LUISS

Dipartimento
di Economia e Management

Cattedra Economia dei Mercati e degli Intermediari Finanziari

BLOCKCHAIN E INTERMEDIARI FINANZIARI

Prof. Francesco Cerri
RELATORE

Giovanni Formicola Matr.209221
CANDIDATO

Anno Accademico 2018/2019

INDICE

INTRODUZIONE

Lo sviluppo dell'informatica ha caratterizzato in maniera particolarmente rilevante i primi venti anni di questo terzo millennio riuscendo a modificare tutti i settori dell'economia in maniera più o meno significativa, le maggiori sfide che le imprese hanno dovuto fronteggiare in questi anni, e che tutt'ora stanno affrontando, sono proprio legate a questo sviluppo molto rapido delle nuove tecnologie, le quali hanno mostrato di poter cambiare le basi della concorrenza facendo fuori chi non è in grado di stare al passo coi tempi. Persino il settore dell'intermediazione finanziaria, che da secoli è al centro del sistema economico di tutti gli Stati, sta affrontando un periodo di difficoltà senza precedenti; nonostante questo sia alimentato, in prevalenza, da un ciclo economico avverso, caratterizzato da due crisi finanziarie ravvicinate che, per una serie di accadimenti, hanno ridotto drasticamente la fiducia delle persone nei confronti degli intermediari, c'è comunque da notare come, anche in questo settore, la componente tecnologica abbia portato delle novità significative tanto da mettere in discussione l'esistenza stessa degli intermediari finanziari.

Quando si fa riferimento all'intermediazione finanziaria molto spesso il collegamento alla figura delle banche risulta immediato, in quanto queste non solo risultano essere l'intermediario finanziario per eccellenza, ma ricoprono anche il ruolo più importante nel sistema economico attuale, sono infatti gli unici soggetti autorizzati ad effettuare la raccolta e la gestione del risparmio tra il pubblico e proprio per questo sono sempre al centro di una costante osservazione e critica, in particolar modo in un periodo complicato come quello attuale.

Proprio perché le banche sono i principali intermediari finanziari è possibile limitarsi ad analizzare gli eventi ad esse collegati per comprendere come, gli accadimenti degli ultimi anni, abbiano assestato dei colpi durissimi alla reputazione di tutti gli intermediari.

Le varie crisi economiche verificatesi nel Novecento avevano già fatto prendere consapevolezza della fragilità di un sistema economico che fosse interamente fondato sulle banche ma, con la crisi del 2007 dei mutui sub-prime, ci si è resi conto, ancor più che in precedenza, di come la rete globale creatasi tra le banche abbia raggiunto un livello di importanza e complessità tale che un qualunque evento, associato a una qualsiasi di queste, sia in grado di dar vita ad una reazione a catena che, inevitabilmente, fa cascare tutte le tessere che compongono il sistema. Ed è proprio per questo che, successivamente il fallimento di Lehman Brothers, prima, e di altre banche sparse in giro per il mondo, poi, ci si è resi conto, ancora di più, di come le fondamenta di questo castello siano ben più fragili di quanto si pensasse in precedenza e di come, si sia raggiunto un livello tale per cui comportamenti discutibili nella gestione delle banche siano in grado di dar vita a problemi di dimensioni globali con conseguenze disastrose. Ed è proprio per questo che gli eventi che dal 2007 in poi hanno portato al fallimento e alla crisi di molte banche hanno colpito duramente la fiducia delle persone nei confronti di queste secolari istituzioni.

Questi accadimenti hanno fatto sì che una nuova tecnologia sia stata in grado di trovare un terreno fertile per il proprio sviluppo, riuscendo a trovare quell'approvazione che, pochi anni prima, essa stessa non era riuscita a riscuotere, una tecnologia capace di mettere in discussione l'esistenza stessa delle banche proprio in quanto pone le basi per il superamento di un sistema fortemente centralizzato come quello attuale: la Blockchain.

Il presente elaborato si propone, dunque, di analizzare quello che è il funzionamento, i vantaggi, gli svantaggi e le applicazioni pratiche di questa nuova tecnologia che, inevitabilmente, sta divenendo una delle più discusse degli ultimi anni proprio per via del suo alto potenziale in quanto ha dimostrato di avere le carte in regola per dare avvio ad un profondo rinnovamento del sistema economico attuale.

A tal fine lo scritto sarà articolato in quattro capitoli:

Nel primo si definiranno le caratteristiche della blockchain e di come queste si siano evolute nel corso del tempo fino al lancio di Bitcoin; il secondo capitolo affronterà, invece, un'analisi delle principali aziende utilizzatrici di questa tecnologia, di come queste abbiano apportato modifiche e migliorie al sistema inizialmente sviluppato e, in particolare, si analizzeranno i casi, Ethereum (con particolare riferimento al caso Maker) e Ripple. Con i capitoli due e tre si entrerà maggiormente nel vivo dell'elaborato in quanto si effettuerà, nel capitolo tre, una valutazione di quelli che sono i vantaggi e gli svantaggi che questa tecnologia comporta, mentre il quarto sarà dedicato interamente all'utilizzo che si sta facendo di questa tecnologia e dunque ai vari progetti che si stanno sviluppando e portando avanti dalle più importanti società a livello mondiale.

CAPITOLO I
BLOCKCHAIN: NASCITA E SVILUPPO

1.1 ELEMENTI DI BASE

Il sistema economico si regge da secoli sull'utilizzo della moneta come strumento di scambio tra le persone; precedentemente gli scambi erano regolati attraverso il baratto che implicava, però, una serie di problemi che ne limitano la velocità di esecuzione delle transazioni, la ricerca di una controparte disposta a cedere uno specifico bene in cambio di un altro, in particolare, risultava piuttosto onerosa in termini di tempo. L'introduzione della moneta riuscì a migliorare l'attività di scambio rendendola più rapida ed efficiente, ma con il tempo e l'evolversi del sistema economico anche questa ha manifestato una serie di limiti non trascurabili.

In origine la moneta si configurava come nient'altro che un oggetto il quale, per via del materiale con cui era realizzato, era riconosciuto dalle persone come dotato di un valore intrinseco e dunque accettato per effettuare degli scambi. L'aumento della complessità del sistema economico e il succedersi di una serie di vicissitudini ha fatto sì, però, che la moneta, col tempo, perdesse quella caratteristica fisica che ne giustificasse il valore intrinseco, per cui, attualmente, quest'ultimo risulta basato non più su un elemento concreto ma solo ed unicamente sulla fiducia che le persone ripongono nello strumento di scambio e dunque nella moneta stessa.

Una delle di criticità principali delle valute attuali, è proprio legato alla fonte di questa fiducia: attualmente una valuta è tanto più affidabile e "forte" sul mercato (e dunque dotata di maggior fiducia) quanto più risulta affidabile e "forte" il suo emittente, proprio perché ci si aspetta che quest'ultimo riesca ad assicurare il valore della valuta e quindi la possibilità di poterla continuare a scambiare anche in futuro. In una sistema simile appare inevitabile che vi sia un ente centrale che in qualche modo deve riuscire a preservare quella fiducia che le persone hanno, nel tempo, maturato nei suoi confronti, tutto ciò al fine di evitare appunto che la valuta perda il proprio valore. Ed

è proprio la presenza di un ente centrale di questo tipo, dotato di un enorme potere di gestione della valuta circolante in uno Stato, o in un gruppo di Stati, che ha favorito la nascita dell'idea che fosse possibile, in qualche modo, stravolgere questa struttura, andando a realizzare un sistema nuovo all'interno del quale non vi fosse più un unico soggetto atto a svolgere questa funzione. Si fa dunque strada l'ipotesi di andare a realizzare una struttura, completamente decentralizzata, all'interno della quale potesse circolare una valuta il cui valore fosse determinato, non più tanto sulla base della fiducia che i singoli hanno nei confronti dell'emittente quanto, piuttosto, fondato sulla fiducia che i singoli hanno nella valuta stessa e della possibilità di poterla scambiare per acquistare beni e servizi.

Le crisi economiche dell'ultimo decennio e gli effetti che queste hanno avuto sull'economia globale, dovuti all'interconnessione esistente tra gli enti centrali emittenti, hanno incentivato notevolmente lo sviluppo di questa idea tanto che si è giunti a dar vita ad una tecnologia innovativa, la Blockchain, che tenta di rendere effettiva l'idea di un sistema di scambio che sia completamente decentralizzato e dunque svincolato da qualsiasi autorità.

1.2 COME FUNZIONA LA BLOCKCHAIN

La crittografia, ossia la disciplina che si occupa di occultare i messaggi al fine di renderli assolutamente incomprensibili ai soggetti non autorizzati a leggerli, è alla base della blockchain.

L'obiettivo originario di questa nuova tecnologia era quello di realizzare una rete che permettesse ad una valuta, completamente digitale, di poter circolare liberamente senza che si presentassero tutta una serie di problematiche relative alla possibilità di contraffazione e duplicazione della stessa. Un problema notevole della moneta fisica è, infatti, legato alla possibilità che questa possa essere contraffatta, nonostante si sia cercato, nel corso del tempo, di rendere tale operazione sempre più difficoltosa adoperando metodi differenti. Negli anni si è tentato anche di impedire la

contraffazione realizzando valute completamente digitali che fossero, dunque, fisicamente impossibili da replicare in quanto inesistenti se non come flusso di dati. La realtà dei fatti ha, però, mostrato come, sebbene non sia possibile creare delle contraffazioni digitali, sia comunque possibile manipolare il sistema andando a "duplicare" le monete esistenti. E' infatti possibile realizzare una moneta digitale, identica ad una già esistente, capace di circolare contemporaneamente con l'originale, andando a generare un problema cosiddetto di "doppia spesa" il quale si configura essendo possibile spendere due o più volte la medesima moneta eseguendo transazioni diverse tra loro e andando di fatto a replicare la moneta e a riproporre le medesime problematiche legate alla contraffazione. Per cui, se da un lato, attraverso una valuta digitale, risulta possibile evitare la contraffazione fisica vera e propria, non è comunque possibile eliminare del tutto la possibilità che si ripresentino le medesime problematiche.

Grazie alla crittografia, invece, la blockchain riesce a dar vita ad un sistema in cui non è possibile contraffare la moneta né poterla spendere due volte, riuscendo così a risolvere, senza dover fare affidamento ad un ente centrale che convalidi tutte le transazioni, i problemi legati alle monete tradizionali.

Il processo informatico seguito dalla blockchain è facilmente comprensibile se si valuta il caso di due soggetti che vogliono eseguire una semplice transazione quale la vendita di un oggetto. In uno scambio tradizionale i due soggetti dovrebbero, al fine di poter eseguire la transazione in maniera corretta, fornire tutte le informazioni circa l'importo da trasferire e l'oggetto del trasferimento ad un ente che assicuri la validità della transazione, in questo caso una banca. Adoperando invece la blockchain le informazioni relative alla vendita del bene risultano note ai soli soggetti interessati, i quali una volta accordatisi sulle modalità e gli importi dello scambio, rendono tali informazioni disponibili agli utenti della rete. Prima che queste possano essere però diffuse vengono criptate attraverso l'utilizzo di una funzione di hash. L'hashing è un'operazione di crittografia attraverso la quale è possibile trasformare un messaggio in una serie di caratteri che lo identificano univocamente ma che, allo stesso tempo,

lo rendono assolutamente incomprensibile in mancanza delle chiavi di lettura. Tali chiavi sono in possesso, solo ed unicamente, dai due soggetti coinvolti nella transazione, per cui solo loro sono in grado di accedere alle informazioni relative alla transazione. Una volta effettuato l'hashing delle informazioni relative alla transazione queste vanno a costituire, insieme con le informazioni derivanti da altre transazioni, un blocco (Block) che deve essere convalidato attraverso la risoluzione di un problema matematico molto complesso. A questa operazione di risoluzione e convalida può partecipare qualsiasi utente (nodo) della rete attraverso il proprio terminale mettendo a disposizione la potenza di calcolo della propria CPU. Questa fase di decodifica del blocco risulta una delle più importanti dell'intero processo in quanto, solo attraverso la risoluzione del problema, è possibile garantire che non vi sia stata alcun tipo di duplicazione della moneta e che dunque sia possibile eseguire la transazione in via definitiva e irreversibile.

A concludere il processo vi è infine un'ultima fase durante la quale avviene la registrazione della transazione all'interno di un registro contabile (Ledger) nel quale vengono memorizzati e posizionati, in sequenza, tutti i blocchi decodificati, che vanno così a costituire una sorta di catena (Chain) contenente tutte le transazioni eseguite all'interno del sistema nel corso del tempo. Tale registro risulta disponibile a qualsiasi utente che, scaricandolo, può di fatto divenire garante dell'avvenuta esecuzione di una qualsiasi transazione che sia stata approvata in passato.

Le singole fasi del meccanismo della blockchain ci permettono di capire come questa riesca ad eliminare, tramite la crittografia, i problemi relativi alla contraffazione e alla doppia spesa:

- Attraverso le chiavi private di crittografia il contenuto della transazione viene reso incomprensibile, rendendone impossibile la manipolazione, infatti, l'unico modo per poter accedere alle informazioni è quello di eseguire una forzatura per tentativi del messaggio criptato, la quale, però, per poter essere eseguita in tempi ragionevoli, richiede una potenza di calcolo a tal punto elevata da non poter essere detenuta da un singolo soggetto. Per cui, tramite

l’hashing, la blockchain riesce a garantire livello di sicurezza estremamente elevato impedendo, inoltre, la duplicazione delle monete coinvolte nella transazione risolvendo così il problema della doppia spesa. Al fine di aumentare ulteriormente la sicurezza, il sistema, prevede inoltre che le chiavi di crittografia adoperate per l’esecuzione della transazione vengano sostituite di volta in volta ad ogni nuova operazione. Ciò avviene al fine di garantire l’anonimato assoluto degli utenti in quanto, l’utilizzo ripetuto della medesima chiave pubblica di crittografia, permetterebbe ad altri utenti di risalire, attraverso le transazioni eseguite, all’utente in questione che, sebbene risulti registrato con un nickname e sia dunque irriconoscibile, potrebbe comunque non voler rendere noto quante transazioni esegue.

- Il ledger ricopre anche un ruolo molto importante in tema di sicurezza, questo, registrando in sequenza tutte le transazioni eseguite, fa sì che qualora si tentasse di modificare una transazione effettuata in passato, sarebbe necessario ed inevitabile andare a modificare anche tutti i blocchi successivi. Dunque anche qualora si riuscisse a forzare la funzione di hash e a risalire alle informazioni contenute al suo interno, per poter modificare la transazione sarebbe necessario modificare anche tutte quelle convalidate successivamente. Per cui l’intero sistema risulta pensato e sviluppato per impedire qualsiasi tentativo di alterazione della catena e delle transazioni.
- La seconda fase del processo, ossia la convalida del blocco ad opera degli utenti, fornisce gli elementi necessari al superamento di un altro limite del sistema tradizionale, ossia il superamento del sistema centralizzato. In questo caso vi è una singola autorità centrale che, fungendo da garante, approva tutte le transazioni che vengono effettuate. Attraverso la blockchain invece, grazie alla partecipazione di tutti gli utenti alla risoluzione del problema matematico, si pongono le basi per la realizzazione di un sistema decentralizzato in cui chiunque è in grado di convalidare le transazioni. Anche la creazione del ledger, oltre al sistema di convalida, gioca un ruolo fondamentale sotto questo

profilo, esso infatti garantisce l'esistenza di un registro storico contenente tutte le transazioni avvenute nel corso del tempo che, venendo aggiornato in tempo reale e potendo essere scaricato da tutti gli utenti, risulta, non solo impossibile da perdere, ma anche potenzialmente consultabile in qualsiasi momento al fine di verificare transazioni già avvenute, anche a distanza di molto tempo dalla loro approvazione.

1.3 NASCITA DELLA BLOCKCHAIN

Sebbene la blockchain abbia avuto una risonanza mediatica rilevante solamente negli ultimi anni, essa è stata ideata già da diverso tempo o, quanto meno, la sua base risale agli inizi degli anni '80. L'ideatore dei concetti base della blockchain è David Chaum il quale, nel 1983, realizzò un articolo dal titolo: "Blind signatures for untraceable payments" nel quale teorizzava la creazione di un sistema di pagamento che, facendo uso di chiavi pubbliche e private di crittografia, potesse dare la possibilità di eseguire delle transazioni che garantissero al contempo:

- Un elevato livello di privacy, in quanto impedivano a terze parti di poter controllare i dettagli della transazioni e, in particolare, i beneficiari, i tempi di esecuzione e l'ammontare dei pagamenti.
- La possibilità di poter identificare, in determinate circostanze, il beneficiario, al fine di facilitare le attività di controllo relative a tentativi di frode, evasione fiscale o qualunque altro tipo di attività illegale collegata ai pagamenti.
- La capacità di impedire l'utilizzo di strumenti di pagamento che fossero stati segnalati come rubati, bloccandone la circolazione e, di conseguenza, la possibilità di poter essere nuovamente adoperati, andando a creare un problema di doppia spesa.

