Capitolo I
BLOCKCHAIN E CRIPTOVALUTE

Sommario: **1.1.** Storia e funzionamento della tecnologia blockchain - **1.1.1.** Caratteristiche della blockchain - **1.1.2.** Tipologie di blockchain - **1.1.3.** Formazione del consenso - **1.2.** Aspetti pubblicistici e politiche legislative: tra regolamentazione e deregolamentazione - **1.3.** Token: funzioni e rappresentatività - **1.4.** Blockchain, Regolamento eIDAS e Codice dell'Amministrazione digitale - **1.4.1.** *Segue*. Valenza probatoria e rilevanza delle transazioni su blockchain - **1.5.** Rapporti tra la tecnologia blockchain ed il Regolamento UE n. 679/2016 sulla protezione dei dati personali - **1.5.1.** *Segue*. Soggetti, diritti ed obblighi nella blockchain alla luce del GDPR - **1.6.** Dall'Electronic Data Interchanges agli smart contract - **1.6.1.** Gli smart contract costituiscono un ordinamento autonomo? - **1.6.2.** Disciplina positiva degli Smart Contract: validità, rilevanza e soluzioni - **1.7.** Decentralized Autonomous Organization (DAO) - **1.8.** Decentralized AI: l'incontro tra blockchain ed intelligenza artificiale - **1.9.** Regolamentazione della blockchain - **1.9.1.** *Segue*. Norme positive in tema di blockchain e Distributed Ledger Technology - **1.10.** Applicazioni della blockchain - **1.11.** Criptovalute e legislazione: gli approcci internazionali - **1.12.** Regolamentazione italiana sulle criptovalute - **1.13.** Aspetti di mercato: Initial Coin Offering (ICO) - **1.13.1.** *Segue.* Un tentativo di ricostruzione della disciplina delle Initial Coin Offering

1.1. Storia e funzionamento della tecnologia blockchain

Usualmente quando si ricostruisce il fenomeno della tecnologia blockchain si fa riferimento al *paper* pubblicato sotto lo pseudonimo Satoshi Nakamoto intitolato «*Bitcoin: A Peer-to-Peer Electronic Cash System*»[1].

Questa pubblicazione, di sole nove pagine, ha posto le basi e teorizzato il primo sistema, ancora oggi il più diffuso, di pagamento *trustless* basato su tecnologia blockchain, unendo una serie di tecnologie già note, ma trovando soluzioni innovative ad alcuni problemi che nascono dalla realizzazione di un meccanismo di

[1] Reperibile su https://bitcoin.org/bitcoin.pdf, visitato il 5 agosto 2018.

pagamento distribuito tra persone distanti con eliminazione di un ente centrale a garantire la certezza dei pagamenti stessi.

In realtà, l'idea di uno strumento di pagamento virtuale risale al 1994, e quindi ben più di dieci anni prima del *paper* di Sakamoto, anno in cui viene creato DigiCash, servizio realizzato da David Chaum, in cui però era ancora necessario prevedere l'esistenza di un ente centrale con le funzioni di "stanza di compensazione" delle varie transazioni.

L'idea di assicurare l'anonimato delle transazioni all'interno delle reti telematiche deriva dal movimento cypherpunks, ossia da un gruppo di soggetti (inizialmente costituito da Eric Hughes, Tim May e John Gilmore) che crearono una mailing list sulla quale venivano discussi i temi della privacy e della cifratura dei dati. Nel 1993 viene pubblicato il «*Cypherpunk Manifesto*»[2]. Successivamente, nel 1997, viene proposto Hashcash da Adam Back, un sistema per evitare il fenomeno dello *spam* nella posta elettronica, rendendo computazionalmente oneroso inviare messaggi non desiderati, mentre nel 1998 Wei Dai pubblicava la sua proposta di B-money[3] con cui descriveva per primo un sistema decentralizzato di pagamento garantito dalla cifratura e dalla *c.d.* "*proof of stake*", ossia dall'incentivo dei partecipanti ad agire onestamente nel network potendo altrimenti perdere i fondi depositati in caso di validazione di transazioni fraudolente.

Negli stessi anni Nick Szabo propone la definizione di *smart contract*, vale a dire contratti intelligenti capaci di eseguire automaticamente delle transazioni.

