ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CATANZARO

Gli Speciali de Il Giornale dell'Ingegnere

Blockchain: dal Bitcoin alla Pubblica Amministrazione la rivoluzione democratica del registro distribuito

Fernando Virone

Gli Speciali de Il Giornale dell'Ingegnere

Testi a cura di
Fernando Virone,
Dott. Ing. Esperto Aziendale ICT

Sommario


BLOCK
CHAIN

Prefazione

Sarà che la sua paternità è troppo ingombrante, sarà che se ne parla sempre con una certa diffidenza, forse legata ad alcuni pregiudizi di fondo, sarà che pochi tra i non addetti ai lavori l'hanno sperimentato concretamente, ma la realtà è che il termine "blockchain" continua a essere un illustre sconosciuto in un mondo in cui le nuove frontiere tecnologiche vengono varcate senza troppi riguardi, e i nuovi strumenti vengono acquisiti e metabolizzati in tempo reale dalle comunità di riferimento (consumatori, produttori, investitori, etc.).

Se oggi riteniamo che l'argomento sia meritevole di attenzione è dovuto al fatto che ormai la blockchain è uscita dal recinto della sperimentazione e sia avvia ad acquisire quelle credenziali di natura normativa che le consentiranno l'ingresso in alcuni ambiti finora inviolabili, oltre a dotarsi di standard internazionali che permetteranno l'interoperabilità tra le varie piattaforme applicative già realizzate, nonché, soprattutto, lo sviluppo di progetti di respiro internazionale.

Questo opuscolo non intende addentrarsi in aspetti squisitamente tecnici, di stretto interesse solo per gli addetti ai lavori, ma punta principalmente a descrivere la blockchain come nuovo paradigma tecnico-culturale, evidenziandone i forti aspetti innovativi, che possono portare non solo a uno sviluppo significativo di piattaforme applicative distribuite, ma addirittura a stravolgere i concetti di autorità, controllo e fiducia, per come siamo abituati oggi a considerarli.

Attraverso qualche semplice caso concreto, vedremo lo stato dell'arte del suo cammino normativo, per concludere con le prospettive di crescita e i probabili principali ambiti di applicazione.


BLOCK 01
BLOCK 01
NODE 01

Prima parte

Che cos'è la blockchain

Ci sono tante definizioni di *blockchain*, alcune piuttosto astruse, altre troppo tecniche, altre ancora troppo *filosofiche,* ma se vogliamo veramente capire di cosa si tratta dobbiamo partire da cosa *non è*: innanzitutto non è una tecnologia, ma è legata ad aspetti tecnologici imprescindibili, alcuni originali, altri già applicati in altri ambiti. Queste tecnologie cooperano in modo originale per realizzare il paradigma *blockchain*, che – diciamolo subito – non è finalizzato solo al mondo del Bitcoin o di altre criptovalute, ma è applicabile a una varietà di ambiti caratterizzati da alcuni obiettivi comuni.

Noi partiremo dalla base tecnologica del fenomeno, dicendo che la blockchain è un *registro digitale* strutturato come una *catena di blocchi* (da cui il nome) contenenti le transazioni e la cui validazione è affidata a un meccanismo di *consenso.* Le principali caratteristiche delle tecnologie alla base della blockchain sono:

- Immutabilità del registro
- Trasparenza
- Tracciabilità delle transazioni
- Sicurezza basata su tecniche crittografiche

La blockchain, per definizione, quindi, è basata su una Rete (privata o pubblica), in quanto deve permettere la gestione di una base dati distribuita. Dal punto di vista operativo è un'alternativa agli archivi centralizzati e permette di gestire l'aggiornamento dei dati con la collaborazione dei partecipanti alla Rete e con la possibilità di avere dati condivisi e accessibili, distribuiti presso tutti i partecipanti. Di conseguenza, la blockchain **permette una gestione dei dati in termini di verifica e autorizzazione senza che sia necessaria un'autorità centrale.**

Si comprende, da queste poche righe, che siamo quindi di fronte a un fenomeno che impatta sugli aspetti nevralgici dei meccanismi di governo dei sistemi digitali su cui si basa la nostra società e sui quali forse poco si riflette. L'ottica rivoluzionaria con cui la blockchain si pone rispetto alle logiche di controllo dei grandi sistemi digitali ha fatto

sì che i suoi sostenitori la definiscano come la *nuova generazione di Internet,* in quanto rappresenterebbe una sorta di **Internet delle transazioni,** che si affianca alla ben nota **Internet delle persone** (*Internet of People*), che frequentiamo ogni giorno e che si è orma estesa alla **Internet delle cose (***Internet of Things, IoT*), per arrivare a rappresentare l'**Internet del Valore** sulla base di sette caratteristiche:

1. Decentralizzazione
2. Trasparenza
3. Sicurezza
4. Immutabilità
5. Consenso
6. Responsabilità
7. Programmabilità

Partendo da questi principi, la blockchain è diventata la declinazione in digitale di un *nuovo concetto di fiducia,* assumendo, pertanto, un valore di natura sociale e politico, in quanto può essere vista come una piattaforma che consente lo sviluppo e la concretizzazione di una nuova *forma di rapporto sociale.*

Questa nuovo approccio, grazie alla partecipazione di tutti, è in grado di garantire a tutti la possibilità di verificare, di controllare, di disporre di una **totale trasparenza sugli atti e sulle decisioni,** che vengono registrati in archivi che hanno la caratteristica di essere **inalterabili, immodificabili** e dunque **immuni da corruzione.**