Successivamente la pubblicazione di questo articolo Chaum avviò il primo progetto di realizzazione di una valuta digitale che sfruttasse la crittografia e le cosiddette

“Blind Signatures”, ossia delle firme digitali, apposte su documenti criptati, che garantivano il trasferimento di informazioni e, nel progetto di Chaum, delle monete, le quali impedivano a soggetti terzi di venire a conoscenza del contenuto del trasferimento.

Il progetto di sviluppo della valuta digitale, portato avanti da Chaum, si concretizzò nel 1989 con la nascita della società DigiCash, la quale rese disponibile un sistema di pagamenti che, tramite la moneta nota come Ecash, garantiva la possibilità di effettuare transazioni che fossero in grado di rispettare tutti e 3 i punti del paper di Chaum.

In una fase iniziale il progetto e la società riuscirono ad attirare alcuni investitori e clienti, in particolare negli USA la Mark Twain Bank adottò questo sistema di pagamento per effettuare alcuni test sulle micro transazioni, ma a lungo andare la mancanza di ulteriori clienti, costrinse la società a dichiarare bancarotta nel 1998. Il progetto di Chaum non fu un successo ma riuscì comunque a dimostrare la possibilità di poter realizzare un sistema di pagamento interamente basato su di una moneta digitale. Il tentativo di Chaum riuscì comunque a fornire nuova linfa allo sviluppo della sua idea tanto che, alla fine degli anni ’90, vennero ideati altri due sistemi di monete digitali che furono fondamentali per la successiva nascita dell’odierna blockchain.

Le idee di Adam Back con il sistema “Hashcash” sviluppato nel 1997, e la criptovaluta b-money ideata da Wei Dai nel 1998, fornirono ispirazione per la nascita dell’odierna blockchain e di Bitcoin, che possiamo definire come il progetto che ha sancito il lancio definitivo di questa tecnologia.

1.4 HASHCASH E B-MONEY

Hashcash è un sistema ideato e sviluppato da Adam Back al fine di limitare il fenomeno dello spam di mail che funziona tramite l’utilizzo di un algoritmo di Proof-of-work che individua le e-mail in questione. Semplificando, l’algoritmo posiziona un codice testuale come intestazione di una qualunque e-mail prima che questa possa essere inviata, in tal modo è possibile determinare il tempo impiegato dalla CPU

dell'emittente ad elaborare l'intestazione e comprendere se questo risulti essere uno spammer. L'invio di poche e-mail in contemporanea, infatti, implica un consumo molto ridotto di potenza computazionale e dunque un lasso di tempo limitato per l'elaborazione dell'intestazione, al contrario, quando si invia un numero elevato di e-mail, come nel caso degli spammer, la CPU sarà costretta a dedicare buona parte del proprio potere computazionale e un consistente lasso di tempo alla realizzazione del codice. Successivamente l'algoritmo è stato utilizzato, con uno scopo differente, all'interno della blockchain in quanto è in grado di identificare rapidamente le transazioni ancora da convalidare e dare avvio all'esecuzione del processo stesso di convalida.

L'algoritmo di Hashcash di Adam Back ha indubbiamente fornito uno strumento informatico molto utile per lo sviluppo della blockchain, l'idea invece della cryptocurrency b-money, ideata da Wei Dai nel 1998, ha fornito una base concettuale molto solida sulla quale la tecnologia ha potuto svilupparsi. Wei Dai ha infatti proposto, nel suo paper di presentazione di b-money, la realizzazione di un sistema innovativo basato su due distinti protocolli:

- Un primo protocollo capace di garantire l'anonimato degli utenti partecipanti, grazie all'utilizzo di pseudonimi, e di preservare il database contenente tutte le informazioni relative alle transazioni effettuate;
- Un secondo capace, invece, di individuare il gruppo di partecipanti (Server) che ha il compito di processare le transazioni e pubblicarle così che queste possano essere approvate dai partecipanti al network.

Relativamente al primo protocollo Dai si preoccupò anche di definire come gli account dei singoli utenti sarebbero stati aggiornati, nonché il processo di funzionamento delle transazioni, definì dunque:

- Il sistema garantisce ad ogni utente la possibilità di creare delle monete in seguito alla risoluzione di un problema computazionale. La soluzione deve però essere resa pubblica a tutti i partecipanti della rete attraverso un broadcast, in questo modo gli utenti possono verificarla e, successivamente, quantificare la

potenza di calcolo ed il tempo adoperati dall'utente per la risoluzione del problema. Infine, su questa base, viene determinato il quantitativo di monete da emettere e attribuire all'utente per il lavoro svolto.

- Relativamente alle transazioni, queste, al fine di poter essere eseguite, devono anch'esse essere condivise dal soggetto emittente, a tutti i partecipanti tramite l'utilizzo di un broadcast, andando a definire il soggetto ricevente. Solo successivamente la pubblicazione del messaggio i partecipanti della rete possono dare avvio all'attività di risoluzione del problema e dunque all'approvazione della transazione, questa potrà essere poi eseguita solo qualora l'account del soggetto emittente contenga un quantitativo sufficiente di monete per completare la transazione.
- L'effettiva esecuzione del contratto necessita di un ulteriore condizione, è infatti necessario che venga determinato un ammontare di monete finalizzato a far fronte al rischio di default di una qualsiasi delle parti coinvolte. Per definire questo importo è necessaria una negoziazione tra i due soggetti interessati effettuata in presenza di un "arbitro" che funzioni di mediatore. Al termine della negoziazione le parti coinvolte devono condividere con l'arbitro e la controparte le proprie firme elettroniche, in modo da poter versare su di uno specifico account, creato appositamente per la transazione, le somme stabilite come risarcimento in caso di fallimento di una delle parti.
- Conclusa la transazione tutti i soggetti coinvolti hanno l'obbligo di condividerla con tutti gli altri partecipanti alla rete andando a specificare l'hash identificativo della stessa e la risoluzione dell'annesso problema matematico. Effettuata questa condivisione le monete versate in precedenza come garanzia possono essere restituite e l'account, su cui queste erano state versate, eliminato.
- Qualora le parti non siano in grado di raggiungere un accordo neanche con la mediazione dell'arbitro, esse devono richiedere un parere a tutti i partecipanti della rete relativamente al programma di multa o riparazione della transazione

in caso di inadempienza, preoccupandosi, inoltre, di allegare tutte le argomentazioni e le prove a favore della propria tesi. Successivamente i partecipanti alla transazione possono valutare le proposte ed eventualmente modificare gli account interessati.

- Sebbene Wei Dai nel suo paper fosse riuscito a definire in maniera molto chiara e dettagliata il funzionamento di b-money, questa valuta digitale rimase solo una proposta in quanto egli stesso si rese conto di come il primo protocollo fosse difficilmente realizzabile, e proprio in relazione a quest'ultimo scrisse:

"The first one is impractical, because it makes heavy use of a synchronous and unjammable anonymous broadcast channel."[1]

Andando ad affermare come la componente informatica, alla fine degli anni '90, rappresentasse ancora un enorme ostacolo per la nascita delle valute digitali e ancor di più per un sistema così complesso e articolato come quello pensato da Dai.

Nonostante l'impossibilità realizzativa, il progetto è però riuscito a fornire comunque delle basi solide per la nascita ed il successivo sviluppo della Blockchain e, in particolare, ha ispirato la realizzazione del progetto che, più di tutti, ha riscontrato successo: Bitcoin.

1.5 BITCOIN

L'importanza di Bitcoin nel campo della Blockchain e delle valute digitali è enorme, esso si configura come il vero capostipite di questa tecnologia che, nonostante sia stata teorizzata già da tempo, ha trovato una vera e propria espressione solo con la nascita di questa criptovaluta, che è solo la prima di una moltitudine di altre cryptocurrency nate successivamente le quali hanno, non solo apportato modifiche sostanziali alla struttura iniziale, ma anche fatto aumentare a dismisura l'interesse per

[1] Wei Dai; *B-money*; 1998

la Blockchain . Ed è proprio per questo che quando si parla di Bitcoin la si può definire come una criptovaluta di "prima generazione" in quanto è stata, insieme a poche altre, la prima a dare avvio allo sviluppo definitivo di una tecnologia che da tempo richiedeva un'attenzione maggiore.

Si è dunque creata, nel tempo, una forte associazione tra Bitcoin e Blockchain tanto che, col tempo, nell'ideale comune, i due termini sono divenuti quasi sinonimi proprio a sottolineare come l'avvento e la rilevanza di questa tecnologia siano dovute, per la stragrande maggioranza, proprio a questa criptovaluta.

Il periodo in cui nasce Bitcoin è emblematico e contribuisce a fornire alla Blockchain un'attenzione particolare, gli eventi successivi al 2007 hanno, infatti, contribuito ad alimentare le basi ideologiche sulle quali essa si fonda: la revisione completa dell'assetto economico mondiale, interamente basato sulle banche, resta il punto cardine di questa e fornisce tuttora linfa vitale al suo sviluppo.

Il 2007 verrà sicuramente ricordato come l'anno che ha dato vita ad una delle più grandi crisi finanziarie della storia e, non a caso, il 2008 è stato l'anno della pubblicazione del paper di presentazione di Bitcoin, proprio a voler sancire una rottura definitiva con il sistema economico tradizionale. Il paper in questione esordisce così:

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another ***without going through a financial institution****."*[2]

Fin dall'incipit è chiara l'intenzione dell'ideatore di voler superare la struttura tradizionale dei pagamenti aggirando gli istituti finanziari, attraverso la creazione di

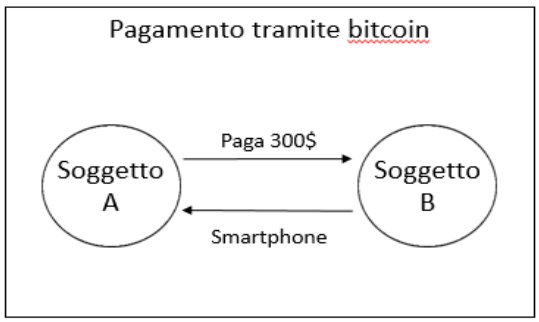
[2] Satoshi Nakamoto; *Bitcoin: A Peer-to-Peer Electronic Cash System*; 2008

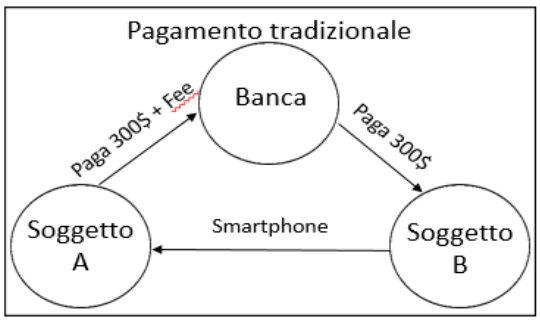
un sistema di pagamenti online capace di inviare denaro direttamente da un soggetto ad un altro senza dover necessariamente passare per una parte terza.

L'autore si firma "Satoshi Nakamoto", uno pseudonimo come quelli da lui stesso ideati per garantire l'anonimità all'interno del suo sistema. Tuttora lo scrittore resta ignoto al pubblico ma la struttura e il codice informatico da lui proposti sono, senza ombra di dubbio, una delle tecnologie più innovative e discusse degli ultimi anni.

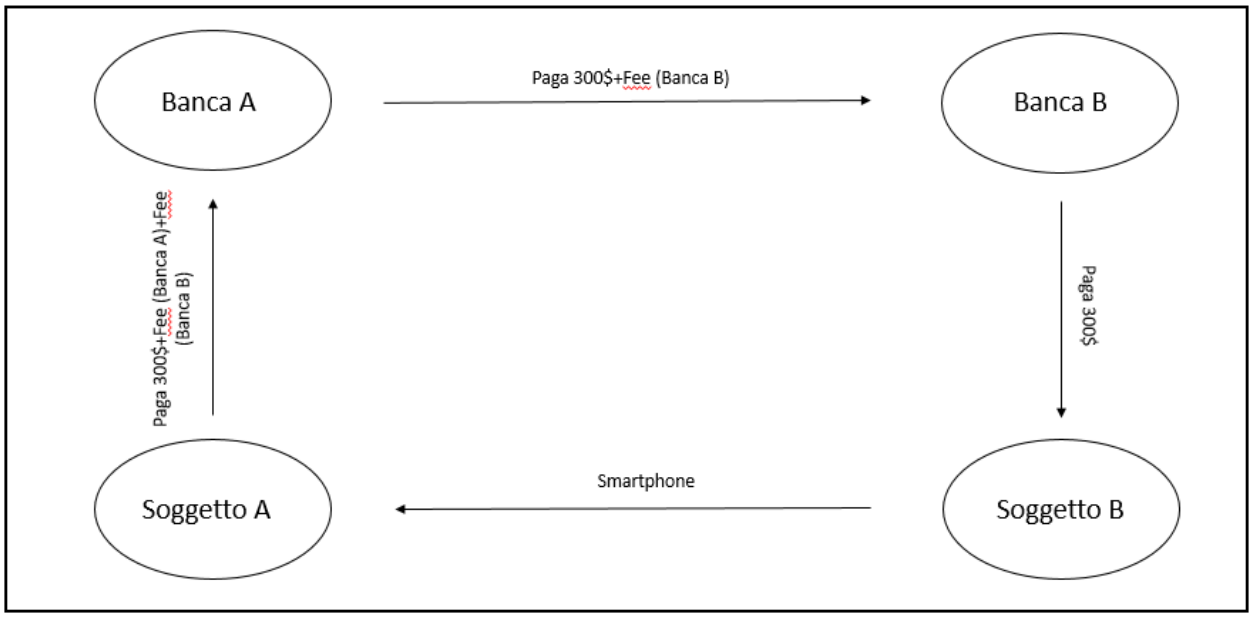
Il paper di Nakamoto attinge a piene mani dal b-money di Wei Dai e dall'algoritmo di Hashcash, descrive un sistema di pagamenti assolutamente rivoluzionario che ha visto la luce in via definitiva nel 2009 con il lancio di Bitcoin, una valuta completamente digitale che implementa la Blockchain esattamente come descritta da Nakamoto. Bitcoin riesce grazie al suo sistema a superare tutti i problemi delle valute digitali precedentemente realizzate e anche tutti i problemi delle valute tradizionali. Permette di effettuare pagamenti direttamente tra i soggetti coinvolti nelle transazioni senza far ricorso ad un terzo ente che ne assicuri il regolare svolgimento e, al tempo stesso, non permette alcun tipo di manipolazione delle monete evitando così di da dar vita a problemi di doppia spesa.

