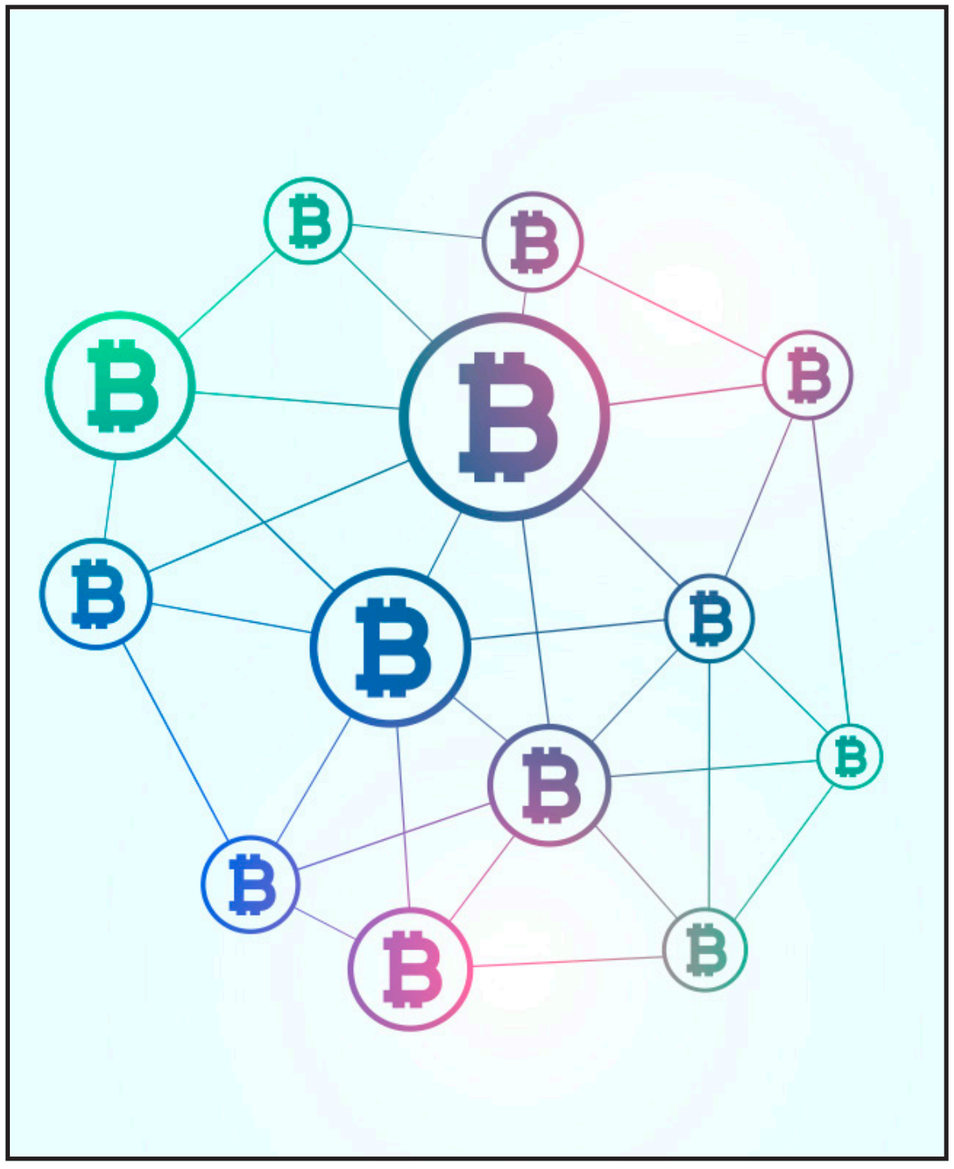
BLOCKCHAIN

a cura di Studio Martelli & Partners S.p.A.

STUDIO MARTELLI & partners

SIMPLY. DIFFERENT. LAWFIRM.

INDICE



INTRODUZIONE

L'IMPORTANZA DELLA BLOCKCHAIN NELLO SVILUPPO DEI BUSINESS FUTURI

Sono sempre stato un appassionato di tecnologia forse è per questo che ho iniziato a studiare la blockchain! Nel corso delle mie ricerche mi sono reso conto che, estrapolata dal più noto contesto monetario, questo sistema possiede un infinito potenziale e una versatilità ancora inesplorata.
Nella sua lettura più semplice, blockchain si configura come una tecnologia di base che ha il potenziale di effettuare una vera a propria trasformazione degli obsoleti modelli di business fino ad ora utilizzati, velocizzandone i processi e riducendone i costi. Basti pensare all'applicazione che può avere nel processo di validazione del Made in Italy, nella certificazione dei prodotti agroalimentari o nella verifica della correttezza degli atti all'interno di un sistema politico. Le declinazioni sono ampie, dal settore giuridico, al bancario, all'assicurativo, al logistico, al contabile, al finanziario, in sintesi in tutte quei sistemi che prevedono il rapporto fra più soggetti e gruppi e che quindi presuppongono una relazione di fiducia che è alla base di tutte le transazioni.
Questa Guida nasce con il duplice obiettivo di dare una prima infarinatura a chi non ha, come me, l'expertise tecnico ma ne è allo stesso tempo incuriosito e di essere uno strumento valido per potere tradurre in business un sistema dall'alto valore tecnologico.

avv. Giovanni Battista Martelli

1. COSA È UNA BLOCKCHAIN

1.1 DEFINIZIONE

La blockchain, termine che deriva dall'unione delle parole *block* (blocco) e *chain* (catena), è un database distribuito decentralizzato strutturato come un catena di blocchi, contenenti transazioni, correlati tra di loro secondo un principio cronologico e la cui integrità è assicurata da un sistema di algoritmi e regole crittografiche. I dati, una volta inseriti all'interno dei blocchi, non possono più essere modificati retroattivamente senza che vengano invalidati tutti i processi successivi e ciò implicherebbe il consenso della maggioranza del sistema. Ogni record viene memorizzato in modo da includere una quota di informazioni che fanno capo alle informazioni precedenti, questa connessione rende virtualmente impossibile l'alterazione senza che essa sia immediatamente visibile a tutta la rete. A loro volta i blocchi per entrare a fare parte della catena vengono sottoposti a un processo di validazione che si basa sul principio del consenso distribuito, consenso che rende superflua la figura di un supervisore che ne assicura la legittimità. La blockchain è quindi un registro decentralizzato basato sul principio della fiducia distribuita che, grazie alla sua innovativa configurazione, non necessita di un terzo potere che ne garantisce l'incorruttibilità perché è la sua stessa natura a tutelarla.

1.2 CENNI STORICI E NORMATIVI

Un primo accenno alla piattaforma blockchain appare nel 2008 nel "*Bitcoin design paper*", il White Paper all'interno del quale Satoshi Nakamoto (pseudonimo la cui vera identità resta ancora sconosciuta) spiega la sua idea di moneta virtuale governata da algoritmi: il Bitcoin. L'obiettivo era quello trovare una soluzione ad alcuni problemi connessi al sistema decentralizzato dei pagamenti che Nakamoto risolve tramite la progettazione di una piattaforma distribuita su un network peer to peer dove i nodi agiscono contemporaneamente da fruitori e distributori di informazioni. L'anno successivo viene creato il Genesis Block, ovvero il blocco iniziale della Blockchain Bitcoin. L'interesse per ciò che si nasconde dietro la criptovaluta, ovvero la tecnologia blockchain, inizia a manifestarsi tra il 2014 e il 2015 quando altre piattaforme come Ethereum e Ripple attingono al principio su cui si fonda per creare smart contract o per facilitare il pagamento interbancario in valute differenti. La tematica blockchain inizia a diventare un tema di interesse mondiale e a richiamare l'attenzione anche di molte copertine, ricordiamo la prima pagina dell'*Economist* del 2015 dal titolo *"The trust machine. How the technology behind Bitcoin could change the world"*. Nello stesso anno la Linux Foundation lancia il progetto Hyperledger per lo sviluppo collaborativo di blockchain mentre nel 2016 il pool di banche R3 rilascerà la sua Distributed Ledger chiamata Corda. Da questo momento in poi l'idea di blockchain si emancipa dalla moneta virtuale e dalla Blockchain con al "B" maiuscola (legata principalmente al Bitcoin) e inizia ad assumere un ruolo da protagonista come "tecnologia blockchain" applicabile in tutti quei processi decentralizzati di scambi di beni in rete che presuppongono, per essere ritenuti validi, affidabilità e incorruttibilità.
In Italia approda nel 2017 ma solo in fase embrionale con la partecipazione di Unicredit e Intesa San Paolo alla sperimentazione del Global Payment Innovation di SWIFT, a cui seguirà la nascita di SiaChain, la piattaforma lanciata da SIA e la sperimentazione della tecnologia blockchain applicata al processo di spunta interbancaria da parte di ABI Lab.
La caratteristica di transnazionalità della blockchain rende complicata una regolamentazione unilaterale da parte di un singolo Stato soprattutto se si vuole applicare l'approccio tipico dei sistemi basati sul controllo diretto degli appartenenti della catena. A livello normativo possiamo fare riferimento alla *"Risoluzione del parlamento Europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione* (2017/2772(RSP)", con cui si invita la Commissione a collaborare con gli Stati membri al fine di garantire la certezza per gli investitori, cittadini e utenti, attivi e passivi, promuovendo contemporaneamente l'armonizzazione all'interno dell'Unione e valutando di inserire un passaporto europeo di progetti basati sulle DTL (Distributed Ledger Technology) sottolineando che *"qualsiasi approccio regolamentare nei confronti della DLT dovrebbe essere favorevole all'innovazione, consentire un sistema di "passaporto"* ed essere improntato ai principi di neutralità tecnologica e neutralità dei modelli aziendali". Lo scopo della Risoluzione è quello di sollecitare la nascita di un quadro giuridico europeo che abbia lo scopo di eliminare gli ostacoli che potrebbero nascere dalla scambio tramite DLT e favorire l'attuazione della blockchain attraverso un atteggiamento proattivo.