Paragrafo 1

Blockchain e blockchain, un po' di storia

È inutile girarci intorno, quando si parla di blockchain bisogna fare i conti con il Bitcoin. Tutti sanno che il progetto Bitcoin ha eletto le tecnologie che oggi chiamiamo *blockchain* come piattaforma di supporto al rilascio e scambio della criptovaluta che avrebbe dovuto rivoluzionare il mondo finanziario. Non intendiamo addentrarci nel terreno minato del bitcoin, né valutarne lo stato attuale né tantomeno le prospettive future, ma dobbiamo riconoscere a questo incredibile progetto il merito di aver lanciato e, soprattutto, stressato, le tecnologie che concorrono al funzionamento della blockchain. Oggi il diritto di primogenitura del Bitcoin è sancito dalla regola non scritta, ma accettata universalmente, che stabilisce che la *Blockchain* (quella con la B maiuscola) è il complesso di regole e tecnologie associate al progetto Bitcoin, mentre la *blockchain* (con la B minuscola) è il paradigma che si applica a *tutto il resto.*
Come tutti gli standard che raggiungono un'affermazione universale, è necessario un lungo periodo di gestazione per *convincere* la comunità scientifica, ma soprattutto gli organismi internazionali preposti a normare e uniformare metodologie e tecnologie, per sancirne l'adottabilità globale, che rappresenta l'anticamera del livello legislativo.
Come già accennato, la tecnologia a blocchi ha avuto la sua vera nascita ed un vertiginoso sviluppo in concomitanza con il decollo del progetto Bitcoin. In estrema sintesi, Bitcoin (in codice, BTC) è una criptovaluta e un sistema di pagamento mondiale creato nel 2009 da un anonimo inventore, noto con lo pseudonimo di **Satoshi Nakamoto**, che sviluppò un'idea da lui stesso presentata su Internet a fine 2008.
A differenza delle valute tradizionali, Bitcoin non fa uso di un ente centrale né di meccanismi finanziari sofisticati, il valore è determinato unicamente dalla leva della domanda e dell'offerta: esso utilizza un database distribuito tra i nodi della rete che tengono traccia delle transazioni, ma sfrutta la crittografia per gestire gli aspetti funzionali, come la generazione di nuova moneta e l'attribuzione della proprietà dei bitcoin.
La rete Bitcoin consente il possesso e il trasferimento anonimo delle monete; i dati necessari a utilizzare i propri bitcoin possono essere salvati su uno o più personal computer o dispositivi elettronici, quali smartphone, sotto forma di *portafoglio digitale*, o mantenuti presso terze parti che svolgono funzioni simili a una banca. In ogni caso, i bitcoin possono essere trasferiti attraverso Internet verso chiunque disponga di un *indirizzo bitcoin*. La struttura paritaria (*peer-to-peer*) della rete Bitcoin e la mancanza di un ente centrale rende impossibile a qualunque autorità, governativa o meno, il blocco dei trasferimenti o il sequestro di bitcoin senza il possesso delle relative chiavi, o la svalutazione dovuta all'immissione di nuova moneta.
Lungi dal volerci addentrare nelle logiche di Bitcoin, argomento di ambito finanziario, ma anche socio-politico nonché purtroppo speculativo (nella peggiore accezione), qui ci preme sottolineare che, molto probabilmente, senza il progetto Bitcoin la blockchain non sarebbe mai nata, per lo meno come si è venuta a strutturare oggi.

Paragrafo 2

A cosa serve la blockchain: gli asset digitali unici

La blockchain ha caratteristiche molteplici e di grande impatto sugli ambiti nei quali può essere applicata. Più avanti vedremo una parte di tali campi di applicazione, ma qui riteniamo fondamentale focalizzarci sulla soluzione che la blockchain offre al problema dell'*unicità degli asset digitali,* che può essere ritenuto il problema chiave dell'immateriale mondo del digitale.

Un **asset digitale** è un bene immateriale che può essere identificato e memorizzato su un dispositivo digitale, ad es. un documento Word. Quando noi scriviamo un testo su un documento Word quel testo è sul nostro computer ed è univoco. Ma nel momento in cui lo inviamo a un collega, quello stesso testo, oltre che sul nostro computer, sarà presente su un server di posta e sul computer del nostro collega, generando, pertanto, una serie di duplicazioni dello stesso documento. Quel testo poi potrà naturalmente essere condiviso a sua volta e inviato ad altri soggetti che ne avranno a loro volta una copia. Come è noto, non ci sono limiti a questa duplicazione e, inoltre, quello stesso documento può essere modificato infinite volte. Il nostro documento word è un *asset* digitale e non è certo unico: è partito dal nostro computer e in pochissimo tempo si è moltiplicato in migliaia di copie. Ma quello stesso asset, crittografato in un registro (*ledger*) blockchain, potrebbe diventare un asset **unico**. Esattamente come nel mondo fisico: se passiamo lo stesso documento scritto in word stampato su carta a un collega ne perdiamo il possesso, quel documento esce dal nostro controllo per entrare nel dominio di un collega. In altre parole: se nel mondo digitale il passaggio implica automaticamente una duplicazione, la blockchain consente di riconquistare al mondo digitale il concetto di **scarsità dei beni del mondo reale** e, nel momento in cui, tramite la blockchain, si passa un asset digitale (il nostro documento) dal nostro computer a un collega, quel documento non è più in alcun modo sotto il **nostro possesso** ed è totalmente in capo al nostro collega. Se anche lui avrà la necessità di condividerlo ne perderà il possesso in favore di un altro soggetto. **Il documento resterà unico e non sarà possibile duplicarlo.** Concludendo, la blockchain ha la capacità di **creare asset digitali unici** e quindi una delle sue naturali vocazioni è quella di **garantire l'unicità e originalità di documenti ufficiali**, azzerandone la contraffabilità e la necessità di ricorrere all'autorità di un ente garante**.**