Nel sistema tradizionale un pagamento tra due soggetti può essere effettuato solo se vi è un ente terzo, generalmente una banca, che funge da garante, in particolare questo ha il compito di ricevere il denaro dal soggetto acquirente e, successivamente, di erogarlo al venditore facendo sì che nessun altro possa manipolarlo. Bitcoin, invece, permette un trasferimento diretto dall'acquirente al venditore senza passare per una banca e senza che ciò possa causare un problema di doppia spesa. Il vantaggio principale di poter cedere direttamente il denaro alla controparte è legato ai costi di transazione. Se si valuta il caso di un soggetto che effettua, ad esempio, l'acquisto online di uno smartphone per 300$, la situazione che verrebbe a configurarsi sarebbe di questo tipo:



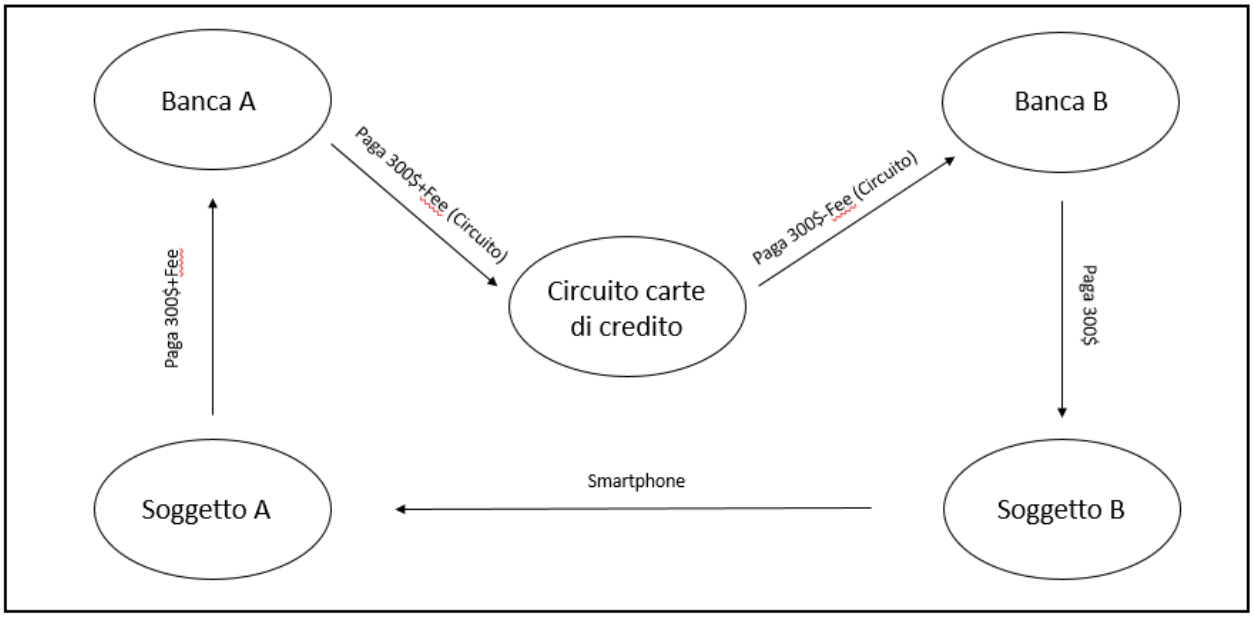


La banca, infatti, non si fa garante della transazione gratuitamente ma richiede un pagamento sotto forma di fee, che rende il trasferimento maggiormente oneroso per l'acquirente in quanto su di esso graverà un'ulteriore spesa oltre quella necessaria per l'acquisto del prodotto. Questo caso è, però, molto semplificato in quanto si presuppone che i due soggetti si affidino alla medesima banca, molto spesso capita, invece, che i due soggetti si affidino a banche differenti per cui il trasferimento di denaro seguirà un percorso ancora più complesso ed oneroso:



In questo caso infatti il soggetto A, acquirente dello smartphone, dovrebbe farsi carico non solo delle fee richieste dalla propria banca per gestire la transazione ma anche di quelle richieste dalla banca del soggetto B venditore. In questo scenario le due banche sono comunque in grado di effettuare un pagamento diretto tra loro, ma attualmente gli acquisti online possono essere effettuati solo ed unicamente grazie alla presenza

di ulteriori soggetti che permettano il trasferimento del denaro tra le banche, come nel caso dei circuiti delle carte di credito i quali rendono ulteriormente complesso il trasferimento:



Il denaro infatti per poter passare dalla banca A alla banca B deve passare per il circuito delle carta di credito adoperata per il pagamento, tale circuito effettua chiaramente l'operazione dietro il pagamento di una fee che viene divisa fra le banche, le quali faranno probabilmente gravare tali costi sull'acquirente. Il sistema può inolre ulteriormente complicarsi con l'aggiunta di nuovi soggetti causando un ulteriore aumento dei costi di transazione.

Attraverso Bitcoin è invece possibile effettuare un trasferimento diretto di denaro con conseguente abbattimento dei costi di transazione in quanto non è in alcun modo necessario passare per soggetti ulteriori che necessitano di essere remunerati per il lavoro da essi svolto. Inoltre la criptovaluta garantisce un maggior controllo del proprio denaro in quanto esso è effettivamente detenuto dall' utente, le banche infatti, sono a tutti gli effetti delle imprese le quali sono inevitabilmente chiamate a coprire una serie di costi nonché a ripagare tutti i propri azionisti fornendogli un rendimento. Per questi motivi il denaro dei conti corrente da parte dei clienti non è effettivamente presente all'interno della banca, in poiché questa lo adopera al fine di generare la redditività necessaria. Le banche, dunque, non dispongono del denaro dei propri

clienti ma solo di una piccola parte sufficiente a far fronte alle loro richieste di liquidità giornaliere, ciò che questi vantano, nei confronti degli istituti bancari, è infatti il solo diritto di restituzione ma, sebbene tale diritto risulti incondizionato e tutelato in vari modi dalla legge, nella pratica, essi non posseggono il proprio denaro. All'opposto il sistema di Bitcoin si basa su una serie di cosiddetti wallets, letteralmente dei "portafogli" digitali, all'interno dei quali i soggetti facenti parte della rete possono inserire le proprie monete e adoperarle in qualsiasi momento senza doverli richiedere ad altri soggetti, proprio perché essi già possiedono e gestiscono tutto il proprio denaro.

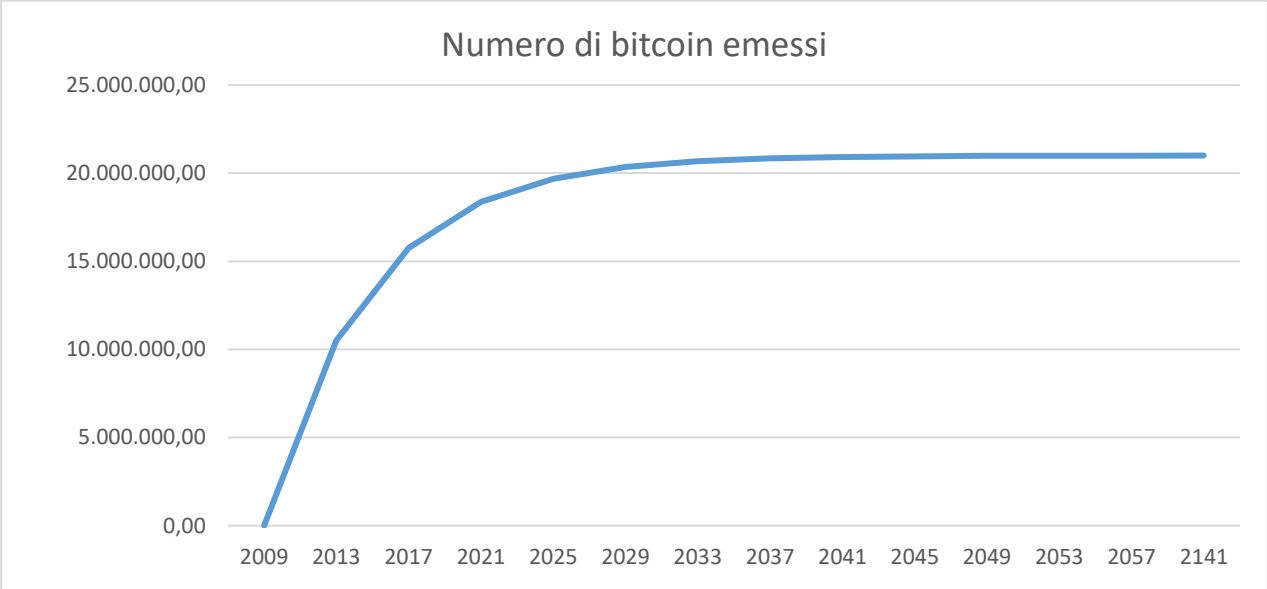
L'intero sistema di Bitcoin funziona in maniera molto semplice grazie l'utilizzo di chiavi di sicurezza pubbliche e private che operano in maniera simile a quelle utilizzate per l'invio di e-mail contenenti informazioni sensibili. In breve, due soggetti possono scambiarsi il denaro semplicemente conoscendo il codice identificativo del wallet della controparte e possedendo una coppia di chiavi private e di chiavi pubbliche. Si effettua dunque un'operazione di crittografia asimmetrica delle informazioni relative alla transazione che questi vogliono eseguire, queste poi, grazie ad un programma di hashing (SHA 256, nel caso specifico di Bitcoin), vengono compresse in una stringa di 64 caratteri incomprensibili che, al tempo stesso, permette di contraddistinguere univocamente la transazione. Successivamente il messaggio generato viene condiviso a tutto il network dei partecipanti che ha il difficile compito di garantire la validità dell'operazione andando a risolvere un complicato problema matematico. Tale risoluzione necessita di un tempo più o meno lungo a seconda del quantitativo di risorse computazionali messe a disposizione dalla rete dei partecipanti, detti "nodi", i quali sono incentivati a contribuire alla risoluzione del quesito grazie ad un sistema di pagamenti che prevede un versamento in Bitcoin direttamente sui wallets degli utenti che hanno fornito risorse per il processo di convalida. Gli importi dei versamenti sono definiti in maniera proporzionale al tempo e alla potenza di calcolo fornita da ciascuno e sulla base di un ammontare complessivo predefinito. Proprio grazie a queste "ricompense" il sistema di Bitcoin, e dunque la Blockchain,

riesce ad eliminare la figura del terzo ente con funzione di garante, lasciando ai partecipanti il compito di convalidare ogni singola transazione. Così facendo si è riusciti ad evitare di dover far affidamento su un unico ente centrale poiché, sebbene la transazione potrebbe essere approvata da chi detiene la maggioranza della potenza di calcolo complessiva, la totalità di questa risulta comunque essere costituita da un numeroso quantitativo di soggetti differenti che rendono pressoché impossibile la detenzione di una simile quantità di potenza di calcolo da parte di un singolo individuo. Appare dunque molto difficile che qualcuno possa appropriarsi totalmente del processo di convalida e che possa sfruttare questa sua posizione per alterare il contenuto delle transazioni e manipolare le monete a piacimento.

Per rendere ulteriormente complicata la manipolazione delle transazioni, come già detto in precedenza, viene adoperata una funzione di hash la quale garantisce l'assoluta segretezza della transazione in quanto la forzatura del digest, ossia la serie di caratteri risultante dalla funzione, è statisticamente impossibile da eseguire in un lasso di tempo sufficientemente breve, anche disponendo di enormi risorse computazionali, ciò permette anche di fornire un livello di privacy particolarmente elevato, limitando la conoscenza delle informazioni relative alla transazione ai singoli partecipanti.

L'attività di convalida delle operazioni ha come ulteriore obiettivo l'emissione di nuove monete, infatti, la ricompensa fornita a coloro che hanno partecipato alla risoluzione del sistema matematico, i cosiddetti "miner", viene automaticamente generata dal sistema il quale, di fatto, non fa altro che creare e attribuire a questi ultimi delle nuove monete. Tale emissione è pensata in modo da evitare che questa possa fenomeni di svalutazione dovuti ad un aumento eccessivo di monete circolanti, per questo motivo il sistema prevede che il tutto sia regolato da un algoritmo che riduce, col passare del numero di blocchi risolti (ogni 210000), il numero di monete massime che possono essere generate successivamente la risoluzione di un blocco. Inizialmente il numero di Bitcoin emessi era pari a 50 unità per ciascun blocco, un quantitativo che nel giro di pochi anni si è dimezzato passando prima a 25 e poi a 12,5. In questo modo

è possibile controllare e limitare il numero di Bitcoin in circolazione il quale non può, proprio per via di questa funzione, che tendere asintoticamente ad un valore massimo di circa 21 milioni, limite che dovrebbe essere raggiunto, alle velocità attuali, solo nel 2140, anche se già nel 2040 l'algoritmo dovrebbe aver generato la stragrande maggioranza dei bitcoin.



Anno di riferimento	Numero di bitcoin in circolazione	% bitcoin emessi rispetto al totale	Numero di bitcoin emesso per ogni blocco convalidato
2009	0,00	0,00000000	50,00000000
2013	10.500.000,00	0,50000000	25,00000000
2017	15.750.000,00	0,75000000	12,50000000
2021	18.375.000,00	0,87500000	6,25000000
2025	19.687.500,00	0,93750000	3,12500000
2029	20.343.750,00	0,96875000	1,56250000
2033	20.671.875,00	0,98437500	0,78125000
2037	20.835.937,50	0,99218750	0,39062500
2041	20.917.968,75	0,99609375	0,19531250
2045	20.958.984,38	0,99804688	0,09765625
2049	20.979.492,19	0,99902344	0,04882813
2053	20.989.746,09	0,99951172	0,02441406
2057	20.994.873,05	0,99975586	0,01220703
2141	21.000.000,00	1,00000000	0,00000001

Per quanto il limite asintotico risulti lontano nel tempo, Questo determina ugualmente una sorta di “scadenza” al sistema di incentivazione, per questo motivo, in maniera non molto dissimile da come avviene nel sistema tradizionale, Nakamoto ha già previsto che gli acquirenti possano fornire un ulteriore pagamento al servizio fornito dai miner, possono dunque, in maniera del tutto autonoma, decidere di pagare ulteriori commissioni le quali però risultano, a differenza di quelle già presenti nel sistema attuale, impostate a piacimento dall’acquirente il quale può determinarne l’importo. Un acquirente è di fatto libero di non pagare ma così facendo esso dovrà inevitabilmente fare i conti con l’effetto disincentivante generato da un simile comportamento, infatti i miner, al fine di aumentare i propri guadagni, si concentrano a risolvere per prime quelle transazioni che forniscono loro maggiori guadagni, per cui a commissioni maggiori corrispondono, generalmente, tempi di convalida minori.

Il sistema progettato da Nakamoto ha anch’esso dei limiti e dei difetti legati ad aspetti tecnici e giuridici. Sicuramente tra i limiti più rilevanti che ancora zavorrano l’ascesa di Bitcoin vi sono i lunghi tempi di attesa per l’approvazione delle transazioni, proprio perché il sistema è pensato per evitare qualunque sorta di manipolazione esso risulta,

al tempo stesso, così complesso da rendere impossibile una rapida esecuzione di tutte le sue fasi, il tempo medio di approvazione di un blocco è, infatti, di circa 10 minuti ma non sono mancati i giorni in cui le transazioni hanno richiesto molte ore di tempo per poter essere approvate. Le tempistiche dunque, seppur accettabili in condizioni favorevoli, risultano, ad oggi, ancora molto lontane dalle velocità di transazione garantite dalle valute e dai sistemi di trasferimento tradizionali.

Altro punto critico è rappresentato dall'anonimità che il sistema garantisce agli utenti, infatti, per quanto possa essere importante la privacy, questa non può essere estesa eccessivamente senza causare necessariamente delle complicazioni relativamente al controllo dell'evasione fiscale o al traffico di merci illegali, non è infatti un caso che questa criptovaluta sia la più usata per perseguire fini illeciti e ed effettuare transazioni sul cosiddetto "dark web".

Tutti questi sono inoltre solo alcuni dei limiti che Bitcoin e anche le altre criptovalute presentano e che più nel dettaglio verranno analizzati e discussi successivamente nel capitolo terzo. Nonostante questi però Bitcoin si configura, senza alcun dubbio, come il primo esperimento, realmente riuscito, di una serie di tentativi che non erano riusciti negli anni precedenti a mostrare la vera forza di un'idea rivoluzionaria, Nakamoto, invece, è riuscito a creare qualcosa capace di attrarre realmente l'interesse delle persone, tanto che, con il passare degli anni, si è giunti ad un punto in cui non sono più solamente in pochi a sostenere questa tecnologia, ma anche imprese e intermediari finanziari si sono resi conto delle potenzialità di questa tanto che hanno iniziato ad investire in molte attività finalizzate allo studio e alla comprensione del suo funzionamento, le quali successivamente si sono sempre più focalizzate sul dar vita a nuove realtà imprenditoriali capaci di esplorare i molteplici campi applicativi di questa tecnologia, tutto ciò perché ritengono che, in un futuro non molto lontano, la Blockchain possa dar vita ad un nuovo "Blue Ocean", aprendo innumerevoli nuove possibilità d'investimento.