---

[2] Reperibile su https://www.activism.net/cypherpunk/manifesto.html, visitato il 5 agosto 2018.

[3] Reperibile su http://www.weidai.com/bmoney.txt, visitato il 5 agosto 2018.

Nel 2004, Hal Finney, basandosi sui principi di Hashcash, teorizza la *proof of work* e nel 2005 Nick Szabo pubblica una proposta avente ad oggetto il *Bitgold*, con alla base l'idea sviluppata dallo stesso Finney, ma senza porre un limite all'ammontare totale dei *Bitgold* prodotti, conferendo loro un valore diverso a seconda delle capacità computazionali investite per produrli.

Sono queste, in sintesi, le basi che conducono, nel 2008, alla pubblicazione del *paper* di Satoshi Nakamoto in cui viene descritto il funzionamento di Bitcoin, che porta, il 3 gennaio 2009, alla creazione del «Genesis Block» ossia del blocco iniziale della Blockchain Bitcoin.

È opportuno sottolineare il contesto culturale in cui tale proposta nasce. Il movimento *cypherpunk* aveva quale principale scopo quello di contrastare le possibili restrizioni delle libertà e del diritto alla privacy, derivanti dalla sempre più pervasiva diffusione delle tecnologie informatiche, le quali avrebbero consentito ai governi ed alle grandi società di monitorare e controllare le informazioni sugli individui potendo inferire i loro stili di vita dall'associazione dei dati raccolti nelle transazioni di consumo. Lo strumento principale di contrasto a tale pericolo era stato individuato in una moneta elettronica anonima ed altri strumenti di pagamento non tracciabili, il tutto utilizzando tecnologie crittografiche su larga scala, che avrebbero anche permesso di realizzare sistemi di messaggistica sicuri, contratti digitali e sistemi di identità digitale rispettosi della privacy.

La proposta di Nakamoto, nel solco di tale ideologia, risolve alcuni dei problemi più rilevanti nel progettare un sistema decentralizzato di pagamenti, mettendo insieme, in maniera originale, una serie di tecnologie già note a quei tempi.

Innanzitutto, la cifratura a chiavi asimmetriche, già ampiamente utilizzata nel 2008[4], la quale, in estrema sintesi, consente di assicurare la paternità di un messaggio e la sua integrità, attraverso il diverso utilizzo di una chiave pubblica ed una chiava privata di cifratura (assegnate alla medesima entità).

In secondo luogo, Nakamoto progetta la blockchain distribuendola su un network *peer-to-peer*, in cui sono i singoli computer degli utenti che operano come "*peer*" o "nodi" agendo contemporaneamente da distributori e fruitori delle informazioni (si pensi a Napster o, in tempi più recenti, a Bitorrent), eliminando in tal modo la presenza di un ente centrale che opera quale validatore delle varie transazioni (e che potrebbe alterare le stesse).

Infine, viene ripreso il principio della *proof of work*, precedentemente proposto in Hashcash, sia come meccanismo di creazione del consenso al fine della validazione delle transazioni sia come strumento di incentivazione per i partecipanti a mettere a disposizione risorse computazionali, con ciò risolvendo, indirettamente, eventuali pericoli di condotte fraudolente all'interno del sistema.

L'insieme di queste tecnologie viene combinato nel *paper* di Nakamoto per creare un protocollo di comunicazione innovativo, che è al contempo un registro immodificabile, in cui le transazioni di bitcoin vengono iscritte attraverso un meccanismo di consenso, al contempo evitando il problema del *c.d.* "double spending"[5].

---

[4] La cifratura a chiavi asimmetriche già nel D.P.R. n. 513/1997 era stata individuata dal Legislatore italiano quale tecnologia alla base della firma digitale. La diffusione di tale tecnologia alla fine degli anni '90 si deve soprattutto al *software* Pretty Good Privacy (PGP), che ha avuto il pregio di renderla accessibile anche all'utente comune.

[5] In un sistema di pagamento uno dei principali problemi da risolvere è evitare che un partecipante possa utilizzare più volte le stesse risorse. Tipicamente ciò viene risolto tramite un controllo centralizzato delle transazioni, registrate

(segue)

Passando brevemente all'esame del funzionamento della blockchain[6] è possibile utilizzare la metafora di un registro immodificabile le cui copie sono distribuite sui vari nodi della rete. Questo registro è organizzato in "blocchi" separati, che raggruppano degli insiemi di transazioni e che sono collegati per formare una "catena" sequenziale marcata temporalmente.