Ma se appare chiara l'importanza di garantire l'unicità e immutabilità di un documento digitale, quando il bene digitale diventa una valuta, la sua unicità diventa un *must* assoluto. Ecco perché il mondo della finanza ha compreso per prima il valore della blockchain nel garantire l'unicità di un asset digitale, e tantissimi altri settori che stanno fornendo prodotti e servizi digitali hanno fatto proprio il paradigma blockchain, in quanto in grado di impedire duplicazioni. L'unicità dell'asset digitale avvicina il mondo dei beni digitali a quello dei beni reali, eliminando, pertanto, una delle principali carenze dell'universo dei bit.

I Token

La possibilità di gestire asset digitali unici spalanca, a questo punto, un'infinità di opportunità, finora impensabili, legate alla possibilità di scambiare *valore* al di fuori dei canali tradizionali. Il concetto di *Token* è l'incarnazione di questo nuovo modo di condividere beni e servizi, basato sulle garanzie offerte dalla blockchain. Un token è un asset digitale basato sulla blockchain che può essere scambiato tra due parti senza che sia necessaria l'azione di un intermediario. Può essere visto come un insieme di informazioni digitali che è in grado di conferire un diritto di proprietà ad un soggetto sull'insieme stesso di informazioni che sono registrate su una blockchain e che possono essere trasferite tramite un protocollo condiviso. Il token può eventualmente incorporare anche altri diritti addizionali che, nel caso, sono governati da un sistema contrattuale, i cosiddetti **smart contracts**. Uno dei primi esempi di token è rappresentato dal bitcoin, ma in poco tempo ne sono apparsi tanti altri, alcuni partendo proprio dall'esperienza del bitcoin stesso, altri utilizzando nuovi modelli e nuovo codice come ad esempio la blockchain Ethereum.

Per capire meglio le potenzialità dei token e, soprattutto, come funzionano, si può utilizzare l'esempio dei gettoni della **SIP** (la *vecchia* compagnia telefonica). I gettoni telefonici servivano per ottenere un servizio molto concreto: la telefonata dalle cabine pubbliche. Il gettone era un token e aveva un valore di 50 lire. **L'emissione di token sul mercato ha lo scopo di ottenere un finanziamento che permette di usufruire di un servizio.** In questo modo la società ottiene delle risorse che può utilizzare senza contrarre nessun obbligo diretto nei confronti di chi ha effettuato gli investimenti, se non quello di rendere poi disponibile il servizio a chi sarà pronto a pagarlo con il proprio token, ovvero spendendo l'asset di valore che ha acquistato.

Il vecchio gettone della SIP, come il token, poteva essere scambiato in ragione del suo valore intrinseco. Un gettone SIP aveva un valore riconosciuto di 50 Lire che i negozianti accettavano perché avevano la certezza di rimettere in circolazione quella moneta che di fatto era un asset di valore. Dunque, il gettone, nato per l'erogazione di un servizio (la telefonata dalle cabine pubbliche) era diventato un asset utilizzato anche per la gestione di piccole transazioni.Se la società titolare del servizio e protagonista dell'emissione decideva, legittimamente, che il valore della telefonata non era più assimilabile a un gettone di 50 Lire bensì a un valore di 100 Lire e, conseguentemente, aumentava il valore del gettone, ecco che chi aveva acquistato un certo numero di gettoni (non per un investimento, ma in previsione di fare molte telefonate) si trovava ad avere lo stesso valore in termini di quantità di servizi telefonici, ma un valore raddoppiato in termini di asset di valore da utilizzare sul mercato come moneta di scambio.

I token digitali sono assimilabili, nel nostro esempio, ai gettoni della SIP. Se chi lo emette promette di erogare un servizio che può essere acquistato grazie al token, si ritrova con un investimento fatto da soggetti che intendono utilizzare quel servizio o che credono nel valore di quel servizio al punto da acquisire tanti gettoni per utilizzare il servizio o per venderli ad altri che potranno utilizzarli. Se dietro al token non ci sono servizi il rischio è che si tratti solo di una nuova forma di investimento. In realtà, se il concetto alla base dei token è ben rappresentato dall'esempio precedente, la gestione concreta è molto più complessa, in quanto legata in particolare alla valutazione del valore effettivo offerto da chi li emette. Qui ci limiteremo, per dare un'idea del fenomeno, a dire che esistono diverse tipologie di token determinate sia dal tipo di approccio tecno-

logico sia dal tipo di utilizzo. In particolare, è importante focalizzare l'attenzione su tre diverse tipologie di token determinati dal tipo di diritti gestiti dai token stessi:

Token di classe 1 – il token si presenta come una una vera e propria *moneta, non prevede* ***nessuna controparte*** *e* può essere trasferito tramite transazioni su blockchain. Il token è anche una garanzia della non modificabilità delle transazioni stesse. Si tratta di una tipologia di token che non conferisce diritti nei confronti di una controparte, ma ha la funzione di registrare un diritto di proprietà del token stesso o l'esistenza di un determinato soggetto/oggetto. Con questo tipo di token il proprietario non ha diritti ulteriori rispetto a quelli correlati alla proprietà del token stesso. Fanno parte della categoria dei Token di classe 1 i token di criptovalute come **Bitcoin**, **Bitcoin Cash**, **Litecoin**, ecc.