1.3 CARATTERISTICHE PRINCIPALI DI UNA BLOCKCHAIN

La blockchain serve a fornire certezze. E' una tecnologia di base attraverso la quale è possibile tracciare delle informazioni, tokenizzare dei beni o reperire fondi attraverso i sistemi di crowdfunding digitale. Le sue caratteristiche principali sono la decentralizzazione, l'immutabilità e la sicurezza.

1.3.1 Decentralizzazione

A differenza dei vecchi registri centralizzati, nella blockchain sono i vari nodi della rete a essere i detentori delle informazioni. Se consideriamo la blockchain come un database dobbiamo pensare a una rete di utenti connessi tra di loro che hanno uguale accesso ai dati senza l'intervento di un terzo potere che li autorizzi e che detenga il monopolio delle transazioni. Nella blockchain ogni nodo ha una funzione attiva e passiva, è nello stesso tempo creatore e validatore. Ogni utente della catena possiede una propria copia della blockchain, non ne esiste una ufficiale e nessun utente è più credibile dell'altro, questo assicura la transnazionalità della tecnologia. Ogni transazione è sorvegliata da una relazione di nodi che ne garantiscono la legittimità e la conservazioni sin dalla sua nascita, un apparato democratico dove le informazioni sono ugualmente accessibili a tutti e altrettanto verificabili. Questo è il principio della fiducia distribuita. La blockchain è un sistema che non necessita di un'autorità centrale perchè le norme che la regolano vengono definite prima. Queste leggi nella blockchain si identificano con l'algoritmo matematico la cui soluzione dà diritto di accesso alla catena. Viene per questo associata spesso al concetto di Distributed Ledger, che affronteremo più avanti, in antitesi il Centralized Ledger (Libro Mastro Centralizzato) proprio perché la blockchain si basa sull'idea di fiducia distribuita tra i vari soggetti o gruppi.

1.3.2 Immutabilita'

Accanto alla decentralizzazione, l'immutabilità del dato è un'altra delle caratteristiche peculiari di questa tecnologia. La blockchain è un registro non modificabile. I record memorizzati all'interno dei blocchi, grazie all'uso di crittografie a chiave pubblica, non possono essere alterati o cancellati dai nodi della rete. Questo sistema di immutabilità determina l'elevato valore dell'informazione che si figura sempre di più come asset unico digitale. In questi termini la blockchain si caratterizza come una Value Chain, una catena del valore, che consente di effettuare delle transazioni certe come ad esempio nel caso Bitcoin.

1.3.3 Sicurezza

La decentralizzazione e l'immutabilità dell'informazione rendono l'informazione stessa sicura. Qualora un Paese volesse bloccare l'accesso al network, la decentralizzazione assicurerebbe l'ingresso ai dati da parte degli altri nodi che possiedono la propria copia della blockchain mentre il principio dell'immutabilità ne impedirebbe la corruzione. Questo rende una transazione, di qualunque natura essa sia - beni, servizi o pagamenti - sicura. Questa tecnologia ha il potenziale quindi di effettuare una vera a propria trasformazione degli obsoleti modelli di business fino ad ora utilizzati, velocizzando i processi e riducendo i costi. Basti pensare all'applicazione che può avere nel processo di validazione del Made in Italy, nella certificazione dei prodotti agroalimentari o nella verifica della correttezza degli atti all'interno di un sistema politico.

1.4 DISTRIBUTED LEDGER TECHNOLOGY

Per comprendere il significato di Distributed Ledger Technology (DLT) bisogna partire dal concetto di ledger. Un ledger è un registro, una memoria storica di tutte le transazioni, un archivio. In Italia esempi di ledger sono il Catasto, il PRA o la Banca Centrale, istituzioni che si basano su una logica centralizzata per la gestione ed elaborazione dei dati. Con l'introduzione della blockchain e l'uso di crittografie e algoritmi, l'accesso alle informazioni non è più riconducibile a livello centrale ma è gestito da un network di attori alla pari, questo sistema ha consentito ai database di evolversi da centralizzati a distribuiti. Il principio del network, attraverso la tecnologia peer to peer, consente a tutti i nodi di partecipare attivamente alla costituzione della rete in modo indipendente ma, contemporaneamente, sotto il controllo degli altri nodi, secondo la logica del consenso distribuito. Il raggiungimento del consenso porta all'autorizzazione dell'operazione e al conseguente aggiornamento di tutta la catena. In quest'ottica non possiamo più pensare al Distributed Ledger come a un archivio ma dovremmo considerarlo come una "relazione" tra utenti e transazioni.

2. LA STRUTTURA DI UNA BLOCKCHAIN

2.1 DEFINIZIONE E RUOLO DELLE PRINCIPALI COMPONENTI DI UNA BLOCKCHAIN

2.1.1 La transazione

La transazione è quel bene, valore o informazione che viene scambiato tra due o più soggetti su una piattaforma blockchain e che necessita di essere approvato e verificato e archiviato. E' costituita dalle informazioni relative all'oggetto della transazione (nel caso di un immobile ad esempio le informazioni saranno il prezzo, l'effettiva proprietà dell'immobile, i dati catastali etc...) e da una Cryptographic Key, ovvero un insieme di crittografie a chiave pubblica che permettono la verifica dell'identità degli utenti.

2.1.2 I nodi

I nodi sono i server della rete attraverso i quali vengono gestite le transazioni. I nodi hanno il compito di conservare una copia aggiornata di tutta la catena.

2.1.3 Il codice di Hash

L' Hash di un blocco rappresenta il suo codice di autenticazione. Possiamo considerarla come una impronta digitale che determina l'unicità e assicura l'inviolabilità del blocco. Si ricava partendo da una serie di dati variabile (input) che vengono processati attraverso la **funzione di hash**. Questa procedura rilascia (output) un codice alfanumerico irreversibile che non consente in alcun modo di risalire ai dati dell'input esattamente come da una impronta digitale di una persona non è possibile risalire al suo DNA.

2.1.4 Il miner e il mining

Il miner è colui che mette a disposizione la potenza di calcolo del proprio computer per validare le transazioni e consentire al blocco di essere inserito nella catena blockchain. Il processo di certificazione effettuato dai miner è definito **mining**. La validazione si ottiene attraverso la ricerca da parte del miner di un numero (nonce) che, se processato insieme ad altri dati tramite funzione di hash, restituisce l'hash corretto. Una volta trovata la soluzione gli altri miner devono verificarne la correttezza. In caso affermativo il miner che ha validato il blocco otterrà una ricompensa, meccanismo della Proof of Work. Il blocco validato verrà poi aggiunto alla catena. I miner quindi sono contemporaneamente creatori di blocchi e validatori.