Tecnicamente ciò si ottiene registrando in ciascuno dei blocchi le transazioni - la cui provenienza e destinazione sono verificate tramite l'utilizzo delle chiavi pubbliche crittografiche - insieme ad altre informazioni che possono essere collegate alla transazione stessa. Ogni blocco, inoltre, è dotato di un "*header*" utilizzato per organizzare il database distribuito. All'interno di questo *header* è contenuto l'*hash*[7] di tutte le transazioni registrate nel blocco, la marcatura temporale e l'*hash* del blocco precedente. La blockchain, quindi, viene collegata attraverso questi dati contenuti in ciascun *header*, in quanto la presenza dell'*hash*

---

in uno o più *database* che tengono traccia di ogni transazione effettuata. In un sistema decentrato ciò è più difficile da realizzare, proprio per l'assenza di un unico intermediario. Il sistema deve assicurare che l'ammontare totale dei fondi in circolazione sia certo e che i singoli non possano aggiungere fondi in maniera non controllata. Inoltre, si deve anche assicurare un registro non ripudiabile delle transazioni che tenga conto di tutta la moneta virtuale presente ad un certo istante nel sistema.

[6] Per esigenze di sintesi e per gli scopi del presente scritto la descrizione del funzionamento della blockchain sarà necessariamente riassuntiva. Per un'analisi più approfondita della tecnologia si rinvia a: Roberto Garavaglia, *Tutto su blockchain*, 2018, Hoepli; Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 2015, O'Reilly; Melanie Swan, *Blockchain: blueprint for a new economy*, 2015, O'Reilly; Henning Diedrich, *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*, 2016, Wildfire Publishing.

[7] La funzione di *hash* consente di ridurre in maniera univoca un insieme di bit in una stringa alfanumerica, univocamente riconducibile al contenuto originario, fornendo una sorta di "impronta digitale". Mentre non è possibile risalire al contenuto originario dalla stringa risultato della funzione, eventuali modifiche di tale contenuto possono essere rilevate in quanto l'applicazione della funzione sul nuovo contenuto porterà alla creazione di una stringa diversa.

del blocco precedente consente di ricostruire in maniera cronologica (essendo presente anche la marcatura temporale) la catena di blocchi.

Per proteggere la sicurezza ed integrità del sistema Nakamoto, riprendendo il concetto di *proof of work*, ha inserito un meccanismo per rendere difficoltosa la modifica o la cancellazione delle informazioni una volta salvate. La generazione degli *hash* - che contenendo l'impronta delle transazioni assicurano l'immodificabilità delle stesse e la conseguenzialità della catena - non avviene in modo automatico, bensì solo dopo una particolare procedura che richiede l'impiego di risorse computazionali per risolvere un determinato algoritmo matematico. I vari nodi, quindi, sono in competizione tra loro per la generazione di ogni *hash* di chiusura di ciascun blocco della catena, ed il primo che riesce a risolvere tale algoritmo, dando quindi prova di aver impiegato risorse per giungere a tale scopo (e per tale motivo viene definita "proof of work"), comunicherà la soluzione nel network, che verrà verificata dagli altri nodi[8]. Se tale soluzione è corretta il blocco è aggiunto alla blockchain e quindi salvato su tutti i nodi partecipanti al network. In questo modo il network raggiunge il "consenso" sull'ammontare di valore posseduto da ciascuno dei partecipanti.

---

[8] Tale processo di risoluzione dell'algoritmo matematico è ciò che viene definito "*mining*". La risoluzione richiede un approccio per tentativi, nel senso che ciascun nodo tenta di fornire varie soluzioni, in breve lasso di tempo, fino a trovare quella giusta. Il protocollo Bitcoin, inoltre, calibra la difficoltà dell'algoritmo a seconda di quanti sono i partecipanti al *network*, rendendo più difficoltosa la soluzione in caso di aumento del numero dei partecipanti. Nella Blockchain Bitcoin il nodo che per primo risolve il problema matematico riceve inoltre un quantitativo di bitcoin in premio, quale incentivazione alla partecipazione attiva al *network*. Tale premio è decrescente nel tempo ed allo stato attuale, con l'ampia diffusione che ha avuto Bitcoin, è quasi impossibile riuscire a "minare" un blocco con un *hardware* non specializzato.