Token di classe 2 – in questo caso si tratta di token che sono in grado di conferire ai proprietari dei diritti che possono essere esercitati nei confronti del soggetto che ha generato i token o, eventualmente, nei confronti di terzi. Si tratta di token che dunque permettono di esercitare **diritti verso delle controparti.** In parole diverse si potrebbe dire che i **token di classe 2** potrebbero essere definiti come una sorta di titoli di credito, ossia di documenti che (*secondo l'art. 1992 c.c.*) conferiscono al possessore *diritto alla prestazione in esso indicata verso presentazione del titolo*. Come nella realtà quotidiana possono essere i *titoli obbligazionari o di prestito, i titoli di partecipazione, i titoli rappresentativi di merci e documenti di legittimazione.* Ad esempio, possiamo citare:

1. **Token per smart contract relativi alla gestione di pagamenti futuri** – con il conferimento di un diritto a ricevere dei pagamenti futuri, sulla base di determinate condizioni stabilite a livello contrattuale che il token è chiamato a gestire in modo automatico;
2. **Token come asset –** in questo caso il token rappresenta una sorta di diritto di proprietà di un determinato asset (sia materiale sia immateriale) e ad esempio potrebbe anche rappresentare quote di partecipazione dell'entità giuridica emittente o di entità terze.
3. **Token utilizzati per pagamenti standardizzati –** in cui una persona vanta il diritto di ricevere un pagamento per un importo specifico ben definito;
4. **Token per la gestione di prestazione di servizi –** in questa circostanza il titolare del token vanta il diritto di ricevere una determinata prestazione o nel caso anche un bene dal soggetto emettitore o da un terzo che abbia sottoscritto un accordo commerciale. Si tratta ad esempio di token che regolano l'accesso a infrastrutture informatiche, all'erogazione di servizi e che possono anche avere le caratteristiche di una criptovaluta nativa.

Token di classe 3 – Si tratta in questo caso di token che possono svolgere una funzione mista. Sono token che rappresentano **diritti di comproprietà** ovvero che rappresentano una proprietà ma conferiscono anche diritti diversi, come ad esempio il diritto di voto, o diritti di tipo economico per i rappresentanti legali o o soci di una società, ecc. In questa tipologia di token il titolare non ha un diritto esercitabile direttamente verso l'emittente del titolo o verso un terzo.

Smart Contracts

All'interno degli argomenti sopra trattati, abbiamo più volte fatto riferimento ai cosiddetti smart contracts, che rappresentano uno strumento importante e innovativo per regolare i rapporti tra soggetti che effettuano transazioni di compravendita o di altra natura tramite sistemi digitali basati sulla blockchain. Vediamo ora in dettaglio di cosa si tratta.

Gli ***Smart Contracts*** sono stati oggetto di sperimentazione già negli anni '90 quando le tecnologie ne hanno reso possibile una prima implementazione, ma l'idea di **Contratto Intelligente** risale in realtà alla metà degli Anni '70. All'epoca l'esigenza era molto semplice e atteneva alla necessità di gestire l'attivazione o disattivazione di una licenza software in funzione di alcune condizioni molto semplici. La licenza di determinati software venne di fatto gestita da una chiave digitale che permetteva il funzionamento del software se il cliente aveva pagato la licenza e ne cessava il funzionamento alla data di scadenza del contratto.

Lo Smart Contract, che possiamo definire *un contratto automatico che si attiva a fronte di determinate condizioni,* ha bisogno di un supporto legale per la sua stesura, ma non ne ha bisogno per la sua verifica e per la sua attivazione. Lo **Smart Contract fa riferimento a degli standard di comportamento e di accesso a determinati servizi** e viene messo a disposizione, accettato e implementato anche come forma di sviluppo di servizi tradizionali. Uno Smart Contract è la *traduzione* o *trasposizione* in *codice* di un contratto in modo da verificare in automatico l'avverarsi di determinate condizioni (*controllo di dati di base del contratto*) e di *autoeseguire* in automatico azioni (*o dare disposizione affinché si possano eseguire determinate azioni*) nel momento in cui le condizioni determinate tra le parti sono raggiunte e verificate. In altre parole, lo Smart Contract è basato su un codice che *legge* sia le clausole che sono state concordate sia la condizioni operative in base alle quali devono verificarsi le condizioni concordate e si *autoesegue* automaticamente nel momento in cui i dati riferiti alle situazioni reali corrispondono ai dati riferiti alle condizioni e alle clausole concordate.

E proprio perché **l'assenza di un intervento umano corrisponde anche all'assenza di un contributo interpretativo,** lo Smart Contract deve essere basato su descrizioni estremamente precise per tutte le circostanze, tutte le condizioni e tutte le situazioni che devono essere considerate. Ecco che la gestione dei dati diventa un fattore critico essenziale per stabilire la qualità dello Smart Contract.