2.1.5 Il blocco

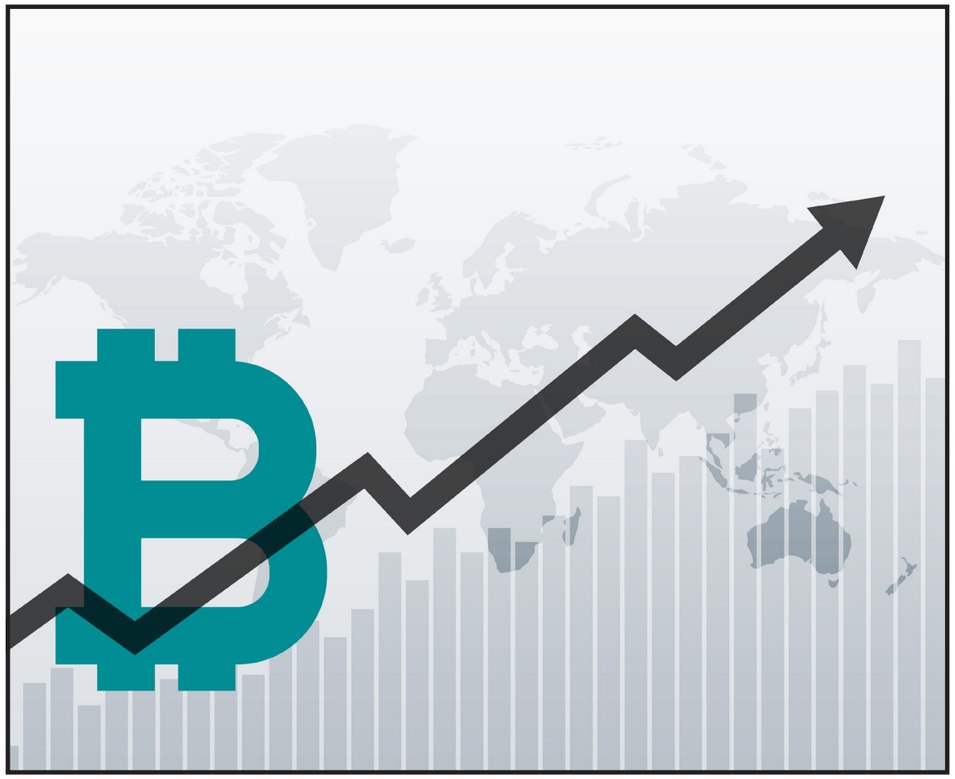
Il blocco è un insieme di transazioni verificate. E' una delle unità che compongono l'insieme della blockchain. Un blocco è composto da due parti principali: l'header e il body. Le transazioni sono racchiuse nel body del blocco e nell'header sono presenti i campi di gestione del blocco stesso. Nella risoluzione dei blocchi è possibile che due miner riescano a trovare una soluzione per lo stesso blocco a distanza di pochi secondi. In questo caso si genererà una **biforcazione** con l'inserimento di due blocchi non perfettamente identici ma che rispettano entrambi la verifica matematica del blocco precedente. Il blocco che formerà la catena più lunga sarà ritenuto valido mentre l'altro, il **blocco orfano**, verrà eliminato.

2.1.6 La Proof of Work e la Proof of Stake

La **Proof of Work (PoW)** è la prova che consente al miner di dimostrare agli altri nodi la validazione del blocco e che permette di ottenere la ricompensa. Nella Blockchain Bitcoin la ricompensa viene rilasciata in automatico e consiste nell'emissione di una nuova criptovaluta. I sistemi di Proof of Work richiedono una grande potenza di calcolo e un enorme dispendio di energia elettrica. Inoltre, la competizione tra i miner tipica dei sistemi PoW causa con maggiore facilità la generazione di una biforcazione della catena.
I sistemi di **Proof of Stake (PoS)** hanno, invece, blocchi più semplici da risolvere, sono più vantaggiosi in termini di scalabilità, necessitano di una potenza di calcolo inferiore e di meno energia. In questi sistemi il miner che avrà la possibilità di risolvere il blocco viene scelto sulla base di precisi parametri. I nodi che fanno maggiormente girare l'economia del sistema si qualificano ad essere i prescelti. Non esistono ricompense per la validazione delle transazioni. La PoS è un sistema non competitivo dove ciò che conta è l'efficienza del sistema.

2.1.7 I Fork

Con Fork si intende una biforcazione della blockchain originaria che genera una catena che mantiene tutte le caratteristiche della blockchain precedente. Spesso si generano a seguito della creazione di nuovi token. Creare token da zero è il metodo più comune e prevede un copia e incolla del codice esistente che poi viene modificato e lanciato come nuovo token. Un metodo alternativo è invece quello di biforcare. In questo caso le modifiche vengono applicate alla blockchain esistente che si divide. Esistono due tipologia e fork: **hard e soft**. Con la prima si fa riferimento a una scissione incompatibile con la blockchain precedente, scissione che porta a una netta divisione dei due codici tra i quali non potrà più esserci scambio di dati. Gli hard fork possono essere usati per modificare o migliorare un protocollo esistente, oppure per creare un nuovo protocollo e una nuova blockchain indipendente. E' il caso del Bitcoin Cash nato da un fork su Bitcoin risalente all'agosto 2017. I soft fork indicano invece una scissione capace di mantenere un collegamento con la catena precedente. Questo significa che i nodi non aggiornati sono ancora in grado di elaborare transazioni e aggiungere nuovi blocchi alla blockchain, a condizione che non vadano in contrasto con le regole del nuovo protocollo.



2.2 COME FUNZIONA
UNA BLOCKCHAIN

2.2.1 Creazione di una transazione

Su una piattaforma blockchain la transazione serve scambiare asset di qualsiasi natura tra un due o più soggetti. Prima di avviare il processo, è necessario creare una transazione firmandola a doppia chiave. La procedura prevede la creazione da parte del soggetto mittente di un Digest (un'impronta digitale) tramite la funzione di Hash. Una volta creato il Digest, il soggetto mittente lo firma usando la propria chiave privata a cui aggiunge la chiave pubblica del destinatario della transazione. Quest'ultimo, essendo in possesso della propria chiave pubblica, quando riceverà la transazione sarà in grado di decifrare la firma digitale per risalire al Digest.

2.2.2 Validazione della transazione

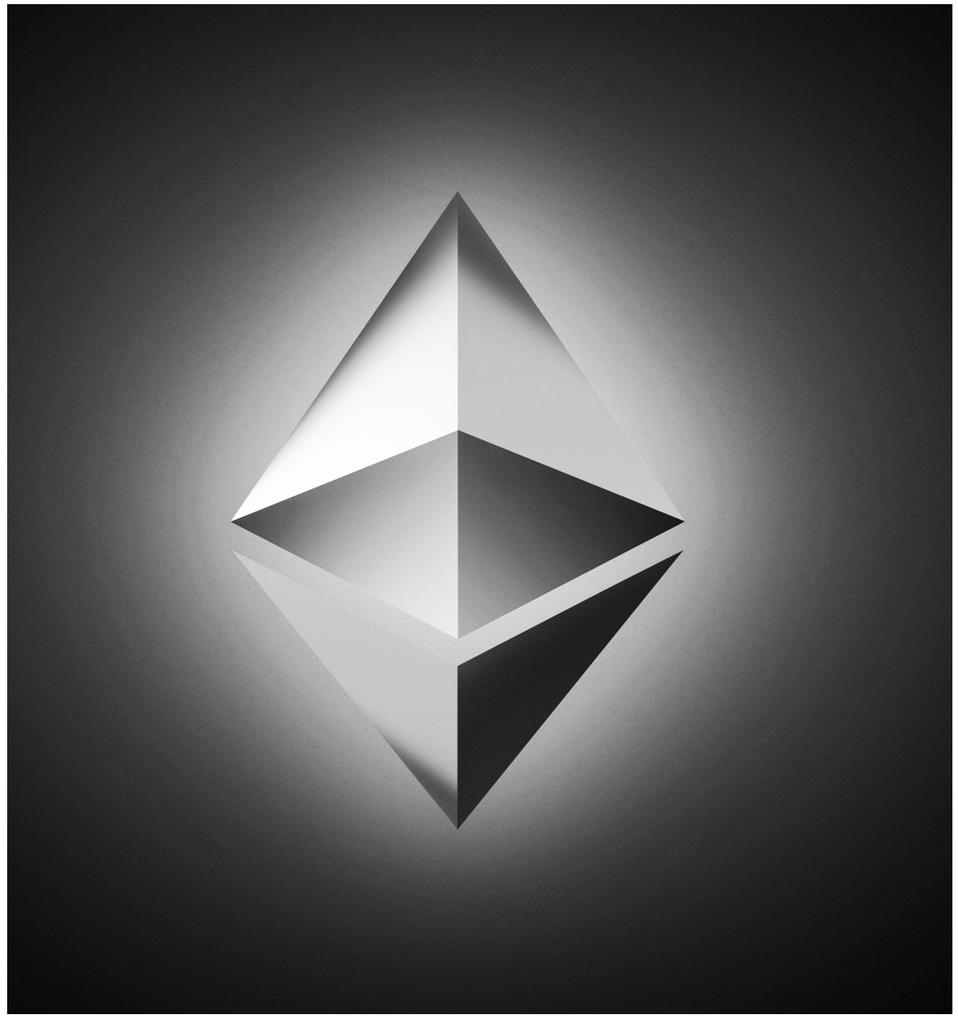
Una volta creata, la transazione e il suo Hash vengono propagati agli altri nodi del network per la verifica. In questo caso si tratta di un procedimento indipendente perchè effettuato da ogni singolo nodo. Quando il nodo riceve una transazione inizia a costruire un blocco dando l'avvio a quel processo di validazione che viene chiamato mining e che consiste nel gareggiare con gli altri nodi per risoluzione del puzzle crittografico che consta di tempo ed energia elettrica.