Il meccanismo della *proof of work* collegata all'algoritmo di consenso previene anche condotte tese a creare transazioni false o ad alterare i blocchi già registrati. Dato che ciascun blocco contiene l'*hash* del precedente, qualsiasi tentativo di modificare un blocco già registrato comporterebbe la "rottura della catena", in quanto porterebbe alla modifica dell'*hash* di tale blocco ed a quella di tutti i successivi[9].

Inoltre, ogni dieci minuti il network Bitcoin aggiorna il proprio stato, calcolando il "saldo" di tutti gli *account* registrati nel sistema. È opportuno evidenziare che in verità le transazioni non vengono associate ad un account tramite il concetto di "conto", bensì le unità di valore vengono assegnate all'interno della Blockchain ad un determinato proprietario, ma rimangono per così dire "disseminate" all'interno dei vari blocchi.

Infine, una peculiare caratteristica della Blockchain di Bitcoin è la possibilità di veicolare nelle transazioni dei particolari codici informatici (ossia degli *script*) per determinare alcune azioni che i nodi debbono svolgere sulla transazione stessa. In questo modo è possibile vincolare la criptovalute oggetto di transazione a specifiche situazioni, rendendo quindi programmabile il trasferimento delle stesse secondo determinate condizioni.

Quella sopra descritta è la Blockchain Bitcoin ideata e realizzata secondo il *paper* pubblicato sotto lo pseudonimo di Nakamoto e che ha avuto una rapida crescita e diffusione. Tale

---

[9] Una possibile modalità di modifica delle registrazioni su blockchain è quella che viene definita "attacco 51%", ossia quando un gruppo di nodi, rappresentanti complessivamente il 51% del *network*, agiscono in forma unitaria per approvare transazioni ad una velocità maggiore del resto dei partecipanti. In base ai numeri attuali della Blockchain, però, un attacco del genere avrebbe costi economici assai rilevanti, nell'ordine di centinaia di milioni di dollari, e, soprattutto, provocherebbe sicuramente l'effetto di sfiduciare la blockchain in questione, comportando l'abbandono della stessa da parte dei partecipanti "in buona fede" e la svalutazione dell'eventuale valuta virtuale ad essa collegata.

Blockchain, però, è principalmente progettata per lo scambio di valuta virtuale, ed offre limitate soluzioni per chi voglia utilizzare la stessa per altri scopi.

Nel corso degli anni sono quindi nati altri progetti, volti ad utilizzare la blockchain non solo quale strumento per lo scambio di valore, ma anche, ad esempio, per consentire l'esecuzione di applicazioni decentralizzate. Nel 2014, quindi, è stato lanciato il progetto Ethereum, poi realizzato nel 2015: una blockchain progettata per essere una sorta di sistema operativo distribuito, implementando numerose funzionalità rispetto Bitcoin. Ethereum ha sempre la struttura di un network *peer-to-peer*, con un codice sorgente *open* e libero, una sua criptovaluta ed un meccanismo di *proof of work* per validare le transazioni. Questa blockchain, però, aggiorna il proprio stato ogni dodici secondo, rispetto ai dieci minuti di Bitcoin, ed è dotata di una *Ethereum Virtual Machine* (EVM) che elabora i programmi software che possono essere attestati nella blockchain, realizzati con l'apposito linguaggio di programmazione (Solidity), rendendo molto più semplice la creazione di smart contract sul network da parte degli sviluppatori.

Scopo primario di Ethereum, quindi, a differenza di Bitcoin, è quello di fornire una piattaforma per lo sviluppo di applicazioni che risiedono sulla blockchain, facilitando la loro implementazione tramite un apposito linguaggio, con la conseguenza di poter superare il concetto "classico" di applicazione client/server mediante la decentralizzazione dei punti da cui le applicazioni stesse sono erogate. Uno dei più rilevanti effetti derivante dall'implementazione e diffusione di Ethereum è stato il rapido incremento nel corso del 2017 di utilizzatori della tecnologia blockchain, soprattutto per avviare Initial Coin Offering (ossia

offerte iniziali di criptovalute), in conseguenza della maggior facilità di programmazione di nuovi *token*.