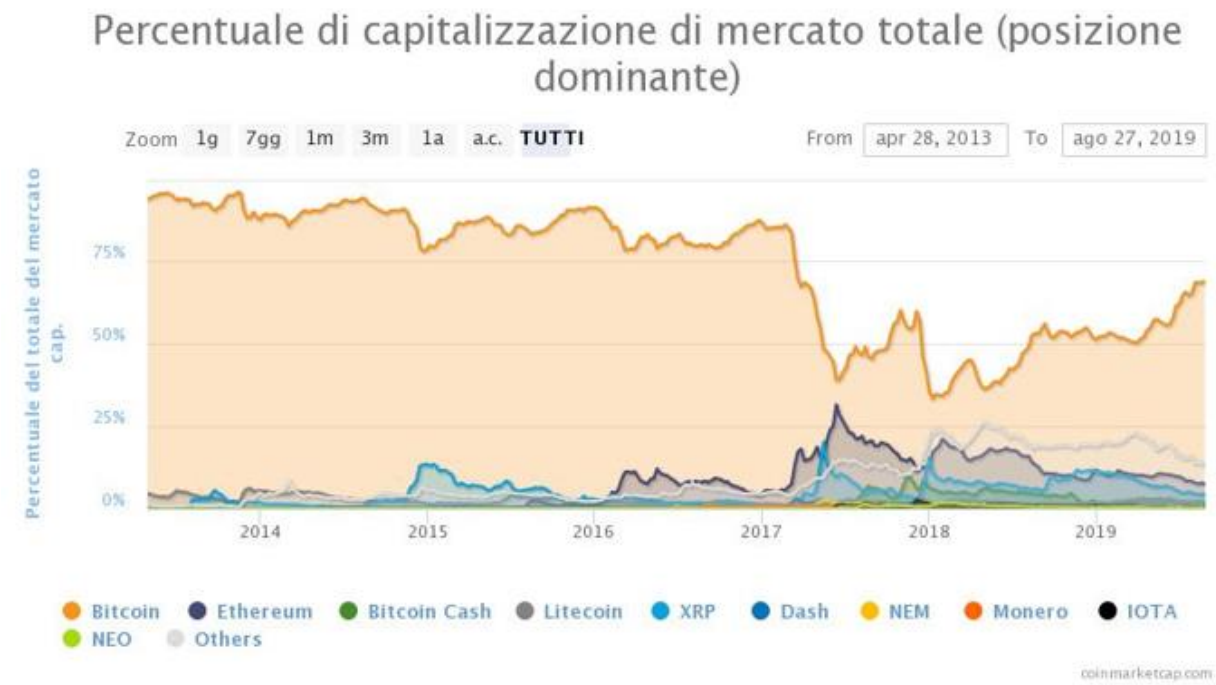
Bitcoin rappresenta quindi un punto di svolta nello sviluppo di un'idea rivoluzionaria, se prima della sua nascita essa appariva un'utopia piuttosto che un qualcosa di concreto e realizzabile, con la nascita di Bitcoin ci si è resi conto delle vere potenzialità di questa tecnologia. Una presa di coscienza che è cresciuta successivamente, in maniera ancor più decisa, grazie alla velocità con cui una moltitudine di progetti sono nati subito dopo Bitcoin. Volendo potremmo, infatti, definire questa prima criptovaluta come il trampolino di lancio della Blockchain che risulta la "vera protagonista" di questa rivoluzione tecnologica, tanto che forse con Bitcoin, Nakamoto abbia voluto, più di tutto il resto, rendere disponibile una tecnologia innovativa capace di scardinare e sostituire le fondamenta di un sistema, ormai sempre più obsoleto e incapace di soddisfare pienamente la società moderna. A prova di ciò Nakamoto ha infatti lanciato Bitcoin nel 2009 come un software open source, ossia un programma disponibile a tutti, distribuito gratuitamente, il cui codice di programmazione è a disposizione di tutti coloro che siano interessati a conoscerlo nonché a modificarlo e migliorarlo a piacimento, senza rischiare alcun tipo di sanzione. Ciò ha permesso la nascita in pochi anni di innumerevoli progetti che adoperano la stessa tecnologia in maniera similare, che hanno permesso di dar vita a attività mai viste prima che hanno cercato e cercano tuttora di superare quei numerosi limiti che la tecnologia ancora possiede e che si sono cimentate nel testare le capacità della Blockchain nei campi di applicazione più svariati e anche totalmente differenti da quelli individuati alla nascita di Bitcoin.

Anche i dati confermano come l'interesse per le criptovalute sia cresciuto in maniera esponenziale, se si analizza il totale dei soldi capitalizzati all'interno dei progetti crypto è possibile notare come questi siano aumentati in maniera molto rapida nel giro di pochi anni:

È evidente come dai primi anni dalla nascita di Bitcoin il quantitativo di denaro circolante in questo nuovo mercato abbia conosciuto degli incrementi significativi, sebbene i picchi massimi raggiunti, che si aggiravano intorno ai 1000 miliardi di dollari, siano il frutto di una fase fortemente speculativa, è comunque possibile notare come l'ultimo anno abbia visto una tendenza a stabilizzarsi intorno ai 250 miliardi di dollari, una cifra non da poco soprattutto se la si considera in relazione agli anni precedenti, come il 2013, quando essa contava poco più di qualche miliardo.

Andando ad analizzare la capitalizzazione delle prime cinque criptovalute possiamo anche notare come la stragrande maggioranza di questa capitalizzazione risulti ancora dovuta al Bitcoin che, a distanza di anni risulta ancora la valuta che più di tutte le altre riscontra la fiducia delle persone:

Se si valuta però come la capitalizzazione di Bitcoin sia variata in relazione alla capitalizzazione totale possiamo notare che nel corso degli anni questa abbia subito una drastica riduzione che sancisse proprio come buona parte dell'interesse nato intorno alle criptovalute, sia frutto di tutta quella serie di nuovi progetti che sono nati successivamente Bitcoin e che hanno dato avvio ad un processo di sviluppo della tecnologia ben più significativo, migliorando considerevolmente le aspettative degli investitori relativamente al futuro della Blockchain.



CAPITOLO II
I CASI ETHEREUM E RIPPLE

2.1 ETHEREUM

Il lancio di Bitcoin nel 2009 ha permesso alle criptovalute di ritagliarsi uno spazio significativo nel mondo della ricerca tecnologica. L'attenzione non si è focalizzata tanto sul progetto Bitcoin quanto sulla Blockchain, infatti centinaia di nuove criptovalute sono nate poco dopo il lancio di Bitcoin, presentando strutture e caratteristiche differenti, sebbene esse abbiano mantenuto in buona parte sia la componente tecnologica che quella ideologica.

Tra i progetti Ethereum è sicuramente uno di quelli meglio riusciti, il suo sviluppo è partito nel 2013 da un'idea di Vitalik Buterin, all'epoca un diciannovenne, che riuscì a riunire un team di lavoro per sviluppare una piattaforma finalizzata a facilitare e incentivare la creazione di nuovi programmi e progetti che adottassero la Blockchain.

Ethereum si discosta in maniera significativa da Bitcoin in termini di obiettivi in quanto tenta di diffondere quanto più possibile la Blockchain, spingendo la realizzazione di programmi in campi anche molto diversi da quello delle transazioni. Nasce con l'obiettivo di voler essere una piattaforma capace di fornire una base solida sulla quale, chiunque abbia conoscenze sufficienti in ambito di programmazione, può dar vita al proprio programma che adotti la Blockchain e che, anche grazie all'ausilio degli smart contracts, possa dar vita ad un progetto innovativo. La vera forza della piattaforma risiede nella possibilità di integrare, all'interno di questi programmi, un sistema di pagamento unico sviluppato dalla medesima società la quale, attraverso la criptovaluta Ether (ETH), permette di eseguire qualunque tipo di transazione. Così facendo, Buterin ed il suo team di sviluppatori, sono riusciti a realizzare una rete che cresce incessantemente grazie alla capacità di attirare un sempre maggior numero di

soggetti interessati ad adoperare gli ETH pur di usufruire dei programmi sviluppati sulla piattaforma.

Sotto un profilo tecnico la criptovaluta di Ethereum opera in maniera molto simile a Bitcoin, gli sviluppatori hanno voluto conservare la struttura decentralizzata, l'anonimato degli utenti e il sistema di mining ma si sono anche preoccupati di velocizzare i processi di convalida. La criptovaluta costituisce comunque solo una componente residuale al sistema di Buterin, il cuore di Ethereum è infatti la piattaforma di sviluppo che permette a tutti di poter utilizzare la Blockchain, con questa è possibile realizzare i programmi più svariati, che permettono di effettuare le più svariate operazioni come l'acquisto di polizze assicurative estremamente specifiche, favorendo anche la nascita di mercati non regolamentati sui quali poter scambiare attività finanziarie non standardizzate. Questo tipo di operazioni sono possibili grazie alla possibilità, fornita dalla piattaforma, di realizzare e pagare i contratti in maniera del tutto automatica grazie all'utilizzo degli smart contracts. Le applicazioni sono insomma molteplici e non hanno limiti se non quelli imposti dall'ingegno degli sviluppatori grazie alla piattaforma sono infatti nati negli ultimi anni più di 90 applicazioni dalle diverse funzionalità che hanno permesso una più rapida diffusione della tecnologia. Questa capacità di Ethereum di attirare l'attenzione su di sé è sancita dai risultati ottenuti essendo gli Ether divenuti la seconda criptovaluta per capitalizzazione, prossima, al momento della stesura, ai 20 miliardi di dollari.

2.2 LE APPLICAZIONI

Molte sono le applicazioni sviluppate tramite la piattaforma di Ethereum, tra le tante, alcune hanno raggiunto un discreto successo evidenziando come la Blockchain possa essere adoperata in campi differenti da quello delle transazioni:

- **Gitcoin**: è un network realizzato per incentivare gli sviluppatori di software alla realizzazione di programmi open source. Molto semplicemente, chiunque

abbia un'esigenza particolare o un problema da risolvere può pubblicare una cosiddetta "Bounty" la quale può essere visualizzata da tutti i programmatori che adoperano la piattaforma, questi possono valutare la richiesta e, qualora interessati, possono effettuare una "candidatura" finalizzata alla realizzazione di un programma capace di far fronte alle esigenze del cliente. Una volta ultimato questo viene inviato al cliente, il quale effettua una propria valutazione, se il programma soddisfa le sue esigenze, egli lo approva effettuando in automatico il pagamento in ETH promesso nella "Bounty" agli sviluppatori. Il network riesce così a motivare e incentivare i programmatori nella risoluzione dei problemi posti dagli utenti, l'unica condizione alla quale essi sono sottoposti è la pubblicazione del software come open source.

- **Cent**: è un social network realizzato per incentivare le pubblicazioni di post dall'elevato contenuto, il sistema prevede che i partecipanti possano leggere gli articoli e, successivamente, effettuare delle offerte in ETH agli autori degli stessi. Di queste donazioni, però, solo il 25% del loro ammontare viene effettivamente versato al creatore del contenuto in quanto, la rimanente parte, viene, invece, ridistribuita tra tutti i precedenti donatori, in tal modo Cent ha cercato di creare un sistema all'interno del quale le offerte incentivino non solo i realizzatori dei post ma anche i donatori stessi, cosicché anch'essi siano incentivati ad effettuare donazioni a post dal contenuto rilevante e a continuare a farlo anche in futuro.
- **OpenLaw**: è una piattaforma realizzata per velocizzare e ridurre i costi per la stesura dei contratti. Due dei problemi più grandi legati alla stipula di un contratto sono infatti il tempo di attesa ed i costi elevati per la stesura, è infatti necessaria la presenza di una figura specializzata che si preoccupi di curare l'aspetto formale e giuridico dello stesso, la quale però implica dei costi più o meno elevati e dei tempi più o meno lunghi, per questi motivi gli sviluppatori di OpenLaw si sono impegnati nel cercare di realizzare una piattaforma sulla quale, attraverso l'utilizzo degli smart contracts, fosse possibile stipulare tutta

una serie di contratti standardizzati, in maniera molto rapida riducendo drasticamente costi e tempi. Con OpenLaw, semplicemente definendo la tipologia di contratto ed inserendo tutti i dati necessari, è infatti possibile generare automaticamente diverse tipologie di contratti inoltre, grazie ad Ethereum, il pagamento degli importi definiti su base contrattuale può essere effettuato direttamente dalla piattaforma tramite una criptovaluta, chiamata DAI, sviluppata anch'essa sulla piattaforma di Ethereum.

2.3 MAKERDAO

La criptovaluta appena citata necessita di una menzione particolare poiché fornisce un ulteriore esempio che dimostra l'importanza di Ethereum nel mondo della Blockchain permette, al contempo, l'analisi di uno dei progetti più recenti e interessanti sviluppati in ambito criptovalute.

MakerDAO è un progetto partito nel 2017 con l'obiettivo di risolvere uno dei più grandi problemi delle criptovalute: la volatilità.

Se si analizza l'andamento dei tassi di cambio delle principali criptovalute, come Ether e Bitcoin, con il dollaro statunitense è possibile notare come tali valori risultino estremamente volatili:

Date	Adj close BTC/USD	Rendimenti BTC/USD	Adj close ETH/USD	Rendimenti ETH/USD
2017-06-30	$ 2.883,27	49,6080%	$ 201,33	65,6910%
2017-07-31	$ 4.735,11	-8,2391%	$ 388,33	-24,8882%
2017-08-31	$ 4.360,62	39,1658%	$ 302,77	0,2869%
2017-09-30	$ 6.451,24	43,2974%	$ 303,64	35,9158%
2017-11-01	$ 9.946,76	33,1067%	$ 434,85	53,3175%
2017-12-01	$ 13.850,40	-30,3297%	$ 741,13	40,5119%
2018-01-01	$ 10.226,86	1,0464%	$ 1.111,31	-26,6295%
2018-02-01	$ 10.334,44	-39,7637%	$ 851,50	-77,0471%
2018-03-01	$ 6.943,77	28,6611%	$ 394,07	53,0809%
2018-03-31	$ 9.248,45	-20,9266%	$ 670,04	-14,9097%
2018-04-30	$ 7.502,15	-16,1179%	$ 577,23	-24,1422%
2018-05-31	$ 6.385,38	19,1783%	$ 453,42	-4,8416%
2018-06-30	$ 7.735,30	-9,6040%	$ 431,99	-42,7702%
2018-07-31	$ 7.026,96	-5,9099%	$ 281,66	-19,1380%
2018-08-31	$ 6.623,71	-4,3365%	$ 232,60	-16,1811%
2018-09-30	$ 6.342,61	-45,8581%	$ 197,85	-56,1272%
2018-11-01	$ 4.009,67	-6,7649%	$ 112,87	16,7790%
2018-12-01	$ 3.747,39	-8,7296%	$ 133,49	-22,2226%
2019-01-01	$ 3.434,13	10,7369%	$ 106,89	24,2985%
2019-02-01	$ 3.823,37	7,2945%	$ 136,29	4,3855%
2019-03-01	$ 4.112,69	26,3139%	$ 142,40	14,3602%
2019-03-31	$ 5.350,64	46,8793%	$ 164,39	48,6579%
2019-04-30	$ 8.550,67	5,7837%	$ 267,42	-1,3364%
2019-05-31	$ 9.059,80	-	$ 263,87	-

Utilizzando le osservazioni mensili degli ultimi due anni e calcolando i rendimenti logaritmici è possibile analizzare la volatilità dei tassi di cambio col dollaro statunitense calcolandone la deviazione standard:

Volatilità	
BTC/USD	ETH/USD
27,2327%	37,2563%

I risultati mettono in luce una volatilità piuttosto elevata sintomo di scarsa stabilità delle quotazioni di queste criptovalute. Nella valutazione di questi risultati c'è, però, da tenere in considerazione che essi sono comprensivi dei valori relative al periodo che intercorre tra ottobre 2017 e marzo 2018 durante il quale vi è stato, dapprima, un enorme apprezzamento delle due criptovalute e, successivamente, un altrettanto

rilevante tracollo dello stesso; ciò ha certamente influenzato in maniera significativa valore delle deviazioni standard e dunque delle volatilità, ma anche analizzando i dati mensili dell'ultimo anno e, per una valutazione maggiormente significativa, quelli degli ultimi quattro anni, il risultato non varia molto e si registra comunque una volatilità molto elevata specialmente se confrontata con un cambio di valute tradizionali come può essere l'euro-dollaro (EUR/USD):

Volatilità 1 anno		
BTC/USD	**ETH/USD**	**EUR/USD**
22,8210%	29,1508%	1,0388%

Volatilità 4 anni		
BTC/USD	**ETH/USD**	**EUR/USD**
22,3486%	42,3990%	1,9720%

Questo ci permette di capire come la variabilità dei tassi di cambio di BTC e ETH limiti fortemente la possibilità di effettuare delle transazioni proprio perché il valore di queste oscilla in maniera significativa molto rapidamente nell'arco di un singolo mese, ma la situazione non migliora se si valutano le variazioni che esse fanno registrare nel corso di una singola giornata, non è infatti raro vedere, nel mondo delle criptovalute, apprezzamenti o deprezzamenti del 10% anche nel giro di poche ore.
Per far fronte a questo problema Maker (azienda ideatrice di MakerDAO) ha dato vita ad un sistema piuttosto complesso che è stato però capace di fornire degli ottimi risultati in termini di volatilità, tanto che il DAI (questo è il nome della criptovaluta) ha registrato ha fatto registrare, dal momento della sua prima emissione avvenuta nel Febbraio 2018, una volatilità pari a:

Volatilità DAI/USD da Febbraio 2018
1,1650%

Questi risultati hanno permesso di annoverare DAI tra le cosiddette "stablecoin" ossia quelle criptovalute ideate al fine di mantenere il proprio valore stabile nel tempo.
Già da tempo vi sono diverse criptovalute di questo tipo ma indubbiamente Maker è riuscita a sviluppare un sistema innovativo capace di garantire, oltre alla stabilità della valuta, la decentralizzazione della stessa, infatti criptovalute simili sono riuscite a raggiungere il proprio obiettivo rinunciando alla struttura decentralizzata e ancorandosi ad asset o valute tradizionali eliminando, di fatto, un elemento distintivo delle criptovalute.
L'obiettivo di Maker è garantire il valore dei DAI in prossimità del valore del dollaro, ancorandolo e mantenendo un rapporto di cambio 1:1, a tal fine Maker si avvale di un sistema che opera in maniera simile ad una banca centrale, esso modifica la domanda di moneta al fine di farne variare il prezzo e di bilanciarne il tasso di cambio col dollaro. Il funzionamento è piuttosto complesso e articolato ma funzionale: Maker si avvale di ben due differenti criptovalute: DAI e MKR, le quali operano insieme al fine di far funzionare al meglio il sistema; la prima criptovaluta risulta essere il vero strumento di scambio per eseguire qualunque tipo di transazione ed è la criptovaluta circolante vera e propria; la seconda ha invece il compito di garantire il corretto funzionamento di DAI e del suo sistema di stabilizzazione. Nello specifico quando un soggetto vuole effettuare una transazione esso deve necessariamente procurarsi dei DAI, a tal fine Maker si avvale delle cosiddette CDPs (Collateralized Debt Positions) attraverso le quali, in maniera non dissimile da un repurchase agreement (o pronti contro termine), si ottengono dei DAI in cambio di una somma di Ether, tale operazione viene effettuata sulla base di un tasso di cambio prestabilito. Questa conversione ha ovviamente un costo, definito sulla base di un tasso d'interesse, che il soggetto dovrà necessariamente sostenere ogniqualvolta vorrà riconvertire i DAI ottenuti in Ether. Ammettiamo ad esempio che una persona voglia ottenere 100 DAI il cui valore è circa pari a 100$, per poterlo fare è necessario che questo soggetto crei un CDP versando un ammontare di Ether pari a 100$ ossia 0,35 Ether (al momento della stesura un Ether equivale a circa 287$), questi verranno "congelati" fino al momento della riconversione, la quale potrà avvenire solo qualora il soggetto sia in

grado di versare nuovamente i 100 DAI ricevuti in precedenza e maggiorati del costo, determinato in percentuale sul valore dei DAI dal tasso d'interesse, il quale andrà obbligatoriamente pagato in MKR. Un problema che Maker ha dovuto affrontare è la possibilità che le variazioni di prezzo degli Ether possano influenzare in maniera significativa il prezzo dei DAI, al fine di evitare questa situazione il sistema è stato realizzato pensando a qualsiasi tipo di evenienza per fronteggiare qualunque variazione compresa una significativa discesa del prezzo degli Ether. Per questo motivo per poter creare un CDP il sistema prevede che sia necessario versare un quantitativo di collaterale il cui valore risulti superiore al valore dei DAI ottenuti, ciascun CDP presenta inoltre un proprio tasso di debito specifico determinato dai possessori dei MKR: una delle caratteristiche peculiari di Maker è proprio questa, i possessori dei MKR hanno, di fatto, la possibilità di controllare il sistema, più in particolare, essi possono gestire una moltitudine di aspetti come il tasso di debito di ciascun CDP permettendo al sistema di funzionare al meglio. Questa caratteristica pone però anche un problema legato alla possibilità che i possessori dei MKR possano operare in maniera scorretta causando problemi al sistema; in realtà l'apparato sviluppato da Maker è pensato al fine di incentivare economicamente i possessori dei MKR e a farli operare nella maniera più attenta e diligente possibile.

Tornando all'esempio precedente per ottenere 100 DAI un soggetto dovrà versare un ammontare di Ether il cui valore risulti superiore a 100$, tale importo è definito dal tasso di debito determinato dai possessori di MKR, così facendo Maker riesce a far fronte al problema dell'insolvenza che potrebbe generarsi in caso di deprezzamento del collaterale, il quantitativo maggiorato di ETH non può però superare un livello massimo pari al 60% del valore dei DAI ricevuti, per cui, nel caso dell'esempio, il soggetto potrà essere chiamato a versare un massimo di 160$ di Ether. Tale livello è determinato sulla base della rischiosità del CDP definita sulla base delle fluttuazioni del prezzo di Ether, se il livello massimo dovesse essere sforato, il sistema, al fine di impedire l'insolvenza di alcuni utenti, fornisce a chiunque la possibilità di poter chiudere il CDP ottenendo in cambio tutto il collaterale in esso versato. Questo meccanismo fa sì che qualora vi sia un aumento progressivo del proprio rapporto di

debito, il soggetto interessato sarà incentivato a chiudere rapidamente i CDP proprio per evitare di perdere il collaterale.

Spiegati gli elementi di base del sistema, c'è ancora da definire come questo riesca effettivamente a mantenere stabile il valore dei DAI: come detto il valore della criptovaluta è ancorato al dollaro, per cui il valore target che la valuta tenta di raggiungere è pari a 1$, al fine di perseguire questo obiettivo è stato sviluppato il cosiddetto TRFM (Target Rate Feedback Mechanism) il quale spinge il DAI a seguire l'andamento del dollaro. In sostanza, quando il valore della criptovaluta scende al di sotto del dollaro (consideriamo un deprezzamento del 1%, per cui 1 DAI varrà in questo caso 0,99$), il TRFM si preoccupa di innalzare il valore del DAI del 1%, così che tutti i soggetti siano incentivati ad acquistare nuovi DAI per ottenere un profitto sicuro, in quanto acquisteranno a 0,99$ una valuta del valore di 1$, chiaramente con l'aumentare della domanda di DAI inevitabilmente aumenterà anche il suo valore fino al punto in cui questo non raggiungerà il valore target di 1$. Il meccanismo funziona in maniera opposta nel caso in cui il DAI dovesse superare il valore del dollaro, il TRFM sarebbe allora negativo e disincentiverebbe l'acquisto di DAI andandone a ridurre la domanda e quindi il prezzo.

Maker si è preoccupata anche di pensare ad una eventuale soluzione "finale" nel caso in cui il sistema dovesse smettere di funzionare o essere attaccato a livello informatico, è infatti possibile sciogliere l'intero sistema nel caso in cui la maggioranza dei possessori di Maker siano d'accordo nel ritenere che il sistema non sia più in grado di gestire la situazione creatasi, in questo caso, come "ultima spiaggia", tutti i CDP verranno automaticamente ripagati e gli Ether, impiegati come collaterali, restituiti.

2.4 RIPPLE

Dopo aver trattato della piattaforma Ethereum non è possibile non parlare di Ripple, un altro progetto molto interessante che, a partire dal 2012, ha suscitato un enorme

interesse e al contempo molte polemiche tra i "puristi" delle criptovalute e della blockchain. La società Ripple ha, infatti, realizzato un sistema di pagamento utilizzabile dalle sole banche e finalizzato a sostituire il già presente sistema di pagamento internazionale SWIFT. Sono stati proprio il target ed il funzionamento di Ripple che hanno suscitato più di qualche dubbio tra coloro che hanno sempre intravisto nella Blockchain qualcosa di più di una semplice tecnologia, ritenendolo un strumento capace di cambiare radicalmente quel sistema economico e bancario che da tempo suscita non poche perplessità. L'idea di Ripple ha però mostrato come la Blockchain sia in grado di supportare il sistema già esistente andandolo a rafforzare laddove questo risulta carente senza doverlo necessariamente stravolgere, per questo l'azienda, ad oggi, si configura come una delle meglio riuscite nel settore nonché una tra quelle col più alto potenziale di crescita.

La società è nata al fine di dar vita ad un sistema di pagamenti sostitutivo a quello attuale realizzato dall'omonima società SWIFT (Society for Worldwide Interbank Financial Telecommunication), questo è oramai adottato da anni da tutte le principali banche del mondo e permette a queste di effettuare qualunque tipo di transazione internazionale. Lo SWIFT nonostante esista da molti anni (1973 nascita della SWIFT), non è però mai riuscito a risolvere una serie di problemi che ne riducono l'efficienza, in particolare: la lentezza delle transazioni che impiegano alcuni giorni prima di poter essere convalidate ed effettivamente eseguite; l'alto tasso di fallimento relativo all'esecuzione delle transazioni, prossimo al 4%; gli elevati costi di transazione che rendono il sistema piuttosto oneroso.

Con l'aiuto della Blockchain, Ripple si è preoccupata di realizzare una piattaforma che risolvesse tutti questi problemi. A tal fine è stato necessario rivedere alcune delle caratteristiche distintive della Blockchain: un primo elemento assolutamente assente è il mining, non è infatti possibile per gli utenti partecipare ai processi di convalida né dunque essere premiati con l'emissione di nuove monete, le transazioni sono infatti convalidate grazie al consenso dei partecipanti, ossia coloro che si sono dimostrati di essere degni di fiducia all'interno della rete i quali possono così fare da garanti per l'esecuzione delle transazioni; proprio questo elemento definisce un secondo aspetto

peculiare di Ripple il quale ha optato per una struttura decentralizzata ben più contenuta rispetto ad altri sistemi. Il "potere" di controllo delle transazioni è infatti nelle mani di pochi soggetti autorizzati individuati dalla totalità dei partecipanti.

L'esecuzione delle transazioni in Ripple avviene grazie a una criptovaluta, omonima alla società, la cui sigla identificativa è XRP, con essa le banche possono effettuare le medesime transazioni che eseguono normalmente con il sistema SWIFT, ma in maniera istantanea, sicura e a costi decisamente più contenuti. Per semplificare, una banca che volesse effettuare un trasferimento di denaro tramite Ripple, può farlo senza alcun tipo di problema a prescindere dalla localizzazione geografica del ricevente e dalla valuta in cui questa transazione dev'essere denominata. Grazie ad una serie di market maker, le banche possono effettuare i trasferimenti adoperando una piattaforma, appositamente sviluppata da Ripple, che automaticamente provvede: ad una prima conversione della valuta della banca emittente in XRP, all'invio di questi alla banca ricevente e, infine, ad una seconda conversione da XRP alla valuta della banca ricevente.

Così facendo Ripple riesce ad aggirare e superare tutta una serie di problemi che il sistema SWIFT deve invece gestire, riuscendo così ad eseguire qualunque operazione di trasferimento in tempi rapidissimi.

La velocità di esecuzione è uno dei punti di forza di Ripple, tra tutte le criptovalute, infatti, XRP si configura come una delle più veloci con tempi di convalida medi di soli 4 secondi contro i circa 2 minuti di Ether e le ore richieste invece da Bitcoin (il tempo di convalida di Bitcoin sebbene sia dichiarato di 10 minuti, è in realtà molto variabile a seconda del momento in cui si effettua la transazione). La forza di Ripple risiede inoltre nella capacità di gestire un numero piuttosto elevato di transazioni al secondo, 1500 contro le sole 15 di Ethereum e le 3-6 di Bitcoin. Per cui, senza dubbi, Ripple si configura come un sistema di pagamenti ben più efficace di altre criptovalute, ed il suo unico "punto debole", se così lo si vuole definire, è proprio il target, ossia banche, aziende e istituti finanziari. QQuesto è anche il motivo per cui Ripple si configura, rispetto ad altre società, come meno disruptive e dunque molto

più orientata a fornire un supporto ad enti già esistenti piuttosto che a dar vita ad un vera e propria alternativa a questi.

Sotto il profilo "ideologico" Ripple si configura quindi come una società molto meno rivoluzionaria, ma resta quella che più facilmente potrebbe essere adottata in massa, per via della sua capacità di riuscire a fronteggiare una serie di problematiche che le banche devono gestire adoperando una tecnologia innovativa ma senza "minacciare" eccessivamente il sistema di intermediazione esistente. Non è infatti un caso che Ripple si sia portata al terzo posto tra le criptovalute maggiormente capitalizzate in un lasso di tempo piuttosto breve riuscendo anche, per brevi periodi, a posizionarsi al secondo posto, preceduta solo da Bitcoin che ancora beneficia di un certo vantaggio essendo "first mover", vantaggio che oramai appare alimentato più dalle performance esagerate che BTC ha dimostrato di poter generare negli anni, piuttosto che da un effettivo vantaggio tecnologico.

CAPITOLO III
SVANTAGGI DELLA BLOCKCHAIN

3.1 PREMESSA

Finora l'elaborato si è preoccupato di definire e analizzare in maniera più o meno dettagliata la storia della blockchain, le caratteristiche fondamentali che la caratterizzano e alcuni dei progetti più innovativi e meglio riusciti che impiegano questa nuova tecnologia. Con il seguente capitolo l'analisi verterà sul capire quanto effettivamente questa tecnologia possa tornare utile, soffermandosi anche sul valutare quale siano i limiti e i difetti di questa. Tutto ciò al fine di riuscire, in chiusura di elaborato, a trarre una conclusione sulle effettive potenzialità applicative di questa tecnologia e sulle sue effettive capacità disruptive.

3.2 LIMITI DELLA BLOCKCHAIN

Come già trattato in precedenza, la Blockchain ha fornito una base tecnologica importante attraverso la quale apportare dei cambiamenti significativi all'attuale sistema economico, grazie anche ad una solida base ideologica, essa è riuscita ad attirare anche molte menti disposte a dedicare il proprio tempo, le proprie energie e risorse, al fine di sviluppare e realizzare piattaforme e software sempre più innovativi e pronti a soppiantare un sistema che appare oramai obsoleto. Nonostante vi siano molte persone che si dedicano allo studio, alla comprensione e allo sviluppo dei sistemi che adoperano la Blockchain, questa col tempo sta mostrando una serie di mancanze che in precedenza venivano ignorate per via di una scarsa conoscenza della tecnologia. Da quando però questa ha cominciato ad attrarre sempre più attenzioni, ha lentamente rivelato di possedere ancora una grossa serie di limiti che ne zavorrano l'ascesa, frenando di fatto lo sviluppo e la diffusione.

Tali limiti potremmo raggrupparli sulla base degli ambiti d'interesse ai quali essi si riferiscono, possiamo dunque soffermarci sull'analizzare gli aspetti meramente tecnologici, quelli economici e quelli giuridici.

3.3 ASPETTI TECNOLOGICI

Sotto il profilo meramente tecnologico la Blockchain è fin da subito apparsa come rivoluzionaria ed innovativa, in quanto in grado di risolvere i molti problemi esistenti in tema di valute digitali, tuttavia essa presenta ancora dei limiti notevoli sotto questo aspetto che non possono essere ignorati.

Uno dei "freni" che maggiormente rallentano lo sviluppo e la diffusione della Blockchain, sotto il profilo tecnico, è la cosiddetta "scalabilità". Con questo termine s'intende la capacità del sistema di gestire contemporaneamente più transazioni. Come già detto nel capitolo precedente, Bitcoin è in grado di gestire in contemporanea un numero di transazioni che varia dalle 3 alle 6 al secondo. Valori simili appaiono piuttosto bassi se li si confronta con quelli di sistemi di pagamento, ben più diffusi e noti, come PayPal o Visa, i quali attualmente raggiungono valori di TPS (Transactions per second) di molto superiori a Bitcoin riuscendo a gestire quasi 200 transazioni, PayPal, e oltre 1700, Visa. Tali valori appaiono, a prima vista, totalmente privi di significato ma, in realtà, non è complicato capire come, a una migliore capacità di gestione delle transazioni, segua inevitabilmente una più rapida esecuzione delle stesse, la quale risulta fondamentale quando si parla di metodi di pagamento e, ancor di più, quando si valutano dei sistemi di pagamento adottati su scala mondiale. Ed è proprio perché le criptovalute nascono per imporsi come standard di pagamento a livello internazionale che, al fine di colmare il gap, si è cercato coi progetti nati successivamente Bitcoin, di migliorare questo aspetto, riuscendo, quantomeno, a raggiungere risultati accettabili, Ethereum, ad esempio, è riuscito a triplicare il valore di TPS rispetto a Bitcoin, raggiungendo la quota di 15 transazioni al secondo, che rappresenta certamente un significativo passo in avanti ma ancora non riduce in

maniera significativa la differenza con i sistemi già affermati da tempo nel campo dei pagamenti.

Sebbene questo ostacolo appaia piuttosto complicato da superare, alcune criptovalute hanno comunque già dimostrato come, la blockchain possa in realtà riuscire a gestire numeri elevati di transazioni in contemporanea, proprio Ripple, con lo sviluppo di XRP, è riuscita a raggiungere ottimi risultati in questo senso, riuscendo a raggiungere le 1500 transazioni al secondo, ed è innegabile come un simile valore sia più che sufficiente a fronteggiare la concorrenza. Il vero problema, di tutta questa faccenda è che, non vi è ancora alcuna criptovaluta capace di essere al contempo, sufficientemente scalabile e di preservare quella che è la caratteristica distintiva della blockchain, ossia la piena decentralizzazione del sistema la quale viene molto spesso, come nel caso di Ripple, fortemente ridimensionata al fine di velocizzare i processi di convalida, per cui tutti quei progetti che sono riusciti ad avvicinarsi a livelli così alti di scalabilità, in realtà hanno comunque dovuto rimuovere il vero elemento disruttivo di questa tecnologia.