2.2.3 Il fenomeno del *Double Spending*

Visto che ogni nodo contiene le stesse informazioni degli altri nodi della catena e conosce tutta la storia delle transazioni avvenute in passato potrebbe volutamente inserire delle transazioni non veritiere per alterare la storia precedente, fenomeno del Double Spending. Il processo di mining e la Proof of Work servono proprio per creare consenso sulla rete e per decidere quale delle due transazioni è da considerare valida. Nel protocollo bitcoin, ad esempio, per Double Spending si intende quel rarissimo fenomeno per il quale un utente può spendere contemporaneamente i propri bitcoin verso due riceventi. Il bitcoin non può essere duplicato o speso due volte per questo, ogni volta che vengono inviati, è necessario verificare che questi non siano già stati spesi in passato.

2.2.4 Verifica del blocco

Una volta risolto l'algoritmo, il nodo validatore segnala agli altri nodi della network che il blocco è stato validato in modo che i possano verificarne l'effettiva correttezza. Dopo la verifica il blocco validato viene aggiunto alla catena.



3. EVOLUZIONE DELLA BLOCKCHAIN

3.1 BLOCKCHAIN PUBBLICHE E PRIVATE

I modelli di gestione del consenso determinano la differenza tra Distributed Ledger Pubbliche e Private. Le prime, dette anche Unpermissioned ledger, sono aperte e non hanno una proprietà. Le più famose sono la Blockchain Bitcoin ed Ethereum.
Queste strutture sono completamente decentralizzate e non hanno restrizioni di accesso. Sono condivise tra tutti i nodi allo stesso modo. Nessun utente della rete ha privilegi sugli altri, nessuno può controllare le informazioni che vengono memorizzate su di essa, modificarle o eliminarle e nessuno può alterare il protocollo che determina il funzionamento di questa tecnologia. Presentano però un problema di fondo, quello della scalabilità perchè al crescere della quantità dei nodi la velocità della transazione rimane invariata pur aumentando la stabilità del sistema che si presenta di volta in volta più sicuro.
Le seconde, Permissioned ledger, possono essere controllate e avere una proprietà.
E' questa autorità che determina i criteri di accesso e quali sono i ruoli che un utente può ricoprire all'interno della rete. In questa tipologia di struttura i dati, al momento dell'inserimento, sono sottoposti alla verifica non della maggioranza ma di un gruppo ristretto di attori preventivamente autorizzati.
Sono tipologie di blockchain prevalentemente utilizzate da enti pubblici, banche, imprese e presenta una serie di vantaggi: sono più performanti, veloci, è possibile modificarne le regole, ripristinare le transazioni e, a differenza delle blockchain pubbliche, necessitano di una Governance che ne definisca le regole di accesso, i principi di validazione e ne disciplini l'attività.

3.2 LE PRINCIPALI PIATTAFORME
BLOCKCHAIN

3.2.1 La Blockchain Bitcoin

La Blockchain Bitcoin è la piattaforma blockchain lanciata il 3 gennaio 2009 per lo scambio della valuta virtuale denominata bitcoin.
Come funziona? Ogni nodo/utente può, tramite la creazione di un account, costruire il proprio wallet, un portafoglio che funge da deposito e da conto da cui prelevare bitcoin e la cui inviolabilità è garantita da una serie di codici alfanumerici. Ogni wallet è legato a un indirizzo attraverso cui è possibile effettuare transazioni come inviare denaro o acquistare un prodotto o un servizio. Dal punto di vista tecnico l'utente (A) predispone un indirizzo a chiave pubblica per ricevere la transazione. L'utente (B) dopo avere identificato uno dei suoi indirizzi (che indica un quantitativo specifico di bitcoin) fa partire la transazione associando la chiave pubblica dell'utente (A) al suo indirizzo. Ad ogni chiave pubblica viene associato l'equivalente di una firma digitale, chiave privata, utile per assicurarsi che solo il proprietario di un certo indirizzo possa avviare una transazione ed esso legata. Generalmente, per facilitare l'anonimato e rendere meno complicate le transazioni, ognuna di queste è gestita tramite la generazione di un nuovo indirizzo su cui ricevere la valuta. La chiave privata e il controllo sugli input pregressi garantiscono la sicurezza e la tracciabilità della transazione. Una delle caratteristiche principali della Blockchain Bitcoin è la tracciabilità. Nella rete non è possibile trovare impronta del saldo del conto dei singoli utenti, la proprietà di una certa quota di bitcoin è dimostrata dalle transazioni effettuate in precedenza. Ogni transazione è composta da una serie di input - che fa riferimento a un indirizzo bitcoin - correlati alle transazioni passate. I nodi della rete per verificare le transazioni controllano gli input a loro associati con lo scopo di validare la proprietà delle somme. Per rendere possibile questa operazione, in fase di installazione di un wallet, viene scaricato lo storico di tutte le operazioni svolte che vengono immediatamente elaborate per verificarne l'autenticità, operazione che può richiedere anche diverse ore. Oltre alla tracciabilità, il bitcoin garantisce sicurezza tramite:

- l'impiego della chiave privata che permette di assicurarsi che solo il reale proprietario di un certo quantitativo di bitcoin possa creare una transazione legata a quel bitcoin;
- il controllo degli input pregressi che sono a loro volta utilizzati per accertare che il mittente abbia veramente il numero di bitcoin necessari per sostenere la transazione.

3.2.2 Ethereum

Progettata da Vitalik Buterni nel 2015, Ethereum è una piattaforma decentralizzata pubblica progettata per creare, pubblicare e gestire smart contract tramite tecnologia peer to peer. Il funzionamento di Ethereum è simile a quello della Bitcoin ma rispetto ad essa è più veloce e più potente. Possiamo considerare Ethereum come una evoluzione dell'originaria piattaforma blockchain, con essa si passa dal concetto di Distrubuted Database al concetto Distributed Computing, un computer in grado di fornire una enorme potenza disponibile ovunque. Per questo viene considerata un'evoluzione della piattaforma originaria, una sorta di "piattaforma di nuova generazione" o piattaforma 2.0.
Ethereum è classificabile come Unpermissioned ledger, una blockchain dove tutti possono accedere alla rete e pensata per non essere censurata e bloccata, e come Programmable Blockchain ovvero una piattaforma che non si limita allo sviluppo di operazioni predefinite ma consente agli utenti di attivare delle proprie operazioni: gli smart contract. L'utilizzo della potenza di calcolo di Ethereum viene pagato tramite una cryptocurrency denominata Ether che funge contemporaneamente da criptovaluta e da carburante della piattaforma. Ethereum è un sistema di Turing Complete che permette agli sviluppatori di creare applicazioni che girano su Ethereum Virtual Machine, il motore di ricerca di Ethereum. Questo opera in maniere protetta rispetto al network, il suo codice non ha accesso alla rete e gli stessi smart contract generati sono autonomi e indipendenti da tutti gli altri smart contract.
Nel 2016 Ethereum è stata divisa in due diverse Blockchain: Ethereum Classic ed Ethereum Foundation. La prima rappresenta l'organizzazione che ha come obiettivo la gestione di tutte le attività di sviluppo, di ricerca e di supporto della piattaforma. Ethereum Classic, invece, nasce da una scissione del nucleo originario di Ethereum a livello di Ethereum Foundation ed è costituita da tutti i membri che hanno deciso di dare vita a nuova piattaforma basata sui principi originali di Ethereum a cui si aggiungono una serie di servizi pensati per aumentare la sicurezza e la fruibilità.

3.2.3 Ripple

E' una blockchain di tipo ibrida utilizzata prevalentemente per gli scambi interbancari che si basa sul modello dello Shared Decentralized Ledger. In questo tipo di struttura i nodi validatori sono preselezionati e coincidono con le banche che hanno deciso di utilizzare questo sistema mentre i blocchi vengono validati da un sistema fondato sul voto. Grazie a Ripple le istituzioni finanziarie possono elaborare i pagamenti dei propri clienti in qualsiasi parte del mondo in maniera affidabile, istantanea e sicura. Per gli scambi viene impiegato l'asset digitale XRP, una sorta di sistema valutario privato a cui i partecipanti hanno espresso il loro consenso e il cui impiego ha lo scopo di semplificare le transazioni, abbassare i costi e velocizzare i tempi di lavorazione.