È anche possibile utilizzare le blockchain esistenti per scopi diversi da quelli per cui originariamente sono state create. Ad esempio su blockchain Bitcoin vengono spesso realizzate delle *Colored Coin*, creando token rappresentativi di diversi *assets* tramite l'utilizzo dei metadati all'interno delle transazioni[10].

Da quando Bitcoin è stata attivata, e, soprattutto, dopo la crescente attenzione che le blockchain hanno attirato sul mercato, in conseguenza dei forti rialzi di valore delle criptovalute verificatisi nel 2017, gran parte per fini speculativi, hanno preso forma numerosi progetti per implementare la tecnologia.

Tra questi vi sono blockchain specializzate, come IOTA (una blockchain pensata per l'Internet of Things), Ripple (che facilita la conversione tra valute reali), Filecoin (che mira a creare un repository distribuito tra gli utenti). Alcuni altri progetti sono stati proposti con il fine di superare le attuali limitazioni delle blockchain più conosciute (Bitcoin ed Ethereum), come EOS, che grazie al maggior numero di transazioni processabili al secondo ed all'eliminazione dei costi di esecuzione degli smart contract, mira a porsi quale alternativa di Ethereum.

Vi sono inoltre importanti iniziative, come Hyperledger, che propongono soluzioni *open source* pensate per specifiche esigenze.

Infine, i grandi *player* mondiali hanno creato nei loro servizi *cloud* la possibilità di utilizzare la "*Blockchain as a Service*", consentendo agli utenti di attivare direttamente sulle piattaforme

---

[10] In questo modo è possibile "tokenizzare" un *asset* reale, ossia riferire una transazione sulla blockchain ad un bene presente nella realtà materiale (e non solo virtuale come le criptovalute), attraverso la specificazione del bene stesso all'interno dei metadati associati alla transazione.

la tecnologia blockchain per utilizzarla nell'ambito delle loro organizzazioni.

1.1.1. Caratteristiche della blockchain

In termini riassuntivi la blockchain può essere descritta come un *database* distribuito (ed infatti rientra nella più ampia categoria delle Distributed Ledger Techonology - DLT) che consente al medesimo tempo di eliminare la presenza di una terza parte fidata (ossia di un soggetto che svolga le funzioni di validatore delle transazioni) instaurando un meccanismo alternativo di fiducia[11] e di introdurre il concetto di scarsità digitale.

Tale ultimo concetto è ciò che rende possibile la creazione di valore, rendendo gli asset registrati sulla blockchain scambiabili e suscettibili di una valutazione economica. In ambito informatico, infatti, ogni insieme di informazioni è facilmente replicabile, senza costi od oneri aggiuntivi; un qualsiasi file può essere facilmente copiato, diffuso e trasmesso, così come qualsiasi informazione registrata informaticamente. Il meccanismo della blockchain consente invece di rendere scarsa l'informazione, dando quindi valore ad un bene (immateriale) che altrimenti non ne avrebbe. Ciò è possibile tramite l'uso delle tecnologie crittografiche, la cui applicazione ad un determinato *set* di dati rende univocamente identificabili gli stessi, consentendo la loro identificazione e tracciabilità in un sistema che, altrimenti, vede indistinguibili gli originali dalle copie[12].

---

[11] Tanto da essere definito "The *trust* Protocol", vd. Don Tapscott e Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, 2016, Portfolio, pag. 8.

[12] A ben vedere la legislazione italiana ha già da tempo introdotto il concetto di unicità del documento informatico. Il D.Lgs. n. 82/2005 (CAD) distingue tra duplicato informatico e copia informatica, ossia tra un *file* contenente la *«medesima sequenza di valori binari del documento originario»* ed un *file*

(segue)

La tecnologia blockchain, inoltre, ha alcune caratteristiche peculiari rispetto alle altre ad oggi maggiormente utilizzate, che la caratterizzano in maniera specifica ma che, al contempo, ne costituiscono anche il limite[13].