Nello stesso tempo per gli Smart Contract è fondamentale definire in modo estremamente preciso le fonti di dati alle quali il contratto è chiamato ad attenersi. **Gli Smart Contract sono chiamati a ricevere dati e informazioni che vengono definite e certificate dalle parti nel contratto stesso** e che devono essere individuate, controllate, lette e interpretate dallo Smart Contract

sulla base di **precise regole** che, a loro volta, rappresentano una delle parti più rilevanti e strategiche del contratto in quanto determinano ovviamente l'output finale.
E qui viene il punto più rilevante relativo alle differenze sostanziali tra contratto tradizionale e Smart Contract. **Lo Smart Contract è di fatto figlio dell'esecuzione di un codice da parte di un computer**. È un programma che elabora in modo deterministico (*con identici risultati a fronte di identiche condizioni*) le informazioni che vengono raccolte. *In altre parole, se gli input sono gli stessi i risultati saranno identici.* Questo punto è estremamente rilevante perché, se da una parte rappresenta una certezza e una sicurezza in quanto garantisce alle parti una assoluta **certezza di giudizio oggettivo,** escludendo qualsiasi forma di interpretazione, *dall'altra sposta sul codice, sulla programmazione, sullo sviluppo il peso e la responsabilità o anche il potere di decidere.*
Ai contraenti spetta il compito di definire condizioni, clausole, modalità e regole di controllo e azione, ma, una volta che il loro contratto è diventato codice e dunque uno Smart Contract e i contraenti lo accettano, **ecco che gli effetti non dipendono più dalla loro volontà**.
Tra i tanti possibili esempi, citiamo quello che proviene dal mondo delle assicurazioni per autoveicoli, che, sulla base di dati rilevati grazie ad apparecchiature IoT a bordo delle vetture, sono in grado di fornire dati sul comportamento del conducente che possono influire e creare determinate condizioni che attivano o disattivano clausole di vantaggio o svantaggio. Ad esempio, il superamento di limiti di velocità determinati dal contratto può essere interpretato come una condizione di maggior pericolo e determinare un cambiamento contrattuale delle condizioni applicate, ad esempio, nel valore del premio assicurativo.
Un altro esempio arriva dal mondo dei media dove con i **Digital Rights Management** viene gestita la erogazione e l'accesso a determinati servizi multimediali.

Seconda parte

Governance della blockchain

Ora che abbiamo cominciato a familiarizzare con gli aspetti chiave della blockchain, siamo pronti ad affrontare l'argomento che rappresenta il principale oggetto di dibattito tra gli addetti ai lavori e i portatori di interesse (i cosiddetti *stakeholders*) che dovrebbero sposare il progetto blockchain come strumento di innovazione tecnologica e organizzativa sicuro e affidabile: *chi governa la blockchain?* Abbiamo accennato che la blockchain è assimilabile ad un libro mastro distribuito, che, a differenza di quello centralizzato, non è gestito da un'autorità centrale che fa da garante verso tutti gli interessati, bensì è gestito da tutti coloro che ne condividono l'utilizzo in rete, ed è modificabile solo previo consenso di tutti gli utenti. Fermo restando questo principio comune, è però necessario operare un netto *distinguo*, sotto il profilo della *gover*nance, tra le due tipologie di blockchain oggi adottabili:

- **Blockchain pubbliche** *(permissionless ledger)*
- **Blockchain private** *(permissioned ledger)*

Le Blockchain pubbliche, di cui l'esempio più famoso e diffuso è rappresentato dalla Blockchain Bitcoin, sono aperte, non hanno una proprietà o un attore di riferimento e sono concepite per non essere controllate. L'obiettivo delle Permissioneless Ledger è quello di permettere a ciascuno di contribuire all'aggiornamento dei dati sul registro e di disporre, in qualità di partecipante, di tutte le copie immutabili di tutte le operazioni. Ovvero di disporre di tutte le copie identiche di tutto quanto viene approvato grazie al consenso. Questo modello di blockchain impedisce ogni forma di censura, nessuno è nella condizione di impedire che una transazione possa avvenire e che possa

essere aggiunta al Ledger una volta che ha conquistato il consenso necessario tra tutti i nodi (partecipanti) alla blockchain.
Le Permissionless Ledger possono essere utilizzate come database globale per tutti quei documenti che hanno la necessità di essere assolutamente immutabili nel tempo, a meno di aggiornamenti che richiedono la massima sicurezza in termini di consenso, come ad esempio i contratti di proprietà o i testamenti.
Le **Blockchain private** possono invece essere controllate e dunque possono avere una proprietà. Quando un nuovo dato o record viene aggiunto, il sistema di approvazione non è vincolato alla maggioranza dei partecipanti alla blockchain, bensì a un numero limitato di attori che sono definibili come **Trusted**. Questo tipo di blockchain può essere utilizzata da istituzioni, grandi imprese che devono gestire filiere con una serie di attori, imprese che devono gestire fornitori e subfornitori, banche, società di servizi, operatori nell'ambito del Retail. In questo caso le **Permissioned Ledger** rispondono alle necessità di un aggiornamento diffuso su più attori che possono operare in modo indipendente, ma con un **controllo limitato** a coloro che sono **autorizzati**. Le Permissioned Ledger permettono poi di definire **speciali regole per l'accesso e la visibilità di tutti i dati**. In altre parole le Permissioned Ledger introducono nella blockchain un concetto di Governance e di definizione di regole di comportamento. Tecnicamente le Permissioned Ledger sono anche più performanti e veloci delle Permissionless Ledger.