3.2.4 Corda

Il sistema di Corda, come quello di Ripple, si basa sul principio della Shared Decentralized Ledger. E' una piattaforma utilizzato per impiego bancario dedicata prevalentemente alle soluzioni enterprise, sviluppatosi a seguito della nascita del Consorzio R3, un pool di istituti finanziari a cui hanno aderito un centinaio di banche nel 2015. Il White Paper *"The Corda Platform: An Introduction"* di Richard Gendal Brown, CTO di R3, descrive le caratteristiche tecniche di Corda e ne evidenzia le principali differenze verso le blockchain pubbliche come Bitcoin o Ethereum. La principale diversità consiste nella presenza di un unico nodo validatore a cui viene conferita l'autorità di supervisionare e regolamentare le attività della rete, il nodo centrale chiamato state object è un documento digitale che raccoglie tutte le informazioni rilevanti su un accordo condiviso tra le parti, inclusa la sua esistenza, il contenuto e lo stato corrente. Il consenso i viene raggiunto sullo specifico state object che viene condiviso solo tra chi è autorizzato a vederlo mentre hash crittografici sicuri vengono utilizzati per identificare i soggetti e i dati e per collegare gli state object alle versioni precedenti, dando vita così a una catena di provenienza.

3.2.5 EOS

EOS è un un nuovo tipo di blockchain ideata per sviluppare applicazioni decentralizzate e capace di supportare grandi volumi di transazioni al secondo. E' stata lanciata da Daniel Larimer e presentata per la prima volta durante una conferenza nel 2017 con il lancio di una ICO. Pur essendo molto simile ad Ethereum è molto più veloce, più scalabile e più efficace. Grazie al sistema della scalatura orizzontale, EOS è in grado di elaborare milioni di transazioni al secondo, contro le 15 transazioni di Ethereum. Si tratta di un software open-source che dà diritto a tutti gli utenti che possiedono un token EOS di utilizzare le risorse in base alle quote acquisite. Questo rende le transazioni gratuite al 100%. EOS utilizza un algoritmo di consenso chiamato Delegated Proof of Stake (DPoS) per proteggere la sua blockchain. Nel DPoS è un ristretto numero di delegati eletti dall'intera rete con un sistema di consensi a provvedere alla convalida di ogni singola transazione della rete. I delegati possono produrre blocchi in proporzione al numero di voti che ricevono rispetto a tutti gli altri produttori. Un blocco viene prodotto ogni 3 secondi da un singolo produttore autorizzato. EOS, inoltre, introduce alcune nuove misure di sicurezza che prevengono i furti e che possono ripristinare i fondi rubati. E' inoltre una blockchain flessibile in quanto dà la possibilità di poter bloccare l'operazione nel caso in cui si verifichi un errore. Grazie alla reversibilità è quindi possibile ripetere la transazione senza intoppi.

3.3 LO SMART CONTRACT

3.3.1 Definizione

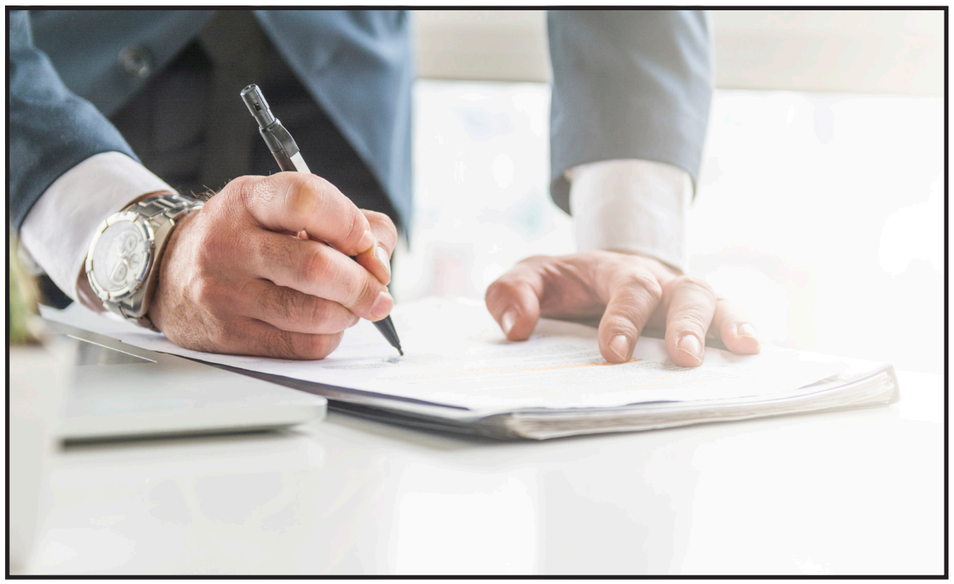
Lo smart contract è la trasposizione in codice di un contratto che ha la capacità in automatico di verificare l'avverarsi di determinate condizioni e di eseguire azioni o dare disposizioni in merito. Tecnicamente si basa su script che leggono le varie clausole del contratto e le condizioni operative entro le quali si devono e si auto attiva nel momento in cui i dati riferiti alle situazioni reali corrispondono ai dati riferiti alle condizioni contrattuali concordate.
Contrariamente a quanto si pensa, lo smart contract non nasce con la blockchain ma è antecedente. Già negli anni '70 si hanno tracce di un primo contratto intelligente impiegato per gestire l'attivazione o disattivazione di una licenza software, gestione avveniva tramite una chiave digitale in grado di avviare il funzionamento del software qualora il cliente avesse pagato la licenza. In seguito nel 1996 da Nick Szabo, il primo a sperimentare l'uso dello smart contract, conia il termine e lo definisce nel White Paper *"Smart Contracts: Building Blocks for Digital Free Markets"*. La sua idea era quella di incorporare una serie di dati contrattuali all'interno di un software capace di automatizzare l'esecuzione e attivare delle conseguenze nel caso in cui le clausole non fossero state rispettate.

3.3.2 Dal contratto automatico al contratto semantico

Come abbiamo visto lo smart contract nasce come contratto automatico. Nel corso degli anni, però, lo sviluppo della tecnologia blockchain e il crescente impiego di questo sistema per le transazioni digitali hanno reso necessaria la nascita di uno strumento che fosse in grado di automatizzare le relazioni tra le diverse parti che operano nella transazione. Questo passaggio è possibile solo tramite una trasformazione del contratto digitale che da automatico deve evolversi in semantico. L'implementazione di questo fattore consente di aumentare la precisione nell'interpretazione dei significati delle parole e in modo direttamente proporzionale permette di aumentare la precisione nella gestione delle azione che gli smart contract sono chiamati ad attivare. Lo smart contract, contrariamente a quanto si pensa, non elimina la figura dell'avvocato o del notaio, ruoli necessari come advisor delle parti in causa nella definizione delle clausole, delle modalità e delle regole di controllo e azione ma elimina il loro intervento nella fase in cui il contratto si trasforma in codice ed esegue automaticamente e in maniera indipendente dai contraenti le condizioni precedentemente stabilite. Questo punto è fondamentale per capire la differenza che sussiste tra il contratto tradizionale e smart contract che, alla luce di quanto descritto, appare come un programma che elabora in modo deterministico le informazioni che vengono raccolte. Se da una parte questa caratteristica è fonte di sicurezza in quanto garantisce l'assoluta certezza di giudizio oggettivo escludendo qualsiasi forma di interpretazione, dall'altra parte affida al codice il potere e la responsabilità di decidere. In questo quadro, l'aspetto semantico assume un ruolo primario nello sviluppo e nella precisione di azione di questo strumento.

3.3.3 Rapporto tra smart contract e blockchain

Il rapporto tra blockchain smart contract appare chiaro nel momento in cui nasce la necessità di rendere questi contratti digitali sicuri e affidabili. La struttura della blockchain assume così il ruolo di autorità garante e di controllo che attesta l'immutabilità delle clausole e verifica l'esecuzione al realizzarsi delle condizioni stabilite. In questo senso lo sviluppo e la gestione di progetti smart contract vanno a vantaggio di quelle realtà professionali capaci di unire una competenza sul profilo legale con solide competenze tecniche e di sviluppo. Si comprende in questi termini quali possono essere i molteplici impieghi degli smart contract sulla piattaforma blockchain. Un esempio molto frequente è quello relativo all'acquisto di un'auto a rate. Basterà incorporare in uno smart contract tutte le informazioni relative all'acquirente, al prezzo, alla modalità di pagamento etc... dati che, una volta inserite in blockchain, non potranno più essere modificati. Lo smart contract gestirà automaticamente tutti gli aspetti definiti nelle clausole contrattuali, tra queste anche quelle relative all'inadempienza dei pagamenti delle rate. In questo caso lo smart contract, rilevando l'insolvenza, andrà ad attivare un dispositivo installato sull'auto che bloccherà le funzioni principali della macchina, come ad esempio l'accensione. Questo è possibile in quanto il contratto di acquisto, riscontrando il mancato rispetto della clausola relativa pagamento della quota, riconoscerà un'anomalia e automaticamente farà scattare la sanzione. Un altro esempio è l'acquisto di un servizio multimediale. Lo smart contract andrà a gestire le condizioni di utilizzo del servizio nel rispetto di quanto stabilito al momento della sua definizione in sede contrattuale. Se si è scelto un servizio di utilizzo su base temporale e nella fruizione si va oltre il valore stabilito dal contratto, lo smart contract bloccherà in automatico l'erogazione del servizio.