A differenza della gran parte dei servizi online, la blockchain è decentralizzata ed ha una vocazione transnazionale che si contrappone alla situazione attuale, in cui le interazioni *online* sono caratterizzate dall'essere veicolate da enti o soggetti i quali operano come detentori delle informazioni (sia che si tratti di effettuare ricerche online, di acquistare beni o servizi o di effettuare dei pagamenti). La gran parte dei servizi prevedono la presenza di un soggetto che opera quale erogatore degli stessi o che intermedia tra altre parti. La blockchain consente, invece, di eliminare tale presenza, mettendo in diretto collegamento gli utenti, tramite un meccanismo *peer-to-peer*, in cui ciascuno svolge un ruolo contemporaneamente attivo per la creazione e validazione delle transazioni e passivo per la conservazione della memoria delle stesse. Il *database* delle informazioni è distribuito su tutti i nodi del network, e ciò conferisce anche la caratteristica di transnazionalità della tecnologia. Qualora un Paese decida di bloccare l'accesso al network comunque tutte le transazioni sarebbero conservate in ciascuno dei nodi, potendo così facilmente ripristinarne l'operatività dello stesso.

---

che invece ha una «*diversa sequenza di valori binari*». Con la blockchain, una volta creata la sequenza di bit, ossia l'informazione originaria, tramite l'applicazione della chiave privata e la registrazione del relativo *hash* in un blocco detta sequenza diviene tracciabile e quindi non duplicabile acquisendo unicità all'interno del *network*.

[13] Per una disamina delle caratteristiche e limitazioni vd. De Filippi, Wright, *Blockchain and the law, The Rule of Code, 2018*, Harvard University Press, pag. 34.

La blockchain, inoltre, è un registro immodificabile, nel senso che le informazioni sono memorizzate in una modalità tale che non è possibile per il singolo partecipante cancellarle o variarle. I dati registrati, inoltre, in conseguenza dell'utilizzo della crittografia a chiave pubblica, sono non ripudiabili da coloro che li hanno generati, e possono essere sempre verificati. Il sistema, infatti, conserva i metadati e le informazioni di contesto delle singole transazioni, rendendo riconducibili le stesse agli account partecipanti al network.

Altra caratteristica peculiare della blockchain è il meccanismo di incentivazione dei partecipanti. La tecnologia è logicamente strutturata per indurre ad agire in buona fede, incentivando la partecipazione al sistema, tramite meccanismi di guadagno e rendendo estremamente difficili le condotte abusive. Su tali incentivi si riflettono anche meccanismi di mercato, a volte speculativi, in cui entrano in gioco i valori assunti dalle criptovalute in un dato momento rispetto ai costi necessari a produrle.

Ulteriori caratteristiche della tecnologia blockchain sono la pseudonimizzazione dei partecipanti, e su tale aspetto ritorneremo nei prossimi paragrafi, dato che, almeno su Bitcoin ed Ethereum, i titolari degli account non sono direttamente identificabili; la capacità di creare meccanismi per la formazione del consenso nell'ambito del network senza la necessità di un organismo centralizzato; la possibilità di creare software che operano quali agenti autonomi, distribuiti su tutto il network, che agiscono in maniera indipendente e che possono svolgere funzioni in maniera automatica al verificarsi di alcune condizioni, senza dover dipendere da un singolo soggetto erogatore.

Da un punto di vista concettuale, infine, è opportuno chiarire che la tecnologia blockchain si inquadra come un protocollo

aggiuntivo sopra i protocolli di trasporto, ossia un protocollo applicativo che si aggiunge a quelli esistenti (come il TCP/IP, il protocollo SMTP o quello FTP), che consente di conservare le informazioni ed effettuare operazioni computazionali. Il protocollo blockchain può, quindi, interagire con gli altri protocolli applicativi a seconda dei servizi che si intendono implementare. Ciò significa che non siamo in presenza di una semplice applicazione, ma di un vero e proprio ulteriore *layer* di comunicazione su cui possono essere sviluppate innovative soluzioni che riescono a sfruttare le caratteristiche delle blockchain esaminate in questo paragrafo.