A questo punto è però necessario anche andare a chiarire se risulti effettivamente utile avere un sistema così altamente scalabile. L'utilizzo delle criptovalute è al momento limitato per cui quello della scalabilità è un "falso problema" o meglio un problema a lunga scadenza, questo perché, sebbene la differenza con i sistemi di pagamento attuali risulti considerevole, c'è comunque anche da tenere in considerazione che le più utilizzate e diffuse, come Bitcoin ed Ethereum, gestiscono un quantitativo di transazioni molto basso soprattutto se paragonato a quello dei sistemi più tradizionali. Per cui la scalabilità sarebbe un elemento utile qualora il quantitativo di transazioni da convalidare risultasse particolarmente elevato, ma, alle condizioni attuali, il livello di scalabilità raggiunto da Ethereum è già sufficiente a far fronte alle esigenze dei suoi utilizzatori in quanto garantisce già dei tempi di esecuzione accettabili. C'è però da dire che per una tecnologia nata con l'intenzione di rivoluzionare completamente il sistema dei pagamenti, possedere ancora, a distanza di diversi anni, un limite rilevante come questo, sicuramente non aiuta a velocizzare la diffusione della

tecnologia e dunque, per quanto risulti poco utile al momento, esso non può in alcun modo essere ignorato né tantomeno giustificato.

A questo punto appare chiaro che ad una scarsa scalabilità coincidono, inevitabilmente anche dei tempi di convalida delle transazioni più dilatati, ciò non fa altro che penalizzare la blockchain poiché un utente dovrà attendere molto più tempo per veder avvenire un trasferimento di denaro, impattando inevitabilmente sulla comodità del servizio offerto dalle criptovalute rispetto a quello garantito da altri sistemi di pagamento maggiormente diffusi. Le motivazioni di questa lentezza sono da ricercare, però, non solo nell'incapacità dei sistemi di gestire più transazioni contemporaneamente ma anche nei processi stessi di convalida di questa tecnologia, i quali rappresentano al tempo stesso il più grande pregio ed il più grande limite della blockchain. Le nuove criptovalute si sono concentrate sul migliorare questa lentezza complessiva dei sistemi, cercando, nella maggior parte dei casi, di semplificare ed alleggerire i processi di convalida delle transazioni, riuscendo, come nel caso della scalabilità, ad ottenere risultati accettabili, rendendo il pagamento tramite questi sistemi, ben più comodo per gli utenti. Ethereum, ad esempio, è riuscita a far sì che le transazioni in ETH vengano convalidate nel giro di pochi minuti, abbattendo drasticamente le tempistiche imposte da Bitcoin che, in alcuni casi potevano richiedere anche svariate ore per il completamento di una transazione. Anche in questo caso, però, il confronto con i sistemi tradizionali o con le criptovalute parzialmente centralizzate come Ripple, risulta decisamente a sfavorevole, in quanto devono competere con tempi di convalida di pochi secondi e quindi pressoché istantanei.

È comunque evidente come, nonostante sul fronte delle valute digitali siano stati fatti enormi passi da gigante soprattutto dal punto di vista informatico e tecnologico, ci sia, in realtà, ancora molta strada da fare per rendere la Blockchain effettivamente in grado di competere ad armi pari con i principali concorrenti e poter finalmente offrire un servizio utilizzabile nella quotidianità.

3.4 ASPETTI ECONOMICI

Analizzati gli aspetti più prettamente tecnici, è ora necessario andare a trattare anche di tutta una serie di altre criticità che la Blockchain si porta dietro, i quali non si limitano alla sola scalabilità o ai soli aspetti tecnologici, ma sfociano in ambiti ben più articolati dove è più difficile trovare delle soluzioni efficaci, in particolare il campo economico e, come verrà analizzato più avanti, quello giuridico.

Dal punto di vista economico questa tecnologia presenta diversi problemi che, inevitabilmente, vanno ad alimentare lo scetticismo e contribuiscono a rallentarne lo sviluppo in quanto disincentivano gli investimenti.

L'attività di mining è quella che più di tutte presenta grosse criticità e che, in un certo senso, mette in luce anche alcune contraddizioni ideologiche alla base stessa della tecnologia. Come già affermato nei capitoli precedenti, il mining non è altro che un espediente innovativo finalizzato ad incentivare gli utenti della rete, a partecipare, mettendo a disposizione i propri terminali, al funzionamento del sistema stesso garantendo il mantenimento della struttura decentralizzata. La blockchain, essendo null'altro che un codice informatico, non è infatti in grado di poter distinguere i diversi soggetti tra loro se non identificandoli come una CPU, ossia il sistema dà per scontato che a ciascuna di esse coincida un soggetto differente. Questo crea inevitabilmente un problema di fondo poiché la decentralizzazione non è legata al numero delle CPU adoperate nel processo, quanto al numero degli effettivi possessori di queste, a processori diversi dovrebbero dunque corrispondere soggetti diversi ma, in realtà, ciascun utente, o nodo, può tranquillamente possedere un maggior numero di CPU e farle lavorare contemporaneamente alla risoluzione dei problemi matematici posti dal sistema stesso. Chiaramente, se il numero di CPU implicate nel processo risulta enorme, è inevitabile pensare che queste siano allocate tra una moltitudine più o meno ampia di soggetti differenti. Ciò chiaramente non basta a garantire la decentralizzazione del sistema per cui, proprio al fine di aumentare in maniera considerevole il numero di processori coinvolti nell'attività di convalida, e dunque di

aumentare anche il quantitativo di soggetti coinvolti, Satoshi Nakamoto, con Bitcoin, ha ideato appunto il mining, ossia un processo attraverso il quale il sistema ricompensa tutti i soggetti disposti a fornire risorse computazionali. In particolare, tutti i soggetti che hanno partecipato alle operazioni di convalida delle transazioni, vengono pagati dal programma attraverso l'emissione e l'assegnazione di nuove monete (ed è per questo che si parla di "mining" perché, come i minatori estraggono l'oro o qualunque altro minerale dalle miniere, allo stesso modo i miners "estraggono" monete dal sistema). Il processo di creazione delle nuove monete è pensato al fine di evitare, come detto già in precedenza quando si è parlato di Bitcoin, che il numero di monete possa aumentare eccessivamente ed in maniera incontrollata causando, di conseguenza, problemi di tipo inflazionistici. Dunque l'assegnazione delle nuove monete rappresenta un vero e proprio pagamento, che si configura come un incentivo a intraprendere o quanto meno a proseguire l'attività di convalida.

Se lo si analizza da un punto di vista meramente teorico, questo sistema risulta pienamente funzionante e, anche nella pratica, per un certo lasso di tempo lo è effettivamente stato, i problemi sono però sorti a distanza di alcuni anni, quando il sistema di incentivi si è mostrato piuttosto fallace, per via di una serie di elementi che lo hanno reso particolarmente altalenante in termini di profitto, in particolare esso è influenzato prevalentemente:

- Dalle quotazioni delle criptovalute che si stanno "minando", che, come già mostrato, risultano piuttosto variabili sia per lassi di tempo brevi che per periodi più lunghi;
- Dal numero di monete generate per ogni blocco: sulla base di quanto stabilito dall'algoritmo, più transazioni vengono convalidate più il numero di nuove monete generate si riduce (nel caso di Bitcoin);
- Dai prezzi relativi alla strumentazione necessaria al fine di poter effettuare l'attività di mining in maniera efficace;
- Dal costo dell'energia elettrica necessario per far funzionare i computer adoperati per eseguire l'attività.

A questo punto appare necessario andare ad analizzare ognuno di questi punti di volta in volta al fine di comprendere effettivamente come questi alterino, inevitabilmente, il sistema di incentivazione, mettendo in luce una serie di problemi significativi.

- **Volatilità delle quotazioni**

  Relativamente al fattore "quotazioni", come già visto quando si è trattato della stablecoin di Maker, il mercato risulta piuttosto imprevedibile e instabile per questo motivo risulta quasi impossibile, a priori, effettuare delle stime sensate relativamente ai valori futuri che le criptovalute potrebbero raggiungere.

  Ma le quotazioni causano problemi anche all'attività di mining la quale, prevedendo un sistema di incentivi basato sull'emissione di nuove monete, risente delle fluttuazioni negative che vanno chiaramente a disincentivare l'attività stessa Per cui il problema della volatilità ha un effetto negativo, non solo sull'utilizzo delle criptovalute, ma anche al funzionamento del sistema. Al tempo stesso c'è da sottolineare come, sebbene siano le sole fluttuazioni negative a generare degli effetti disincentivanti, quelle positive, nonostante abbiano un effetto opposto, vanno a contribuire anch'esse all'instabilità del sistema, che risente in maniera rilevante della variazione continua del numero di nodi coinvolti nelle operazioni di convalida, soprattutto in termini di tempistiche nell'esecuzione delle transazioni. Infatti quando vi è un maggior numero di soggetti coinvolti, la potenza di calcolo fornita risulta superiore e di conseguenza il tempo necessario ad eseguire le operazioni si riduce, viceversa, al ridursi dei soggetti coinvolti, si ridurranno anche le risorse a disposizione del sistema e dunque anche i tempi di convalida ne risentiranno inevitabilmente.

  C'è comunque da tenere in considerazione il fatto che, fintanto che ci sarà fiducia in futuri aumenti del valore delle criptovalute, le variazioni del numero dei soggetti coinvolti, risulteranno contenute, poiché anche chi trova nell'immediato poco conveniente partecipare all'attività di mining, potrebbe comunque, in virtù delle proprie aspettative, continuare ad operare e ad ottenere

nuove monete, nella speranza di generare dei ritorni superiori in futuro, quando le quotazioni risulteranno maggiormente favorevoli. Nella pratica però, appare evidente, anche alla luce degli altri fattori che influenzano gli incentivi forniti dal sistema, come risulti piuttosto limitato il numero di soggetti in grado di operare per lungo tempo affidandosi alle sole attese future.

- **Numero di monete generate**

  Altro fattore da tenere in considerazione quando si parla dell'attività di mining è il quantitativo di monete generate dal sistema. In questo caso il riferimento è al Bitcoin e a tutte quelle criptovalute che adoperano sistemi di riduzione progressiva, all'interno dei quali il numero di monete emesse si riduce progressivamente all'aumentare del numero di transazioni convalidate. Non tutte le criptovalute adoperano questo meccanismo poiché ognuna ha sviluppato sistemi differenti, per cui, da questo punto di vista, andrebbe effettuata un'analisi specifica per ciascuna di esse ma, essendovene un numero enorme, ciò risulta complicato, per cui verrà analizzato il solo caso del Bitcoin avendo fornito la base strutturale a molte criptovalute che dunque, in un modo o in un altro, si ritrovano ad affrontare problematiche simili.

  Come già detto, mano a mano che il numero di transazioni convalidate aumenta il sistema si preoccupa di emettere, per ciascun blocco, un numero sempre decrescente di nuove monete, per la precisione tale numero si dimezza con una cadenza all'incirca quadriennale. Questo ci fa subito capire come, inevitabilmente, i miners col passare del tempo vedranno ridursi i guadagni qualora le quotazioni restassero invariate o quanto meno vedranno dimezzarsi le monete ricevute. Ciò implica che, affinché gli incentivi forniti ai miners possano restare invariati nel tempo, il valore delle monete, ad ogni riduzione, dovrebbe almeno raddoppiare mantenendo anche tutte le altre condizioni invariate. A prima vista appare dunque piuttosto complicato che una situazione

simile possa verificarsi, eppure alla luce dei fatti, la tendenza risulta anche ben più che confermata, infatti, in corrispondenza della riduzione del quantitativo di Bitcoin emessi, le quotazioni, nel corso dei medesimi anni, sono ben più che semplicemente raddoppiate: nel 2013, anno della prima riduzione, gli incrementi furono spropositati, le quotazioni passarono dai 20$ per BTC di gennaio 2013 a ben 800$ per BTC all'inizio di gennaio 2014; similmente anche nel 2017, anno della seconda riduzione, le quotazioni sono passate dai 966$ di gennaio 2017 ai ben 10284$ per BTC di gennaio 2018, dopo aver fatto registrare, nel frattempo, anche l'attuale massimo storico, nella fine del 2017, raggiungendo circa 20000$ per BTC. Sebbene le quotazioni al momento dimostrino come in realtà la riduzione del quantitativo di monete emesse risulti totalmente ininfluente, non significa che questa situazione continuerà a verificarsi anche in futuro, soprattutto con simili incrementi esponenziali, va però dato atto che, alla luce dei fatti, le quotazioni hanno ben più che compensato le riduzioni del quantitativo di monete emesse. Per un'analisi più significativa del fenomeno ci sarebbe anche da capire quanto effettivamente le motivazioni dietro questi incrementi, in corrispondenza di queste specifiche annate, siano effettivamente attribuibili alla riduzione delle monete emesse dal sistema e quanto queste siano, invece, frutto di ben altri elementi; sicuramente però la riduzione delle monete emesse ha giocato un ruolo importante in questi aumenti, soprattutto se si considera il fatto che Bitcoin è provvisto di un limite massimo di monete generabili dal sistema, Nakamoto ha infatti imposto un limite di 21 milioni di monete così che, ad un certo punto, non si corra il rischio di emetterne troppe facendo nascere ulteriori problemi. Di certo non sono però sufficienti solo questi due elementi a giustificare incrementi cosi esagerati che, indubbiamente, sono anche legati al "hype" che si è creato intorno alle criptovalute nel corso degli anni e, in particolar modo negli anni sopra citati. Il problema continua comunque a persistere in quanto nessuno può garantire il ripetersi di certi incrementi né tantomeno è possibile garantire che, qualora si riducesse l'interesse per Bitcoin, in futuro potremmo avere anche delle flessioni

significative in concomitanza di queste annate particolari. A quel punto il sistema rischierebbe però di collassare su sé stesso, per via di un forte disincentivo a partecipare all'attività di mining che potrebbe causare un conseguente abbandono della piattaforma dovuto all'impossibilità di utilizzarla.

- **Costo della strumentazione**

  Un forte disincentivo all'attività di mining è fornito, invece, dalla strumentazione necessaria per poter effettuare in maniera efficace questo tipo di attività. Teoricamente chiunque possegga un PC può partecipare senza alcun tipo di vincolo all'attività, ma nella pratica la situazione è ben diversa, soprattutto se ci si aspetta un ritorno economico.

  Il quantitativo di risorse necessario per la risoluzione dei problemi e dunque la convalida delle transazioni è stato fin da subito piuttosto elevato, ciò al fine di rendere pressoché impossibile ad un unico utente di monopolizzare l'intero sistema rischiando, di conseguenza, una possibile manomissione dello stesso. Per questo motivo la partecipazione tramite PC poco prestazionali fornisce un apporto di risorse molto scarso che, di conseguenza, genera ricompense molto esigue tanto da essere praticamente nulle. Per cui solo coloro che hanno l'effettiva intenzione di investire in un'attrezzatura adeguata vengono di fatto incentivati dal sistema, ciò significa che, l'utente che volesse divenire un nodo all'interno della rete, dovrà, necessariamente, sostenere dei costi piuttosto elevati. Infatti PC capaci di fornire una potenza di calcolo di 180 MHs (Megahash al secondo, ossia 180 milioni di hash generati ad ogni secondo) che risulta comunque insufficiente a fornire profitti accettabili, almeno relativamente alle attuali quotazioni di Bitcoin (10800$ per BTC circa), ha un costo di circa 6000€ che, pur non essendo una spesa folle, sicuramente esclude un gran numero di persone disposte a fornire il proprio supporto al sistema. Il problema appare ancora più complesso e di difficile risoluzione se si pensa che

tutte le criptovalute adottano espedienti finalizzati ad impedire che in futuro qualcuno possa essere in grado di controllare l'intero sistema di convalida, gli sviluppatori hanno infatti tenuto in considerazione la possibilità che, per via del progresso tecnologico che di anno in anno compie passi da gigante, soprattutto in termini di prestazioni, sia possibile ad un certo punto, mantenendo la difficoltà dei problemi matematici invariata, che qualcuno possa prendere il sopravvento all'interno del sistema e imporsi come ente convalidante. Per questo motivo si sono realizzati sistemi che permettono, in maniera progressiva, di aumentare la difficoltà dei processi di convalida, in modo tale da impedire che qualcuno possa monopolizzare facilmente il sistema, ciò però fa sì che si riducano ulteriormente i guadagni che i miners possono ottenere, infatti, per poter rimanere all'interno del sistema, tenendo costanti le proprie entrate, i miners devono necessariamente aggiornare le loro strumentazioni e sostenere ulteriori costi per l'aggiornamento delle stesse. Per cui, anche in questo caso, il sistema che in origine era stato pensato per garantire la decentralizzazione, nel tempo sta mostrando di essere piuttosto fallace tanto che, attualmente, il concetto stesso di decentralizzazione sta venendo messo in crisi. Se inizialmente "decentralizzato" implicava una suddivisione del compito di convalida delle transazioni tra tutta una serie di soggetti differenti, mano a mano che si è andati avanti, questo numero di utenti che effettivamente possono fornire un contributo significativo, si sta sempre più riducendo e concentrando nelle mani di poche persone e, ancor più, nelle mani di poche società le quali, sfruttando le economie di scala, sono le uniche a poter sostenere un certo tipo di costi. Fortunatamente i sistemi sono stati sviluppati in modo da impedire un accentramento tale della capacità computazionale da garantire ad un unico soggetto la gestione dell'intero sistema ma, al tempo stesso, appare evidente come questa idea della decentralizzazione, posta alla base della blockchain, si stia sempre più ridimensionando e sgretolando dinnanzi alla realtà dei fatti e del tempo, tanto che si sta rischiando di mettere in crisi il vero punto di forza di questa tecnologia.