3.4 TOKEN E TOKENIZZAZIONE

3.4.1 Definizione di token e caratteristiche principali

Un token è un asset digitale che può essere scambiato su piattaforma blockchain tra due parti senza che sia necessaria l'azione di un intermediario. Il token rappresenta digitalmente un valore associato a un bene, un servizio o un diritto di proprietà.
I token si caratterizzano per:

- **liquidità**: può essere facilmente trasformato in valuta corrente o criptovaluta;
- **frazionabilità**: permette la suddivisione del valore in unità anche molto piccole;
- **scambiabilità**: consente di effettuare compravendite;
- **immutabilità**: una volta inserite le informazioni digitali su blockchain non sarà più possibile modificarle.

3.4.2 Classificazione dei token

Token di classe 1, 2 e 3

- **Token di classe 1 o token coin** che può essere trasferito tramite transazioni su blockchain. Questa tipologia non conferisce diritti nei confronti di una controparte ma ha la funzione di registrare un diritto di proprietà del token stesso o l'esistenza (su blockchain) di un determinato soggetto/oggetto. Rientrano in questa categoria i token di criptovalute come **Bitcoin Cash, Litecoin**, etc...;
- **Token di classe 2**. I token di questa categoria prevedono l'esistenza di una controparte e conferiscono ai proprietari dei diritti da esercitare nei confronti o del soggetto che ha generato i token o nei confronti di terzi. Alcuni esempi sono:
  - **Token per pagamenti di specifico ammontare**: in questi casi il titolare ha diritto di ricevere un pagamento per un importo specifico;
  - **Token per pagamenti futuri**: conferisce il diritto a ricevere dei pagamenti futuri sulla base di determinate condizioni;
  - **Token per la prestazione di servizi o il ricevimento di beni materiali e immateriali**. In questo caso il titolare ha il diritto di ricevere una determinata prestazione o un bene dal soggetto emettitore o da un terzo che abbia stipulato accordi commerciali con questi. In tale ambito rientrano anche i token per l'accesso a infrastrutture informatiche che possono anche avere

le caratteristiche di criptovaluta nativa e conferiscono la possibilità di utilizzare un'infrastruttura specifica di blockchain;

- **Token asset**: questi rappresentano il diritto di proprietà di un determinato asset materiale o immateriale. Possono figurare anche quote di partecipazione dell'entità giuridica emittente o di entità terze. Di questo ultimo esempio fanno parte gli equity token che rappresentano sostanzialmente la proprietà della società sottostante di cui se ne condividono le fortune e gli eventuali fallimenti.

Queste informazioni registrate su blockchain possono essere trasferite tramite un protocollo e possono incorporare altri diritti addizionali governati da smart contract. Più in generale i token di classe 2 potrebbero essere inquadrati in quelli che il nostro ordinamento conosce come titoli di credito, ossia documenti che, secondo l'art. 1992 c.c., conferiscono al possessore "diritto alla prestazione in esso indicata verso presentazione del titolo", nelle varie tipologie di titoli cambiari, titoli obbligazionari o di prestito, titoli di partecipazione, titoli rappresentativi di merci e documenti di legittimazione.

- **Token di classe 3**. L'ultima categoria riguarda il token che conferisce diritti di comproprietà in quanto oltre a rappresentare una proprietà conferisce anche diritti diversi, quali diritti di voto, diritti economici, etc... In questa tipologia il titolare non ha un diritto esercitabile verso l'emittente del titolo o verso un terzo.

Security token e Utility token

Un'altra importante classificazione è quella che viene fatta tra **Security** e **Utility token**. I **Security token** sono considerati come dei veri e propri investimenti finanziari per cui il possessore detiene parte del valore del sottostante che viene creato da terze parti, come ad esempio le azioni di una compagnia quotata in Borsa.

Gli **Utility Token** rappresentano invece un mezzo di accesso ad un servizio e non sono considerati dalla SEC (la Security and Exchange Commission) come investimenti finanziari. Ad esempio, Ethereum e Bitcoin sono da considerarsi Utility. Per quanto riguarda la loro regolamentazione bisogna considerare come principale punto di riferimento la disciplina antiriciclaggio del 2017 (D.l.vo 25/5/2017). Questo testo normativo ha portato nel mondo dell'antiriciclaggio il termine "valuta digitale".

Fungible Token e Not Fungible Token

I Fungible Token (FT) sono quei token il cui valore è da considerarsi intercambiabile. L'esempio classico è quello della moneta: il valore di 1 Euro è lo stesso di qualsiasi altro Euro, la stessa cosa vale per l'Ether o il Bitcoin. I Not Fungible Token (NFT) hanno invece un valore unico nel loro genere, non intercambiabile. I NFT sono indivisibili e sulla piattaforma blockchain hanno un ID univoco.

3.4.3 Il processo di tokenizzazione

Il processo di tokenizzazione consiste nella conversione dei diritti di un bene/servizio in un token digitale registrato su blockchain, dove il bene reale e il token sono collegati da uno smart contract. Tokenizzare significa creare un token e collegarlo a un bene fisico tramite contratto intelligente, processo che si realizza su piattaforma blockchain.

3.4.4 Esempi di beni tokenizzati

Il settore immobiliare è uno dei primi campi in cui la tokenizzazione ha preso piede ma in realtà è un processo applicabile a molti settori di investimento.

Tokenizzazione di una nave

Il proprietario di un'imbarcazione che deciderà di tokenizzare la propria nave, frazionerà tutto o parte del proprio yacht in quote che saranno poi convertite in certificati di proprietà digitali (token) e messi in vendita su blockchain. Lo smart contract, oltre a collegare la quota fisica al token su piattaforma, andrà ad escludere anche la possibilità di censura, interruzioni, frodi o interferenze di terzi. L'investitore potrà così comprare, in sicurezza, una o più quote tramite blockchain diventando "azionista" della nave in proporzione al valore dei token acquistati. Questa attività racchiude molti vantaggi:

- il processo, di per sé democratico, consentirà anche ai piccoli investitori di diventare proprietari di un bene che in altri casi sarebbe loro precluso;
- eliminazione di mutui o intermediari;
- velocizzazione del processo di vendita e incasso immediato;
- certezza e sicurezza dell'operazione garantita dal sistema blockchain;
- l'emittente resterà proprietario della nave potendo usufruire dei vantaggi;
- qualora l'imbarcazione fosse messa in charter, ogni singolo "azionista" ne trarrebbe beneficio economico in proporzione al valore dei token acquisiti.

Tokenizzazione di un'opera d'arte

Un altro esempio, molto meno comune ma utile per comprendere le potenzialità infinite di questo processo, è quello relativo alla tokenizzazione di un'opera d'arte. La maggior parte delle volte un bene materiale privato, come un'opera d'arte, è illiquido cioè incapace di produrre denaro. Questo perché spesso i procedimenti di vendita richiedono la presenza di intermediari il cui intervento è quasi sempre dispendioso in termini di moneta e tempo. Tokenizzare un'opera d'arte consente di accelerare i processi e assicurare la liquidità. Non dimentichiamo che un bene tokenizzato ha un valore più elevato rispetto l'equivalente fisico perché si hanno maggiori possibilità di reperire su di esso informazioni certe tramite blockchain. Anche in questo esempio, come per l'imbarcazione, il procedimento di tokenizzazione prevederà la conversione di tutti o parte dei diritti di proprietà sull'opera in token che verranno emessi su piattaforma blockchain per lo scambio. L'acquirente comprerà token/quote dell'opera diventando proprietario non di un bene fisico ma di un certificato di proprietà digitale. Grazie a blockchain la transazione verrà gestita direttamente dalle parti in causa che potranno verificare in tempo reale il processo di scambio e incassare, per ciò che concerne la parte venditrice, immediatamente la liquidità. Volendo semplificare e sintetizzare ulteriormente, possiamo paragonare un bene tokenizzato a un puzzle dove le tessere possono avere tutte lo stesso valore o valore univoco. Le tessere/quote/azioni etc… saranno messe in vendita dal soggetto proprietario del bene come certificati di proprietà digitali (token) su una piattaforma blockchain. Ogni token avrà un proprio ID specifico che lo collegherà alla frazione di bene corrispondente. Questo collegamento è garantito dallo smart contract. L'acquirente potrà decidere se comprare una o più tessere del puzzle in base all'investimento che vorrà realizzare. L'acquisto dei token consentirà di essere proprietari di un bene di solito inaccessibile, permetterà al venditore di trasformare quel bene da "perdita" a "guadagno" e darà la possibilità agli acquirenti di incassare ulteriore liquidità nel caso in cui il bene in oggetto venga "movimentato" allo scopo di produrre un ritorno economico.