1.1.2. Tipologie di blockchain

Nell'ambito delle varie tipologie di blockchain esistono alcune distinzioni in base alla possibilità di accesso ed al grado di distribuzione delle stesse. In verità, sembra che tali distinzioni siano oggi troppo accentuante e frammentarie, dato che si parla di *Permissioned Ledger, Unpermissioned Ledger, Shared Ledger, Distributed Ledger, Replicated Shared Ledgers, Distributed Ledger Systems, Permissioned Distributed Ledgers, Permissioned Permission - lessness Ledgers*, e così via, trovando sempre più segmentazioni spesso fondate su lievi distinzioni dei meccanismi di accesso.

Semplificando rispetto tale eccessiva frammentazione, si possono individuare tre grandi tipologie di blockchain, così come anche tipizzate dall'Osservatorio blockchain & distributed ledger della School of Management del Politecnico di Milano[14] e ciò sulla base di alcune caratteristiche comuni:

- *blockchain pubbliche* (*c.d. permissionless*): si tratta di blockchain che sono liberamente accessibili a chiunque. Non vi

[14] Vd. Mauro Bellini, *Blockchain & Bitcoin*, 2018, Milano Finanza, pag. 41 ss.

sono restrizioni circa la lettura delle transazioni, l'effettuazione delle stesse (con l'aspettativa che vengano inserite nella blockchain) e la possibilità di partecipare al meccanismo di consenso. Si tratta del modello su cui è stata realizzata la Blockchain Bitcoin, finalizzato a disintermediare i meccanismi di fiducia, che come tale non pone requisiti specifici alla partecipazione del network ed anzi ne incentiva l'espansione tramite meccanismi che gratificano coloro che mettono a disposizione delle risorse. Le blockchain pubbliche hanno tendenzialmente una vocazione globale, creano dei meccanismi di fiducia tra i partecipanti, non prevedono barriere all'ingresso nel network e tendenzialmente sono sempre accessibili;

- *blockchain ibride:* in tale tipologia il meccanismo di consenso sulle transazioni è controllato da un insieme di nodi preselezionati. Questi nodi hanno un'influenza maggiore rispetto agli altri ed anzi, tramite varie soluzioni (solitamente di voto), determinano quali transazioni possono essere incluse nei blocchi. In lettura una blockchain ibrida può essere accessibile al pubblico o limitata ai partecipanti. In sintesi, tali tipologie sono blockchain parzialmente decentrate, i nodi vengono chiamati "*contributors*" e non sono posti sullo stesso piano rispetto alle operazioni che possono compiere nel sistema;
- *blockchain private (permissioned)*: una blockchain privata è una blockchain in cui le autorizzazioni di scrittura e di lettura vengono gestite da uno o più soggetti selezionati. Si tratta, quindi, di una blockchain chiusa, in cui la partecipazione al network è autorizzata solo a determinati soggetti e non è accessibile pubblicamente.

Una blockchain privata presenta una serie di vantaggi rispetto quella pubblica, quali la possibilità di modificare le regole della

blockchain, ripristinare le transazioni, modificare i saldi, ecc. Si presta ad essere utilizzata per applicazioni ed utilizzi sia da parte di privati ed aziende, che possono impiegarla per gestire transazioni ricorrenti tra loro, sia in alcuni ambiti della Pubblica Amministrazione in cui è necessario mantenere un governo delle transazioni che vengono registrate ed il controllo formale e di legittimità da parte dell'Autorità amministrativa.

Le blockchain ibride si prestano a casi d'uso in cui è necessario mantenere il governo sulla registrazione delle transazioni, ma è possibile, e desiderabile, rendere pubblica la consultazione della blockchain. Si pensi, ad esempio, a tutti i registri pubblici distribuiti, in cui più Amministrazione pubbliche partecipano nell'inserire (o validare) informazioni che per loro natura sono però destinate alla pubblicità. Si potrebbe ipotizzare l'adozione di una tale tecnologia nell'ambito dei procedimenti amministrativi a cui partecipano diverse Pubbliche Amministrazioni, ad esempio tramite conferenza di servizi, in cui ognuna di esse ha un ruolo ed una potestà amministrativa autonomi. La validazione delle informazioni, tramite il meccanismo del "voto dei pochi" permetterebbe di registrare su una blockchain ibrida gli esiti delle singole valutazioni delle Pubbliche Amministrazioni. La pubblicità delle informazioni garantirebbe d'altra parte la trasparenza dell'agire amministrativo, senza possibilità di modificare *ex post* le varie fasi della procedura.