- **Consumo energetico**

  Ultimo problema rilevante collegato all'attività di mining è il consumo di energia elettrica necessario a far funzionare l'intero sistema di convalida. Il processo che garantisce l'esistenza di un sistema decentralizzato e perfettamente funzionante è piuttosto complesso e articolato e necessita di una grossa potenza di calcolo per poter essere portato a termine in un lasso di tempo ragionevole. Un simile sforzo computazionale implica necessariamente che un numero elevato di processori lavori in contemporanea alla risoluzione dei problemi matematici che il sistema pone in essere. Tutte queste CPU necessitano chiaramente di energia elettrica per poter funzionare e, dovendo operare ininterrottamente per un lungo lasso di tempo, senza surriscaldarsi e divenire meno efficienti, necessitano anche di appositi sistemi di raffreddamento a loro volta alimentati con energia elettrica. Il consumo elettrico impiegato risulta dunque molto elevato soprattutto se valutato in relazione all'utilizzo che attualmente si fa di questa tecnologia. Esso è a tal punto elevato che l'energia necessaria ad alimentare tutti i computer adoperati per il mining, stando ad alcune stime, sarebbe sufficiente a soddisfare il fabbisogno energetico di buona parte dell'Italia, circa il 15% dell'intero consumo annuale di energia elettrica. Appare chiaro come questo elemento si configuri inevitabilmente come un costo rilevante da dover sostenere per il miner, il quale, a seconda del Paese in cui opera, dovrà far fronte a una spesa più o meno elevata. Tale differenza dei prezzi dell'energia elettrica tra i Paesi dà vita, a sua volta, ad altri due problemi piuttosto rilevanti in quanto genera una forte azione disincentivante all'attività di mining e causa un aumento significativo dell'inquinamento.

  Partendo dal primo punto è chiaro come il costo dell'energia elettrica riduca fortemente i guadagni che i miners possono generare tramite questa attività, per

cui qualora vi fosse qualcuno disposto a fornire un supporto al sistema senza però effettuare alcun tipo di investimento iniziale, questo non solo dovrebbe accettare di adoperare il proprio terminale ininterrottamente, ma dovrebbe anche farlo nella consapevolezza di rimetterci dei soldi, con molta probabilità, per via di un costo dell'energia elettrica così elevato da superare i profitti che questo andrà a nell'immediato.

C'è da chiarire che i profitti realizzati dal mining dipendono molto dalle risorse computazionali fornite, infatti, all'aumentare di queste, il quantitativo di monete ottenute cresce in maniera più che proporzionale all'incremento della potenza di calcolo necessaria, per cui raggiunto un certo livello il terminale (generalmente un rig) riuscirà a generare dei profitti anche piuttosto rilevanti. Il problema è che, anche chi fosse disposto ad investire e a puntare fortemente su questa attività, dovrebbe fare i conti con la realtà dei fatti e prendere consapevolezza che le somme necessarie per rendere questa attività profittevole, risultano assolutamente inaccessibili alla maggior parte delle persone. E' quindi facile capire come in realtà la totale decentralizzazione risulti qualcosa che non va molto al di là della teoria. Il numero di enti che può effettivamente permettersi di acquistare e mantenere in funzione un certo quantitativo di computer è piuttosto ridotto e fortemente geo-localizzato. Non è da sottovalutare quest'ultimo aspetto: coloro che possono eseguire l'attività di mining senza incorrere in delle perdite, non solo sono pochi, ma anche fortemente localizzati in specifici Stati per via del costo dell'energia elettrica. Ogni Paese produce infatti un quantitativo differente di energia elettrica, in alcuni Stati la produzione soddisfa pienamente il fabbisogno nazionale ed in alcuni casi lo eccede, in altri Paesi, invece, la produzione non è sufficiente a far fronte alle esigenze nazionali, per cui essi si vedono costretti ad acquistare da altri Paesi la restante fornitura energetica, chiaramente in questi casi il costo dell'energia risulta di gran lunga più elevato che negli Stati che la producono autonomamente. Questo fa sì che, nel mondo, il costo dell'energia elettrica vari significativamente a seconda del Paese che si sta considerando. In Italia, ad

esempio, la produzione è in grado di far fronte solo al 88,2% della richiesta energetica nazionale (stando ai dati pubblicati nel 2017 da Terna, ossia l'ente di gestione delle reti per la trasmissione dell'energia elettrica in Italia), per cui, la restante parte, ossia l'11,8%, è acquistata da altri Stati ad un costo maggiorato rispetto a quello di produzione, per cui un italiano sostiene per la fornitura elettrica un costo generalmente più alto rispetto a quello sostenuto dai cittadini di altri Stati del mondo, dove l'energia viene prodotta in quantità sufficienti sul suolo nazionale, tramite centrali a carbone, nucleari o attraverso fonti rinnovabili. Un caso emblematico per capire come questo elemento influenzi l'attività di mining, è quello dell'Islanda, la quale, grazie all'elevata produzione elettrica e al basso costo di questa, è stata presa di mira dalle società specializzate in questa attività, le quali hanno fatto richiesta per poter aprire grossi impianti di "estrazione" di criptovalute, andando a causare problemi notevoli per lo Stato in quanto ha visto aumentare, proprio per far fronte a tali esigenze, i consumi energetici nazionali in maniera considerevole.

In una simile situazione, in presenza di barriere d'ingresso e costi di mantenimento elevati e a fronte di profitti poco stabili, appare ancora più evidente come, la tanto osannata struttura decentralizzata risulti molto scarsa, in quanto solo pochi individui, o meglio, società localizzati in specifici Paesi, sono effettivamente in grado di fari carico di certi costi e dunque portare avanti in maniera profittevole l'attività di mining. Ciò è anche dimostrato dalla forte concentrazione delle società in Cina, la quale può far leva su un basso costo dell'energia elettrica, dovuto ad un'enorme disponibilità di carbone che permette di alimentare le numerosissime centrali elettriche del Paese, e ad una crescita economica notevole che, negli ultimi decenni, ha fornito enormi risorse economiche pronte per essere investite in progetti di questo tipo, tutto ciò, unito ad una richiesta maggiore di criptovalute dovuta a una serie di limitazioni nei movimenti dei capitali imposti dal Governo, ha fatto sì che questa nazione diventasse la prima per quantitativo di risorse computazionali fornite all'attività di mining.

Electricity prices, Second semester of 2015-2017
(EUR per kWh)

	Households(¹)			Non-households(²)		
	2015S2	2016S2	2017S2	2015S2	2016S2	2017S2
EU-28	0.2103	0.2053	0.2048	0.1183	0.1133	0.1121
Euro area	0.2209	0.2203	0.2181	0.1230	0.1197	0.1183
Belgium	0.2352	0.2745	0.2877	0.1081	0.1158	0.1087
Bulgaria	0.0957	0.0938	0.0983	0.0782	0.0788	0.0742
Czech Republic	0.1408	0.1421	0.1488	0.0783	0.0732	0.0710
Denmark	0.3042	0.3084	0.3010	0.0906	0.0936	0.0978
Germany	0.2946	0.2977	0.3048	0.1493	0.1492	0.1514
Estonia	0.1291	0.1238	0.1319	0.0958	0.0896	0.0846
Ireland	0.2454	0.2338	0.2355	0.1357	0.1245	0.1241
Greece	0.1771	0.1723	0.1620	0.1150	0.1115	0.1190
Spain	0.2370	0.2284	0.2177	0.1133	0.1029	0.1032
France	0.1682	0.1711	0.1756	0.0951	0.0903	0.0920
Croatia	0.1312	0.1331	0.1236	0.0928	0.0877	0.0920
Italy	0.2428	0.2340	0.2080	0.1597	0.1556	0.1449
Cyprus	0.1838	0.1621	0.1826	0.1412	0.1295	0.1392
Latvia	0.1650	0.1624	0.1582	0.1183	0.1201	0.1159
Lithuania	0.1243	0.1171	0.1107	0.0997	0.0882	0.0825
Luxembourg	0.1767	0.1698	0.1618	0.0893	0.0858	0.0803
Hungary	0.1145	0.1125	0.1134	0.0870	0.0796	0.0779
Malta	0.1269	0.1274	0.1364	0.1405	0.1399	0.1377
Netherlands	0.1846	0.1592	0.1556	0.0846	0.0805	0.0764
Austria	0.1983	0.2010	0.1978	0.1047	0.1004	0.0997
Poland	0.1418	0.1352	0.1451	0.0861	0.0815	0.0862
Portugal	0.2285	0.2298	0.2230	0.1154	0.1132	0.1147
Romania	0.1319	0.1233	0.1289	0.0802	0.0771	0.0786
Slovenia	0.1631	0.1629	0.1613	0.0870	0.0832	0.0784
Slovakia	0.1517	0.1537	0.1442	0.1122	0.1112	0.1113
Finland	0.1530	0.1545	0.1599	0.0706	0.0694	0.0676
Sweden	0.1874	0.1962	0.1993	0.0590	0.0656	0.0647
United Kingdom	0.2183	0.1831	0.1856	0.1520	0.1278	0.1246
Iceland	0.1265	0.1478	0.1518	:	0.0652	:
Liechtenstein	0.1803	0.1678	:	0.1612	0.1479	:
Norway	0.1434	0.1631	0.1605	0.0685	0.0813	0.0703
Montenegro	0.0988	0.0970	0.1003	0.0764	0.0782	0.0770
Former Yugoslav Republic of Macedonia	0.0835	0.0828	0.0811	0.0811	0.0521	0.0561
Albania	0.0819	0.0835	0.0856	:	:	:
Serbia	0.0645	0.0654	0.0695	0.0678	0.0470	0.0751
Turkey	0.1222	0.1205	0.0959	0.0702	0.0725	0.0601
Bosnia and Herzegovina	0.0828	0.0844	:	0.0613	0.0607	:
Kosovo*	0.0614	0.0592	0.0654	0.0809	0.0771	0.0799
Moldova	0.0881	0.0923	0.1013	0.0765	0.0778	0.0852
Ukraine	:	0.0320p	0.0383	:	:	:

(*) This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo Declaration of Independence.

(:) not available
(p) Provisionnal
(¹) Annual consumption: 2 500 kWh < consumption < 5 000 kWh.
(²) Annual consumption: 500 MWh < consumption < 2 000 MWh.
Source: Eurostat (online data codes: nrg_pc_204 and nrg_pc_205)

eurostat

Ulteriore prova delle differenze, anche piuttosto significative, del costo dell'energia elettrica, è fornita dai dati dell'Eurostat che, valutando il costo medio negli Stati europei per i consumatori domestici, mettono in luce come anche solo tra gli Stati Europei vi siano discrepanze notevoli che identificano i Paesi decisamente più convenienti per l'attività di mining. Dall'osservazione è visibile come l'Italia, dove il costo per un kWh risulta, nel secondo semestre del 2017 di ben 0,2080€, risulti molto meno appetibile soprattutto se

confrontata con altri Stati quali l'Islanda, che ha un costo di 0,1518€ per kWh o all'Ucraina che, con un costo di soli 0,0383€ kWh, si configura come la più adatta, in Europa, per ospitare questo tipo di attività.

Come accennato, il consumo elevato di energia non ha solo implicazioni rilevanti sul sistema di incentivazione dell'attività di mining, ma genera anche effetti negativi sull'ambiente. Questo elemento risulta anch'esso rilevante poiché, se ci si concentra sui soli aspetti economici, definisce un costo ulteriore che va sostenuto per far sì che la Blockchain possa funzionare. Questo risulta però alquanto difficile da stimare in termini monetari, non è semplice definire quanti danni vengano effettivamente arrecati dall'inquinamento essendo che questo impatta in maniera significativa su molti aspetti, come la salute delle persone, per i quali è complicato effettuare delle stime significative, ma ciò che è certo è che questo danno sia effettivamente arrecato e causi dei costi aggiuntivi.

Il motivo per cui la Blockchain vada di fatto a generare un aumento dell'inquinamento è stato già definito in precedenza, la maggior parte della forza computazionale è localizzata nei paesi Orientali, dove l'energia elettrica è in prevalenza prodotta ancora da centrali a carbone che hanno un forte impatto ambientale. Per cui alla Blockchain è possibile attribuire una parte dell'inquinamento rendendola, di fatto, ancora meno conveniente di quanto non lo sia già. Questo aspetto rappresenta ancora una componente secondaria per via della scarsa diffusione dello strumento, ma certamente, qualora si dovesse verificare un'adozione di massa in futuro, questo dato potrebbe divenire alquanto significativo obbligando gli Stati a cercare delle soluzioni efficaci per risolverlo, come potrebbe essere una conversione definitiva alle fonti rinnovabili, le quali avranno comunque il compito di dover fronteggiare una richiesta enorme di energia anche superiore a quella attuale.

3.5 ASPETTI GIURDICI

Se sotto il profilo tecnologico ed economico la Blockchain presenta dei limiti superabili tramite modifiche al codice di programmazione, i problemi giuridici, che questa ha fatto nascere nel corso del tempo, sono ciò che, più di tutto il resto, frenano la sua diffusione. Questi problemi non possono difatti essere risolti da un gruppo di programmatori ma necessitano dell'accordo di un folto gruppo di legislatori che deve tener conto di molteplici interessi nonché di visioni politiche differenti.

Tra i vari punti di criticità molti sono legati al problema della privacy che da sempre risulta uno dei punti di forza delle criptovalute essendo elevato il livello di protezione delle informazioni che queste garantiscono.

Dal punto di vista giuridico le criptovalute, a distanza di oramai 10 anni dal lancio di Bitcoin, non sono ancora state inquadrate dalla stragrande maggioranza dei Paesi, i quali non sono ancora riusciti a fornire una base giuridica solida a questi nuovi sistemi di pagamento nonostante, nel corso degli anni, si siano lentamente diffusi. Il problema principale è relativo alla necessità di dover realizzare un apparato di leggi specifiche per definire il fenomeno in quanto le norme già in vigore, in tema di pagamenti elettronici (come quelli effettuati tramite carta di credito), sono impossibilitate dal ricomprendere la categoria dei trasferimenti in criptovalute, poiché non rispettano le caratteristiche tipiche che riconducono alla fattispecie esistente. I pagamenti attualmente più utilizzati sono giuridicamente inquadrati come trasferimenti di diritti di credito nei confronti delle banche, le criptovalute, invece, non presumono alcun tipo di trasferimento di diritti essendo, il passaggio delle monete, non mediato da alcun tipo di ente. Al tempo stesso anche la fattispecie in tema di moneta circolante, è difficilmente applicabile alle criptovalute, poiché, anche in questo caso, vengono meno alcuni presupposti fondamentali. L'impianto normativo in tema di monete definisce queste come: un mezzo di scambio, un'unità di conto, un riferimento per i pagamenti dilazionati e una riserva di valore.

Così facendo sono definite quattro caratteristiche necessarie affinché sia possibile identificare una moneta. Le criptovalute sembrerebbero apparentemente essere in

linea con questi “requisiti”, ma l’elevata volatilità di queste fa sì che il legislatore non le ritenga in grado di poter essere adoperate come unità di conto o come un riferimento per i pagamenti dilazionati né, tantomeno, come una riserva di valore. Al tempo stesso si è però visto come in realtà alcune criptovalute siano effettivamente in grado di mantenere stabilmente il proprio valore intorno a determinati livelli, per cui, sotto questo profilo, esse potrebbero anche essere effettivamente riconosciute come vere e proprie monete ed essere dunque sottoposte alla medesima fattispecie, ma ciò andrebbe sicuramente a complicare ulteriormente la situazione, per via di una normativa parziale che obbligherebbe, a quel punto, a distinguere tra due gruppi di criptovalute: quelle effettivamente regolamentate e quelle non regolamentate. Volendo ignorare questo caso particolare delle Stablecoins, tutte le criptovalute presentano comunque un problema comune legato al livello di privacy eccessivo che queste garantiscono agli utilizzatori.