3.5 ICO

3.5.1 Definizione

Un Initial Coin Offering (ICO) è un token che ha funzione valutaria. Grazie al sistema blockchain è possibile non solo tokenizzare un bene e venderlo su piattaforma e/o acquistarlo tramite la valuta digitale della piattaforma scelta (Ether, EOS, etc…) ma è anche possibile creare e una propria moneta, vendere il bene tokenizzato tramite l'utilizzo della nuova moneta digitale oppure reperire fondi attraverso essa.

3.5.2 ICO e IPO

L'ICO è il corrispettivo nel mondo delle criptovalute dell'IPO (Initial Public Offering) e consente a una società privata di diventare tutta o in parte pubblica grazie all'emissione e alla vendita sul mercato azionario regolamentato di quote societarie. La differenza principale tra IPO e ICO risiede nel fatto che le prime sono, appunto, regolamentate e prevedono la vendita di azioni che rappresentano un diritto di proprietà mentre le ICO non sono regolamentate e prevedono la vendita di token digitali al quale non corrisponde nessun diritto di proprietà.

3.5.3 Come funzionano le ICO

Lo scopo principale delle ICO è quello di generare moneta per la realizzazione di nuovi progetti. Ad oggi, per le start up, rappresenta un'alternativa al crowdfunding. Tutti coloro che vogliono avviare un nuovo progetto di business possono creare una nuova moneta ed emetterla per la vendita come token su blockchain a un determinato prezzo. L'emissione dei nuovi token è accompagnata, solitamente, dalla pubblicazione del White Paper che include tutte le informazioni relative al progetto in questione. Gli investitori interessati all'idea di business acquisteranno i token e, a seguito della realizzazione del progetto, usufruiranno dei servizi in proporzione alla quota di token acquistati. In questo modo la società otterrà le risorse economiche per avviare i proggetto senza avere alcun obbligo nei confronti degli investitori se non quello di rendere poi disponibile il servizio per il quale hanno acquistato i token. Gli investitori, inoltre, hanno la possibilità di rivendere i token acquistati ad altri acquirenti. Generalmente una ICO può durare da 1 a 3 mesi e, al termine di essa, i token vengono inviati agli investitori nei wallet da loro indicati. Dopo la fine della ICO, la criptovaluta viene listata su uno o più exchange dove potrà essere scambiata con altre criptovalute.

3.5.4 Vantaggi e svantaggi delle ICO

Le ICO presentano numerosi vantaggi:

- anche i piccoli investitori possono partecipare a una ICO;
- i gettoni possono essere acquistati a un basso prezzo;
- è un modo veloce per reperire capitali.

Lo svantaggio principale è l'assenza di regolamentazione che porta a un alto rischio di frode. Gli investitori corrono il pericolo di trovarsi di fronte a contratti assimilabili a strumenti finanziari privi però delle garanzie che vengono fornite in caso di acquisto di prodotti sui mercati regolamentati.

3.5.5 La normativa: l'esperienza maltese, i paesi europei e l'Italia

Con riferimento alla blockchain e alle Distributed Ledger Technology, il 4 luglio 2018 il Governo maltese ha emanato 3 atti legislativi con l'obiettivo di garantire l'integrità del mercato, la protezione dei consumatori e dell'industria in generale. Nello specifico si tratta del:

- *Malta Digital Innovation Authority Act*: relativo all'istituzione di una apposita autorità nazionale che ha lo scopo di supportare lo sviluppo e promuovere l'innovazione tecnologica tra cui la cosiddetta tecnologia Distributed Ledger Technology;
- *Innovative Technology Arrangement and Services Act*: per la regolamentazione di specifiche tecnologie innovative e per regolare l'esercizio di funzioni regolatorie da parte dell'autorità per l'innovazione digitale maltese;
- *Virtual Financial Assets Act* (VFA Act): per regolare l'emissione di asset finanziari virtuali, i cosiddetti Virtual Financial Assets (VFA).

Anche altri paesi europei si sono mossi in questa direzione se pur con modalità e risultati diversi. Tra questi ci sono la Svizzera che ha emesso delle Guidelines sul tema delle ICO e il Liechtenstein che ha pubblicato una specifica Fact Sheet con la quale ha espresso la sua posizione assimilando, in certi casi, i token a degli strumenti finanziari. Purtroppo si tratta di tentativi isolati che mancano di una visione europea globale.

E in Italia? Con il documento *"Le offerte iniziali e gli scambi di cripto-attività"* pubblicato il 19 marzo 2019, la Consob ha cercato di definire le regole da adottare per le offerte e gli scambi di quelle criptovalute che non siano univocamente qualificabili come strumenti finanziari. Un investimento di natura finanziaria, secondo l'Autorità, è quello in cui ricorrano tre elementi:

- l'impiego di capitale;
- l'aspettativa di rendimento di natura finanziaria;
- l'assunzione di un rischio direttamente connesso e correlato all'impiego di capitale.

Nel caso in cui vi sia offerta di prodotti finanziari deve essere applicata la disciplina che prevede l'obbligo di redazione di un prospetto informativo e quella relativa alla promozione e collocamento a distanza di tali tipologie di prodotti. In assenza di tali adempimenti l'Autorità di vigilanza può sospendere le attività promozione della vendita del token verso il pubblico italiano. L'obiettivo del documento, quindi, è quello di proporre una regolamentazione delle offerte di utility token e di token cosiddetti ibridi attraverso la creazione, nel sistema della disciplina delle attività finanziarie, di una categoria apposita e diversa da quella dei prodotti finanziari.

3.5.6 Il caso DAO

DAO è l'acronimo di Decentralized Autonomous Organization. Si tratta di organizzazioni imprenditoriali costituita da persone reali che, con lo scopo di reperire fondi e lanciare idee imprenditoriali, creano una loro piattaforma blockchain sulla quale operano grazie a smart contract come aziende digitali, senza persona giuridica. Nella storia della DAO è noto il caso "DAO", ritenuto uno degli eventi più critici dalla nascita di blockchain e che ha influenzato l'evoluzione di Ethereum. Nel 2016 "DAO" era un'organizzazione creata su Ethereum che raccoglieva fondi tramite lo scambio di Dao token con Ether. I creatori di "DAO" hanno ideato un sito internet dove circolavano le relative comunicazioni; hanno redatto il White Paper in cui è stato descritto il programma e all'audit del codice sorgente degli smart contract utilizzati e hanno provveduto a elaborare gli accordi con alcuni "exchange" per permettere lo scambio dei token acquisiti. L'offerta di "DAO" era mirata a raccogliere capitali da investire su progetti che venivano prima valutati da un comitato e successivamente posti in votazione ai possessori dei token che potevano esprimere il loro voto, proporzionale al quantitativo di DAO Token posseduti, per determinare a quali progetti sarebbero poi stati erogati i capitali. Nel giro di poco tempo "DAO" raccolse 150 milioni di dollari ma a causa di un attacco al codice della piattaforma, in poche ore, ne andarono in fumo circa 70. L'evento indusse la SEC ad analizzare la vicenda per comprendere meglio come poter collocare questo strumento. La SEC considerò i DAO token come delle securities, con la completa applicazione della relativa legge federale e dei principi generali rispetto al diritto degli strumenti finanziari anche ai soggetti che abbiano raccolto risparmio tramite l'uso della Distributed Ledger Technology. La decisione della SEC ha fatto da battistrada alle successive pronunce da parte degli altri enti regolatori, evidenziando quanto sia importante delineare quanto prima un quadro giuridico internazionale entro il quale potersi muovere in sicurezza.

3.6 BLOCKCHAIN E CROWDFUNDING

3.6.1 Cosa e' il crowdfunding

Il *crowdfunding* è uno strumento finanziario che si basa sulla filosofia della partecipazione e condivisione per reperire dal basso finanziamenti per progetti, startup e iniziative di vario genere. Con l'avvento dell'architettura blockchain e delle valute digitali, questo sistema è andato incontro a una vera a propria rivoluzioni. Grazie ai principi su cui si basano le Distributed Ledger Technology è possibile effettuare transazioni sicure e verificate affidandosi non a un ente centrale come una banca ma a una vasta rete di nodi ciascuno dei quali mantiene una sorta di libro contabile di tutte le transazioni.