Paragrafo 1

Prospettive e ambiti applicativi della blockchain

Come ampiamente argomentato, la blockchain ha ormai superato i confini del Bitcoin. La moneta virtuale è infatti solo una delle sue possibili applicazioni. Priva di gestione centralizzata, infatti, la blockchain permette di inviare qualsiasi dato in maniera sicura, tagliando drasticamente la catena degli intermediari, e permettendo quindi uno scambio di dati sicuro tra due persone, senza dover utilizzare mezzi di terze parti quali ad esempio un provider di posta elettronica, oppure un servizio di Cloud Computing esterno.
Si è parlato molto di blockchain anche in occasione del *World Economic Forum* e sono molti gli investitori che stanno puntando ad altri investimenti in ambito blockchain, e quindi, dagli investimenti iniziali che ci sono stati soltanto nella nuova valuta e in nuovi sistemi di pagamento, si passa finalmente a nuovi investimenti, in settori nuovi e diversi tra loro. Proviamo quindi a passare in rassegna i principali tra i nuovi ambiti applicativi della Blockchain in Italia e nel mondo.

1) Blockchain in Finanza e Banche
La Finanza e l'Economia sono sicuramente tra i settori presi più di mira dagli investitori in relazione alla blockchain. Infatti, non essendoci intermediari a gestire le transazioni, la blockchain abbatterebbe i costi delle commissioni delle banche, permettendo risparmi, velocità e affidabilità delle transazioni. Diventa quindi fondamentale investire in questa nuova tecnologia per banche e istituti finanziari, che cercano di accaparrarsi una fetta abbastanza grande di questo nuovo mercato, che rivela già da subito innumerevoli possibilità e opportunità.

2) Blockchain nelle Assicurazioni
Nel settore assicurativo le prospettive di adottare strumenti basati sulla blockchain sono molto allettanti e sono già in corso varie sperimentazioni:
ad es., l'accesso a transazioni sicure e decentralizzate fornisce una base solida per prevenire le frodi, per garantire una maggiore governance, per avere dati e reportistiche migliori. Grazie alla blockchain, inoltre, le assicurazioni possono avere notifiche aggiornate e accurate in relazione ai cambiamenti, e ciò permette loro di migliorare la gestione del rischio e massimizzare le opportunità di capitali e fondi, oltre alla possibilità di adottare strategie di Big Data, che sono molto utili per ottenere informazioni sicure sui propri clienti, sulle loro priorità e preferenze, oltre che eventuali ulteriori informazioni prese da terze parti.
Da un punto di vista tecnico, gli assicuratori vedono nella blockchain un'opportunità per integrare un ecosistema di terze parti affinché riducano i costi delle loro piattaforme di gestione, migliorando allo stesso tempo l'esperienza utente (customer experience) e la quota di mercato, e sviluppando nuove soluzioni e opportunità.
A livello di mercato, inoltre, gli assicuratori hanno opportunità nella governance delle loro aziende, attraverso un accesso ai dati migliorato, controlli di terze parti e sistemi più sofisticati di gestione del rischio, associati ai loro prodotti e servizi, come ad esempio le assicurazioni cibernetiche.

3) Blockchain nei Pagamenti digitali
Anche per quanto riguarda i Pagamenti digitali

ci sono grandi opportunità per la blockchain. Ovviamente ci sono ancora molti problemi che vanno affrontati, come ad esempio il tempo di elaborazione di una transazione, che è ancora piuttosto lento. Anche le performance del sistema andrebbero migliorate, per poter essere meglio assorbite dai pagamenti digitali, e allo stesso modo indicazioni normative chiare e un'analisi più attenta di minacce e opportunità sono le sfide della blockchain nel settore dei pagamenti digitali. Nonostante queste sfide, comunque, esistono tantissime opportunità per questa nuova tecnologia applicata ai pagamenti digitali, e probabilmente molto presto avremmo i primi riscontri dal mercato.

4) Blockchain nell'Agrifood

Nell'Agrifood la blockchain trova un ulteriore ottimo alleato. Alcune delle caratteristiche applicative della blockchain nell'Agrifood sono la tracciabilità, la trasparenza, per chi vuole raccontare la storia del proprio cibo, utilizzando la blockchain per garantire affidabilità. Altre aziende già oggi vogliono tracciare container e trasporti degli alimenti e del cibo in generale utilizzando la blockchain.

In particolare, i benefici della blockchain appaiono particolarmente importanti per l'industria di trasformazione e per tutte le attività e gli sviluppi legati alla certificazione alimentare. La blockchain consente di creare delle filiere aperte in cui tutti gli attori: produttori di materie prime, imprese che si occupano di logistica e trasporti, imprese che operano sulle materie prime a vari livelli di trasformazione, aziende che lavorano su packaging e marketing e infine il retail possono conferire dati e informazioni e controllare, con la massima trasparenza, i dati di tutti gli altri attori. E i dati relativi a ciascun prodotto possono essere messi a beneficio del consumatore finale. La blockchain in questo modo permette di creare delle filiere più aperte, più efficienti e più sicure.

5) Blockchain nell'Industria 4.0

Anche nel manifatturiero la Blockchain può essere un valido alleato. Grazie alla blockchain nell'Industria 4.0, infatti, è possibile sfruttare la logica decentralizzata della blockchain per produrre tecnologie in grado di supportare al meglio la produzione, logistica e Supply Chain, così come altre aree core dell'azienda. Inoltre, grazie alla blockchain, è possibile preservare il dato e la sicurezza del dato stesso, garantendo quindi sicurezza e affidabilità a tutto il processo della filiera produttiva e di distribuzione.