In generale sono stati individuati[15] quattro elementi distintivi delle blockchain private:

1) infrastruttura. Le blockchain private devono essere attestate su reti a loro volta private, la cui sicurezza è gestita dai

[15] Mauro Bellini, *op. loc. cit.*

partecipanti alla blockchain in modo da poter così garantire il meccanismo di fiducia. Ed infatti, proprio perché una blockchain privata non può contare sulla sua diffusione, che costituisce la caratteristica di quelle pubbliche e ne assicura l'immodificabilità delle transazioni tramite un meccanismo distribuito di consenso difficilmente aggredibile, diventano essenziali gli aspetti di sicurezza dell'infrastruttura, che non deve consentire a soggetti estranei al network di parteciparvi, pena il venir meno dell'affidabilità di quanto registrato sulla blockchain;

2) ecosistema. Per ecosistema si intende la necessità che i partecipanti ad una blockchain privata condividano, per quanto attiene alla partecipazione al network, gli stessi valori, obiettivi e regole. L'efficacia di una blockchain privata poggia, infatti, sulla fiducia reciproca dei partecipanti e sull'aspettativa che ciascuno di essi ha nel fatto che gli altri agiranno coerentemente con gli obiettivi del network;
3) applicazioni. La componente applicativa delle blockchain private deve seguire le logiche tecnologiche e di *governance* che sono definite dagli attori del network. In una blockchain le regole di partecipazione vengono, per così dire, direttamente definite a livello di software e pertanto gli sviluppatori devono agire in stretta collaborazione con i soggetti che intendono partecipare alla blockchain privata;
4) governance. La *governance* costituisce l'insieme di regole condivise da tutti gli attori, definite sulla base degli obiettivi del progetto e dei risultati attesi. Tramite la possibilità di modulare i meccanismi di consenso e di creare smart contract che eseguono in maniera automatica determinate operazioni,

la *governance* può essere direttamente disciplinata nel codice software che assume così una funzione "regolatoria"[16].

Ferme rimanendo le categorizzazioni sopra riportate, è opportuno osservare che al fine di superare le limitazioni di scalabilità ed adozione su larga scala delle attuali blockchain, si ipotizza ed auspica da alcune parti[17] che la prossima generazione di blockchain sia realizzata sulla base di criteri di interoperabilità, consentendo quindi a singole blockchain di dialogare tra loro, favorendo lo scambio di dati in quella che potrebbe essere definita una rete confederata di blockchain.

Al livello internazionale sono stati costituiti alcuni tavoli di lavoro a cui partecipa anche l'Italia (il gruppo di lavoro ISO (ISO/TC 307 Blockchain and distributed ledger technologies)[18], il gruppo ITU (ITU Focus Group on Application of Distributed Ledger Technology)[19] ed il gruppo delle Nazioni Unite UNECE (United Nations Centre for Trade Facilitation and Electronic Business)[20], tutti volti alla definizione di regole standard per l'implementazione di soluzioni su tecnologia blockchain, con l'obiettivo di produrre regole uniformi per lo sviluppo delle stesse, favorendo l'interoperabilità e qualità dei sistemi, la cui adozione costituirà un incentivo e darà impulso alla diffusione della blockchain, assicurando una base comune per tutti coloro che vogliano adottarla.

---

[16] Sul tema del ruolo del codice e della progressiva "softwarizzazione" delle norme si vd. De Filippi, Wright, *op. cit.,* pag. 195, nonché De Filippi, Hassan, *The Expansion of Algorithmic Governance: From Code is Law to Law is Code*, 2017, Field *Actions* Science Reports, reperibile su https://journals.openedition.org/factsreports/4518, sito visitato il 13 agosto 2018.

[17] Alessandro Mario Lagana Toschi, *What's the next step in Blockchain technology?* 2018, reperibile su https://hackernoon.com/whats-the-next-*step*-in-blockchain-technology-f479c425027a, sito visitato il 13 agosto 2018.

[18] https://www.iso.org/committee/6266604.html.

[19] https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/*default*.aspx.

[20] https://uncefact.unece.org/display/uncefactpblic/Blockchain+White+Paper.