3.6.2 Come funziona su piattaforma blockchain

Attraverso la creazione di un sito web che lavora su piattaforma blockchain, start up e PMI innovative possono ricercare potenziali investitori che, in cambio di finanziamenti, ottengono quote societarie dell'impresa. Questo procedimento permette agli investitori di ricevere dividendi dai futuri ricavi generati dall'attività e un ritorno sull'investimento in caso di vendita delle quote. La quota di partecipazione societaria viene calcolata sulla base della somma investite, non esiste un limite massimo ma solo un investimento minimo fissato dalla start up. Qualora la campagna di raccolta non raggiunga il target necessario per avviare il progetto, l'importo versato sarà restituito agli investitori, senza alcun costo. Il tutto è regolato da uno smart contract che in automatico gestisce la compravendita e l'eventuale restituzione delle somme dovute.

3.6.3 Rischi e vantaggi

Esistono sicuramente dei rischi in questo tipo di attività. Queste imprese in quanto start up non hanno una storia alle spalle e quindi hanno profili finanziari ad alto rischio, inoltre, in questo tipo di operazione, vengono trattati degli strumenti finanziari non gestiti su mercati regolamentati e quindi difficili da vendere. E' bene ricordare, infine, che nel caso delle start-up, per i primi 5 anni la società non può dividere gli utili tra i soci.
Ci sono però anche dei vantaggi, soprattutto fiscali, le persone fisiche hanno diritto ad una detrazione dall'IRPEF pari al 30% mentre le persone giuridiche godono di una deduzione dal reddito ai fini IRES del 30%.

3.7 CAMPI DI APPLICAZIONE DI UNA BLOCKCHAIN

Come evidenziato più volte nel corso di questa guida, la tecnologia blockchain si configura sempre di più come un sistema di base che ha il potenziale di effettuare una vera a propria trasformazione degli obsoleti modelli di business fino ad ora utilizzati. Vediamo alcuni esempi di applicazione:

- **banche e finanza**: l'assenza di intermediari nelle transazioni e nei pagamenti digitali azzera i costi delle commissioni;
- **assicurazioni**: prevenire frodi e riduzione dei costi delle piattaforme di gestione velocizzando contemporaneamente i processi di liquidazione;
- **sanità**: creazione di un database sul paziente facilmente consultabile dal personale sanitario;
- **pubblica amministrazione**: immediato accesso ai dati con il conseguente abbattimento dei tempi burocratici;
- **gestione delle risorse umane**: possibilità di creare un database unico che raccoglie tutte le precedenti esperienze che conferisce la possibilità di verificare i curricula;
- **agrifood**: verificare la certificazione dei prodotti agricoli e la tracciabilità e facilitare i processi logistici;
- **automotive**: tracciare il prodotto, verificare lo stato di salute di un'auto usata in vendita, combattere la contraffazione dei pezzi nei centri di assistenza;
- **industria 4.0**: ottimizzazione della produzione e della logistica e sicurezza della fiera produttiva;
- **IoT**: possibilità di facilitare l'interconnessione degli oggetti tra di loro e rendere lo scambio più veloce e sicuro;
- **diritto d'autore e copyright**: transazione di acquisto di brani musicali su piattaforme di servizi sicure e regolate da smart contract direttamente connesse con il pagamento di diritti d'autore.

4. CONCLUSIONI

La tecnologia blockchain può veramente cambiarci la vita? La risposta è sì e lo sta già facendo. La blockchain ci permette di raggiungere dei livelli di trasparenza, sicurezza e immutabilità che ad oggi nessun altro strumento è in grado di fare. Una fiducia nata dal basso che si rivolge a tutti, fondata sul principio della condivisione e capace di eliminare quei poteri centrali che negli anni hanno deluso le aspettative. La sua versatilità anche nei settori lontani dal finance ne decretano la sopravvivenza e il successo. La tecnologia blockchain sta influenzando i settori economici di tutto il mondo anche perchè in grado di risolvere problematiche aziendali di vario genere. Andando oltre alla sola applicazione dei pagamenti decentralizzati, la blockchain sta pian piano automatizzando tutti i processi aziendali anche grazie all'utilizzo degli smart contract.

Questa tecnologia ha preparato il terreno all'Internet of Value, inteso come scambio di valore in senso ampio e non solo monetario, ponendosi come sua struttura di riferimento e ha spalancato le porte al futuro, gettando le basi a nuove sfide, attirando talenti, sviluppando nuove idee di business e sradicando i vecchi paradigmi sociali.

STUDIO MARTELLI
& PARTNERS S.p.A.

Lo Studio Martelli & Partners nasce nel 1959 con l' Avvocato Domenico Martelli.
Oggi ha sedi operative a Roma, Milano e Napoli e un ufficio di rappresentanza a Dubai. Strutturato secondo il modello della Law Firm anglosassoni vanta una forte specializzazione in ambito fiscale e societario. Nel 2002 sotto la guida dell'avvocato Giovanni Battista Martelli amplia la propria attività nel settore della consulenza aziendale, nell'area Litigation e ADR e nell'internazionalizzazione con focus sul Middle East North Africa.
E' uno dei primi studi legali a operare nel ramo del Fashion Law, Cyber Law e Blockchain.

Come lavoriamo

Lo Studio Martelli & Partners S.p.A. ha deciso di lavorare su success fee o percentage fee, in base al risultato ottenuto, per quanto riguarda l'implementazione del business aziendale, collaborando in stretto contatto con l'azienda sino al raggiungimento dell'obiettivo.

Cosa facciamo

La mission dello Studio è quella di fornire un'assistenza professionale, competente ed efficiente, attenta alle esigenze reali del Cliente. Le competenze specialistiche in materia fiscale, societaria e l'esperienza maturata ci consentono di fornire consulenze ed elaborare strategie di managing aziendale ad hoc improntate al carattere dell'eccellenza. L'accuratezza e la personalizzazione del servizio offerto, fa dello Studio Martelli & Partners S.p.A. non un semplice studio legale e di consulenza, bensì una boutique del diritto.

I NOSTRI **SERVIZI**

Cyber Law

Con il concetto di Cyber Law si vuole indicare l'insieme di leggi e norme che regolano i rapporti tra i fornitori di apparecchiature e servizi informatici da una parte e gli utenti finali dall'altra. La Cyber Law ha un vasto ambito di applicazione, tra cui:

- **la tutela della cosiddetta "proprietà intellettuale" e del diritto d'autore;**
- **della sicurezza informatica (cracking, privacy e spamming);**
- **del commercio elettronico;**
- **dei principi che, tra certi Stati, possono regolare l'esportazione di hardware e software;**
- **dei diritti che maturano gli acquirenti di token e criptovalute e i fruitori delle tecnologie blockchain;**
- **della corretta fiscalità da applicare ai nuovi paradigmi del profitto digitale.**

In attesa di una armonizzazione delle diverse legislazioni, al fine di garantire la certezza del diritto ed evitare disparità di trattamenti, lo Studio Martelli & Partners S.p.A., ha acquisito la necessaria esperienza per gestire con sicurezza e successo tutti i settori del diritto (nazionale ed internazionale) riguardanti il Web sotto qualsivoglia profilo, civile, contrattuale, societario e penale.

Blockchain, ICO - STO e Smart Contract

Lo Studio Martelli & Partners S.p.A. ha acquisito il necessario expertise per supportare le imprese o le start up nella realizzazione di progetti innovativi su piattaforma Blockchain come ad esempio le ICO e STO.
Nello specifico lo Studio si occupa di:

- **valutare i progetti da lanciare in ICO e STO e valutare l'applicabilità su piattaforma blockchain anche attraverso la specifica applicazione di "smart contracts";**
- **supporta gli investitori nella due – diligence tecnico – giuridica dei "White papers", al fine di orientare un investimento sicuro;**
- **individuare la tipologia di token adatti per il lancio di nuove ICO e STO;**
- **supportare potenziali investitori, privati o istituzionali, nella due diligence, acquisto e gestione connessi ai token;**
- **garantire sicurezza di realizzazione del progetto, sia per l'imprenditore, che per l'investitore, attraverso l'applicazione di strumenti giuridici ad hoc.**

CONTATTI

Milano
ITALIA

Via Montebello 24
20121 - Milano
Tel. +39 02 94437658
Fax: +39 02 89356036

Roma
ITALIA

Viale delle Milizie 4
00192 - Roma
Tel. +39 06 86329688
Fax: +39 06 86211319

Napoli
ITALIA

Via Porzio, 4
(Centro Direzionale Napoli)
Isola G8
80143 NApoli
Tel 081.19757626
Fax 081.19758049

Dubai
UAE

Level 28,
Al Habtoor Business Tower
P.O. Box 29805
Tel. +971 4 453 2684
Fax: +971 4 453 2674
Mobile: +971 50 8545367

www.studiomartelli.it
info@studiomartelli.it

progetto editoriale e grafico Studio Martelli & Partners S.p.A.