6) Blockchain nell'IoT

Anche *nell'Internet delle Cose* la blockchain trova una grande utilità: grazie alla sua facilità di scambio dati, infatti, la tecnologia blockchain potrebbe essere utilizzata per facilitare la comunicazione tra oggetti IoT connessi, oltre a rendere lo scambio di dati più sicuro e veloce. La blockchain è poi utilizzata come piattaforma per soluzioni che hanno lo scopo di gestire *l'identità delle cose*. Grazie alla corretta identificazione è possibile dare vita a soluzioni di certificazione delle filiere basate anche sui dati che arrivano dalle cose (IoT) e lavorare alla certificazione di supply chain. Uno degli esempi più significativi è quello della food supply chain. Oggi è importante rendere sempre più sicuro il riconoscimento end-to-end di oggetti virtuali o fisici, perché è con questi oggetti che si concretizza l'intermediazione delle persone stesse nelle transazioni. Sono cioè gli oggetti che, in definitiva gestiscono le transazioni. In determinati casi, sempre più frequenti, ci sono oggetti che hanno bisogno di farsi identificare senza che dietro ci siano delle persone. Dunque, se grazie alla blockchain, si riescono a identificare gli oggetti, avremmo un nuovo strumento

di identificazione, più sicuro, anche per le persone.

7) Blockchain nella Sanità

Per quanto riguarda blockchain e Sanità, gestire i dati medici dei pazienti attraverso un sistema condiviso, permetterebbe ai medici di condividere informazioni sui pazienti in maniera sicura e veloce, e quindi aiuterebbe molto la medicina e la sanità a migliorare il servizio fatto ai pazienti, con la possibilità di avere sotto controllo l'intera storia clinica di un paziente, in modo da somministrare cure migliori e in tempi più rapidi. La blockchain consente di dare vita a una organizzazione che realizza la vera centralità del paziente, insieme al coordinamento intelligente di tutte le azioni mediche che lo interessano. Considerando che i servizi sanitari sono erogati da strutture diverse con storie digitali molto diverse, la blockchain può aiutare a dare vita a un coordinamento intelligente di tutte le azioni grazie a una rivisitazione della gestione, dell'interoperabilità tra strutture e informazioni eterogenee. Le tecnologie blockchain, per loro natura, possono contribuire a dare risposte nuove in termini di interoperabilità progressiva fra sistemi informativi sanitari nazionali. La blockchain è anche una risposta in termini di *compliance* normativa (Gdpr, Nis Directive) in scenari complessi che devono gestire la presenza e la interazione tra sistemi sanitari interregionali, tra soggetti privati come possono essere i laboratori di analisi, le strutture della sanità privata o anche le assicurazioni.

8) Blockchain nella Pubblica Amministrazione

Anche nella Pubblica Amministrazione la blockchain trova un fertile ambito di applicazione. La blockchain, infatti, oltre a risolvere il problema della certificazione dei documenti ufficiali, cui abbiamo già accennato in precedenza, potrebbe infatti ad esempio aiutare la Pubblica Amministrazione e i cittadini ad avere una vera identità digitale, condivisa e implementata in questo sistema, con diversi vantaggi tra cui: rendere più difficile l'evasione fiscale, avere un controllo maggiore dei cittadini e quindi combattere la criminalità, servizi semplificati in tutti i settori della Pubblica Amministrazione (invio di dati semplificato), e molto altro. In ambito PA, è in atto un'avanzata sperimentazione nel campo dell'*e-voting,* il voto elettronico, che ha sempre manifestato notevoli problemi di sicurezza e che la blockchain, per le sue caratteristiche intrinseche, sembra in grado di superare.

9) Blockchain nel Retail

La blockchain sembra essere un modello interessante da utilizzare nei negozi e nel Retail: con la blockchain, infatti, gli attuali metodi di pagamento in negozio potrebbero essere estesi al Bitcoin, permettendo quindi ai clienti pagamenti molto più rapidi, oltre che più economici. Garantendo pagamenti più veloci ed economici, e quindi più convenienti, può essere offerto un servizio migliore al cliente, che quindi potrebbe dare un vantaggio competitivo agli store che decideranno per primi di abilitare queste nuove tecnologie nei loro punti vendita.

10) Blockchain nella musica

La gestione del copyright è da sempre uno dei temi più controversi e complessi nell'ambito del mercato discografico. Un mercato questo che prima e più di altri ha vissuto una vera e propria trasformazione dettata dal digitale. Si può anzi dire che si tratta di un mercato che di trasformazioni ne ha vissute ben più di una e dove il tema della remunerazione di tutti gli attori della filiera è stato da sempre a dir poco complicato. Lo scambio di brani musicali o la loro diffusione su larga scala, in assenza di una corretta remunerazione

per gli autori e per chi, come arrangiatori e musicisti, contribuivano alla realizzazione del prodotto musicale, ha fatto discutere e ha visto tentativi di ogni tipo. Grazie alla blockchain, agli smart contract e all'iniziativa di diverse startup è oggi possibile automatizzare la remunerazione, in quota parte, della filiera di autori e contributori ai brani musicali, a ogni nostra scelta d'acquisto. Il punto determinante resta racchiuso in quest'ultima parola: scelta d'acquisto. Si deve trattare di una transazione, ovvero dell'acquisto di un brano o della sottoscrizione di un servizio.

11) Blockchain e Smart Energy (Smart Grid)
La smart grid porta il concetto di rete intelligente nell'ambito dell'energia elettrica. Siamo abituati da sempre a utilizzare, come consumatori, l'energia elettrica. Non siamo certamente abituati a vivere questa dimensione come produttori, anche se sempre più spesso ci troviamo o possiamo trovarci ad esserlo. La rete elettrica non è un rapporto univoco dal produttore al cliente ma conta una molteplicità di possibilità a partire dal cittadino che produce mette a disposizione sulla rete la propria energia. Ma l'energia va prodotta quando serve o va utilizzata nel momento in cui se ne dispone in eccesso. In altre parole, serve una gestione intelligente della produzione e dei consumi. Le Smart Grid utilizzano piattaforme di analytics e di scambio per gestire nel modo più preciso possibile consumi e produzione e naturalmente per ridurre al massimo gli sprechi. La blockchain può svolgere un ruolo molto importante per la gestione delle transazioni in ingresso e in uscita con una modalità che permette di rendere più democratica la rete elettrica, ovvero una modalità che permette di gestire anche gli scambi tra coloro che hanno energia in eccesso e coloro che hanno necessità urgenti.

12) La blockchain per gli *Unbanked*
Una grande opportunità sia sul piano sociale sia sul piano del business è quella di dare una banca a chi non ha una banca, ovvero a chi non ha accesso a servizi bancari e finanziari. Stiamo parlando degli *unbanked*, del 31% della popolazione mondiale che in termini assoluti significa 1,7 miliardi di persone. Per gli istituti di credito alla ricerca di nuovo business parrebbe un Eldorado non fosse che questa volta agli unbanked non ci stanno pensando le banche bensì un nome che tutti ben conosciamo e che in condizioni normali faticheremmo non poco ad associare al mestiere di banca. Stiamo parlando di Facebook che è tra i promotori del progetto Libra, la associazione (The Libra Association) che si accinge da dare vita a una criptocurrency, **Libra**, che ha anche la missione di servire tutti coloro che non riescono oggi ad avere una banca e che domani potranno, grazie al proprio smartphone, pagare, spedire e ricevere denaro, nonchè gestire servizi finanziari.

Conclusioni

Al termine di questa rapida carrellata sul fenomeno blockchain, che, lo ribadiamo, non ambisce ad essere esaustiva né a formulare previsioni sulla sua evoluzione, ma solo a fotografare un treno in piena corsa, sottolineandone gli aspetti di maggiore impatto sulla società, proviamo a tirare qualche conclusione.

Innanzitutto, riteniamo importante sottolineare che la blockchain ha fatto il suo ingresso ufficiale nella legislazione italiana, che ha ritenuto di avviare la disciplina del complesso tema delle tecnologie basate sui registri distribuiti (DLT), sulla blockchain e sugli *smart contracts.* È dell'11 febbraio scorso la legge n. 12 di conversione del DL n. 135 del 14 dicembre 2018, recante disposizioni urgenti in materia di sostegno e semplificazioni per imprese e Pubblica Amministrazione, al cui interno è collocata una disposizione in materia di Registri Distribuiti. Nel dettaglio:

- Introduce nell'ordinamento la definizione di tecnologie basate su registri distribuiti
- Definisce cosa siano gli smart contracts equiparandoli ai contratti in forma scritta
- Equipara alla marca temporale il timestamp sulle DLT
- Dispone che AgID (l'Agenzia per l'Italia Digitale) ha il compito di individuare gli standard tecnici che le tecnologie blockchain devono possedere affinchè producano gli effetti giuridici di validazione temporale.

Si tratta solo di un punto di partenza, ma è una *bandierina* fondamentale piantata da questo paradigma, che, solo qualche anno fa, era visto ancora con sospetto, mentre oggi ha raggiunto una maturità tecnologica piuttosto importante e, soprattutto, dimostra una grande versatilità e adattabilità sul versante della *governance.* Certo, rimangono aperti molti problemi, solo per citarne alcuni: l'entità delle risorse di elaborazione necessarie e di conseguenza le performance dei servizi *blockchain based,* la sicurezza delle transazioni, i possibili conflitti con la protezione dei dati personali, l'uso dell'intelligenza artificiale negli *smart contracts,* ecc. Ma, a fronte di questi aspetti, che lasciano molti cantieri ancora aperti, la sensazione (molto vicina alla certezza) è che si sia già superato il punto di non ritorno e che, negli anni a venire, avremo sempre meno sperimentazioni e sempre più applicazioni nei tanti ambiti che abbiamo provato a delineare e in altri ancora.

Inoltre, la progressiva definizione di standard internazionali, in concomitanza con l'adozione di una legislazione di supporto, dovrebbe portare alla nascita di piattaforme internazionali che gestiranno problematiche condivise (alcune già in fase di sperimentazione) e, in ultima istanza, ad una maggiore interoperabilità dei sistemi informativi esistenti.

Concludiamo con un doveroso riferimento all'origine vera del fenomeno, cioè alla catena delle criptovalute: probabilmente stiamo entrando in una nuova fase, più matura e consapevole, in cui la speculazione pura potrebbe lasciare il posto ad un modo completamente innovativo di fare banca e gestire, in generale, i servizi finanziari. Ma l'esito finale di questo processo è condizionato dalla capacità dei cosiddetti *poteri forti* (cioè, di chi oggi detiene il controllo dei processi socio-economico-politici) di riuscire ad addomesticare e, in qualche modo, a neutralizzare l'aspetto più rivoluzionario del paradigma *blockchain,* e cioè la *governance condivisa.* Il rischio che si corre è quello di declassare la blockchain a pura tecnologia e di adottarla disinnescandone gli aspetti a forte impatto socio-economico. *Ma questa è un'altra storia....*