Negli ultimissimi anni la questione della privacy è stata ripetutamente al centro del dibattito giuridico internazionale per via di una reiterata violazione di questa, messa in atto, in prevalenza, da colossi informatici quali Google o Facebook, quest’ultimo, ad esempio, è stato accusato di aver adoperato i dati personali di milioni dei suoi utenti, ricavati dall’omonima piattaforma social per trarne dei profitti, nello specifico, la società avrebbe ceduto tali informazioni riservate ad altre imprese per scopi di profilazione. Per questo e anche per altri episodi, di recente si è trattato molto spesso dell’eccessiva riduzione della privacy alla quale l’utilizzo di internet ci ha sottoposto; le criptovalute però si muovono in controtendenza ponendo in essere problemi completamente opposti. Appare infatti chiaro come, alla luce anche dell’analisi condotta in precedenza sulle varie criptovalute, uno dei punti cardine della Blockchain sia il mantenimento di livelli di privacy particolarmente elevati, raggiunti grazie all’utilizzo della crittografia, dei nickname e di un continuo ricambio di chiavi pubbliche adoperate nelle transazioni, così facendo questa tecnologia garantisce la completa anonimità degli utenti, impedendo, però di fatto anche qualunque tipo di controllo su di essi e le loro transazioni. Certamente un simile livello di privacy risulta

importante per gli utilizzatori, ma al tempo stesso non fa altro che complicare ulteriormente il compito di chi dovrà legiferare al riguardo, proprio perché l'impossibilità di conoscere gli oggetti, gli importi ed i soggetti coinvolti nelle transazioni, impedisce di fatto alle autorità di poter controllare che non siano stati effettuati acquisti di oggetti illegali, quali armi o droghe, né tantomeno è possibile verificare il corretto pagamento delle tasse, potendo, attraverso questa tecnologia, facilmente occultare il proprio denaro.

Per tutti queste motivazioni la Blockchain e le criptovalute sono ancora, nella stragrande maggioranza degli Stati, ancora non regolamentate. Ma c'è da notare come gli Stati abbiano adottato politiche completamente diverse tra loro essendovene alcuni che hanno optato per la strada dei controlli rigidi o dei divieti assoluti di utilizzo della tecnologia, altri che hanno invece preferito seguire una strada ben più liberale prevedendo il libero utilizzo della tecnologia ed altri ancora, infine, che hanno preferito la strada della non legiferazione nell'attesa che il fenomeno prenda una direzione più netta e la tecnologia si stabilizzi, andando di fatto a generare dei vuoti giuridici sull'argomento.

Per quanto riguarda la prima categoria di Stati, che segue la dottrina dei controlli rigidi, essa è guidata da Russia e Cina. La prima ha fin da subito adottato una politica di rigidi controlli e di riduzione della libertà di movimento delle criptovalute, ha poi ritrattato le iniziali posizioni riducendo fortemente le limitazioni imposte in precedenza, per poi ritornare, in ultima istanza, sui propri passi in maniera ancora più rigida di quanto fatto inizialmente, impedendo persino l'accesso ai siti che permettono lo scambio e l'utilizzo di criptovalute. La Cina, invece, in maniera non dissimile dalla Russia, ha optato anch'essa per una linea rigida, limitando la circolazione delle criptovalute tra e verso gli istituti finanziari e le istituzioni statali, al tempo stesso ha però lasciato la possibilità ai privati di poterle utilizzare per eseguire trasferimenti tra loro, ed è anche per questo che, al momento, la popolazione cinese si configura come la principale utilizzatrice al mondo di criptovalute, in particolare di Bitcoin, spinta anche dalle forti limitazioni imposte dal Governo relativamente alla circolazione di

capitali da e verso l'estero, che risultano però facilmente eludibili proprio attraverso l'utilizzo delle criptovalute. Un altro Stato che ha anch'esso adoperato una linea particolarmente dura nei confronti delle criptovalute è l'Islanda, la quale, al fine anche di combattere la crisi economica che l'ha colpita duramente, ha optato per rendere totalmente illegale la loro circolazione, nel paese, infatti, queste non possono essere detenute né tantomeno scambiate. Al contempo però il Governo islandese ha adottato una politica di assoluta apertura nei confronti di società intenzionate ad eseguire attività di mining sul territorio islandese, tanto che oggi si configura come uno dei Paesi maggiormente preso d'assalto dai miners per via di una serie di vantaggi economici che essa garantisce.

Passando invece al fronte degli Stati che hanno optato per una liberalizzazione delle criptovalute, garantendo la possibilità di utilizzare liberamente questi strumenti di pagamento, possiamo citare Australia, Iran e Kenya. Il primo tra questi ha permesso l'utilizzo delle criptovalute e ha avviato una serie di progetti finalizzati ad incentivare la diffusione e l'utilizzo di questa tecnologia all'interno di tutto il Paese, inoltre il Governo si è preoccupato di abbozzare un impianto normativo in materia al fine soprattutto di legiferare sul tema della tassazione definendola sulla base dell'utilizzo che gli utenti fanno delle criptovalute, andando, in particolare, a distinguere tra la detenzione di queste come forma di investimento, la quale viene tassata come una qualsiasi altra plusvalenza realizzata sulla vendita di azioni, e il così definito "uso personale" che comprende tutte le operazioni di trasferimento tramite criptovalute per l'acquisto di prodotti, il quale non viene però tassato in alcun modo. Il Governo australiano si è inoltre preoccupato di creare delle apposite licenze per quelle attività che intendessero accettare o, quanto meno, effettuare pagamenti tramite criptovalute, e ha anche previsto l'obbligo, per tutti coloro che effettuano conversioni di denaro, attraverso opportuni exchange autorizzati, di fornire dati personali quali nome, cognome e indirizzo, così da permettere un più facile controllo di questi soggetti e di tutti gli eventuali guadagni che questi potrebbero conseguire per via delle transazioni effettuate o delle variazioni delle quotazioni. Gli altri due Stati che si sono preoccupati

di rendere legale qualunque tipo di operazione effettuata attraverso le criptovalute, sono, come detto, Iran e Kenya i quali hanno optato per questa linea, per via di una serie di problematiche legate alla scarsa fiducia nella valuta nazionale, nel caso dell'Iran, e alla presenza di un numero molto ridotto di conti corrente, nel caso del Kenya. Per cui in entrambi questi paesi la Blockchain è stata adoperata per far fronte a dei problemi più che altro strutturali e di difficile, o comunque non immediata, risoluzione, piuttosto che come un vero e proprio modo per incentivare la diffusione di questo metodo di pagamento. Oltre questi tre Stati ve ne sono anche molti altri che hanno espresso pareri positivi in merito all'utilizzo di questa tecnologia e si sono preoccupati di non legiferare contro quest'ultima, come nel caso di Regno Unito e USA, i quali, sebbene non abbiano sviluppato alcuna base giuridica che permettesse di inquadrare meglio il fenomeno, si sono comunque impegnati a non ostruire, almeno per ora, il suo sviluppo e diffusione.

Nonostante vi siano alcuni Stati apertamente schierati a favore, ed altri apertamente schierati a sfavore della Blockchain, la stragrande maggioranza dei Governi si limita ad osservare la situazione, senza dare avvio ad alcun tipo di azione nei confronti delle criptovalute né, tantomeno, nei confronti di quelle società che adottano semplicemente la tecnologia senza però fornire alcun tipo di strumento di pagamento. In questo modo questi Stati non dichiarano illegale la circolazione delle criptovalute ma, al contempo, non ne dichiarano neanche la legalità per cui non regolamentano e lasciano, di conseguenza, un vuoto giuridico all'interno del quale tutto è consentito. L'Unione Europea, e dunque la maggior parte degli Stati che ne fanno parte, è parte integrante di questo gruppo di attendisti che non legiferano a favore né a sfavore di questa tecnologia, nonostante, in alcuni casi, essa si sia comunque pronunciata in maniera alquanto scettica sulle criptovalute e, in particolare, sul possibile pericolo che queste potrebbero generare con la loro eccessiva volatilità. Agli occhi dell'Europa esse appaiono, da tempo, come dei meri strumenti speculativi che rischiano di arrecare danni, anche consistenti, a chi, imprudentemente, decide di investirci.

L’ immobilismo giuridico è comunque, in parte, giustificato da una comprensione ancora molto limitata e poco chiara del funzionamento di questi sistemi, non si è ancora infatti compreso appieno come questi operino realmente e come questi possano essere controllati senza andare necessariamente ad eliminare quel livello di privacy che essi garantiscono. Il problema più grande è infatti legato alla difficoltà di controllare le transazioni, è complicato riuscire ad identificare i soggetti che le eseguono e gli oggetti che questi scambiano, per cui, al momento, le criptovalute rappresentano più un pericolo per gli Stati piuttosto che un’opportunità, poiché rischiano soltanto di favorire attività criminali ed illegali che involontariamente ricevono “protezione” dal sistema. A queste difficoltà se ne aggiungono di altre legate all’imposizione delle tasse, essendo impossibile conoscere gli importi delle transazioni e dunque anche determinare il quantitativo di tasse da versare.

I problemi non si limitano però a questi ma ne stanno nascendo di nuovi mano a mano che lo sviluppo procede e sempre più applicazioni vengono pensate e realizzate, per cui nel vuoto normativo stanno rientrando anche altri campi ed attività che, sotto il profilo economico, risultano ben più rilevanti di qualche sporadica transazione eseguita tra privati. Bisogna infatti tener sempre presente che la mancata legiferazione sul tema è anche determinata dalle proporzioni ancora molto ridotte del fenomeno, Bitcoin nel Febbraio del 2019 ha infatti raggiunto appena quota 350000 transazioni eseguite al giorno che, se valutate su scala mondiale, risultano ancora poche per spingere un gran numero di Paesi a realizzare interi impianti normativi dedicati alla tematica. Alcuni progetti recenti, intrapresi da grandi società, hanno però ulteriormente complicato la situazione, andando a generare una certa pressione sui Governi mondiali, i quali a breve saranno chiamati non più a gestire solo progetti realizzati da intermediari finanziari esistenti, già fortemente sottoposti ad un complesso di norme piuttosto articolato, ma a breve dovranno gestire anche molte aziende, che con l’intermediazione finanziaria non hanno nulla a che fare, che si sono preoccupate di dare avvio allo sviluppo di sistemi di pagamento propri che le porteranno ad invadere l’ambito giuridico degli intermediari senza che questi siano

però effettivamente sottoposti alle medesime norme. Ciò andrà a generare, senza dubbi, una moltitudine di problemi giuridici che andranno necessariamente risolti, poiché le imprese coinvolte hanno dimensioni enormi, si parla infatti di Facebook, Amazon, Apple o Samsung che contano un numero di utenti molto elevato e che possono, nel giro di poco tempo, diffondere la tecnologia alla base delle criptovalute in maniera molto rapida. Per cui oramai sta diventando sempre più urgente una legiferazione in materia che non solo definisca in maniera precisa la fattispecie, ma vada anche a sviluppare un metodo chiaro ed efficace sia per controllare questi sistemi sia per tassare in maniera efficace chi ne usufruirà in futuro.

A questo punto al fine di comprendere meglio che tipo di progetti sono stati realizzati e capire quali potrebbero essere i futuri sviluppi di questi, ne verranno analizzati alcuni:

- **Amazon Managed Blockchain**

  È un sevizio attivato alla fine 2018 dal colosso dell'e-commerce Amazon il quale ha realizzato una piattaforma (Amazon Managed Blockchain appunto) che permette di facilitare il processo di creazione di reti che adoperino la Blockchain, riuscendo ad abbattere anche i costi legati alla gestione della stessa. Il progetto ha permesso ai clienti di Amazon, in particolare alle aziende che adoperano l'omonima piattaforma, di realizzare facilmente una propria blockchain interna, finalizzata all'esecuzione più rapida delle transazioni. Al tempo stesso, Amazon ha cercato di eliminare parte dei problemi legati all'utilizzo di questi sistemi, offrendo la possibilità di monitorare costantemente le transazioni eseguite e di ottenere ulteriori informazioni rendendo queste strutture ben più trasparenti.

  Il progetto di Amazon, per poter funzionare, si appoggia a ben due blockchain differenti, in particolare esso adopera sia la piattaforma di Ethereum sia Hyperledger Fabric, quest'ultima già disponibile fin dal lancio per poter essere utilizzata, mentre Ethereum è ancora in fase d'implementazione.

Così realizzata, la Amazon Managed Blockchain non rappresenta in realtà alcuna idea particolarmente innovativa, ma considerando le dimensioni enormi del network di cui dispone la società, è facile capire come questo progetto sia in grado, in maniera molto veloce, di raggiungere un numero molto ampio di aziende che potrebbero essere interessate a sperimentare le capacità della Blockchain ed i servizi che questa può offrire, non è un caso se a distanza di pochi mesi dal lancio, già importanti clienti sono annoverati tra gli utilizzatori di questa nuova piattaforma, tra i tanti Philips e General Electric, con la sua sussidiaria Aviation, sono certamente rilevanti. Il dato importante è che tutte queste società risultano totalmente estranee al mondo dei pagamenti elettronici per cui c'è da sottolineare come vi sia un interesse diffuso ad entrare in contatto con questo mondo, ciò al fine di trovare nuovi metodi finalizzati ad un efficientamento ulteriore dei processi interni o anche per dar vita a nuove strategie, come quelle di lock-in finalizzate alla fidelizzazione del cliente.

- **Apple**

  Tutti i colossi mondiali hanno adocchiato la Blockchain come tecnologia da implementare e sfruttare, tra queste anche Apple, che da anni è all'avanguardia in tema di sviluppo tecnologico, ha deciso di spingere in questa direzione, andando a dotare i suoi nuovi sistemi operativi con dei wallet integrati attraverso i quali l'utente può, in maniera più comoda e semplice, controllare le proprie criptovalute, qualora le possegga o fosse interessato ad acquistarle. Anche in questo caso, come per Amazon, l'idea sviluppata da Apple non è affatto innovativa ma permette comunque, in termini comunicativi, di raggiungere un gran numero di soggetti andando, di fatto, a diffondere l'esistenza della Blockchain. Inoltre, e forse questo è l'aspetto più rilevante, nulla vieta ad Apple di poter sfruttare in futuro questa rete di wallet così realizzata, per lanciare una propria criptovaluta, che potrebbe anche arrivare tra

non molto tempo se si pensa che Samsung, principale concorrente di Apple, ha già divulgato di voler investire in questo senso.

- **Samsung**

  Anche Samsung ha dunque pensato di lanciarsi nel mondo delle criptovalute e della Blockchain, per farlo ha siglato un accordo con un altro colosso mondiale quale IBM per lo sviluppo di nuovi progetti, e ha già da tempo inserito, all'interno dei propri dispositivi, applicazioni di ingresso facilitato ai wallet simili a quelli realizzati da Apple. Samsung si è inoltre preoccupata di sviluppare, non solo un sistema di wallet integrato ma, con l'aiuto di IBM appunto, ha realizzato Nexledger, una piattaforma capace di velocizzare in maniera significativa l'esecuzione delle transazioni effettuate tramite criptovalute.

  Dunque con un certo anticipo rispetto alle concorrenti Samsung si è gettata in questo mercato, spinta molto probabilmente anche dall'elevato numero di dispositivi che essa vende nei paesi asiatici, dove il tasso di utilizzo delle criptovalute è ben più elevato che nel resto del mondo. Queste stesse motivazioni sono, molto probabilmente, il motivo per cui Samsung starebbe pensando di lanciare anche una propria criptovaluta che le permetterebbe di sfruttare l'enorme rete di wallet preinstallati sui suoi dispositivi, e di facilitare e velocizzare le transazioni che avvengono all'interno del proprio store.

  Il progetto appare comunque essere in uno stato embrionale e per ora appare più come una suggestione, ciò non toglie la possibilità che, una società di dimensioni considerevoli come Samsung, possa, prima o poi, piombare in maniera significativa in questo mondo.

- **Facebook**

  Tra i numerosissimi progetti lanciati, quello di Facebook è sicuramente il più interessante nonché quello, al momento, maggiormente sotto i riflettori, in particolare quelli dei legislatori.

  La piattaforma social ideata da Mark Zuckerberg nell'ormai lontano 2004 è stata forse uno dei simboli della rivoluzione informatica e tecnologica degli anni 2000, dall'anno di lancio, Facebook, è diventata una piattaforma senza eguali in termini di dimensioni arrivando a contare ben 2,3 miliardi di account, pari a circa un terzo della popolazione mondiale. Numeri che non molti anni fa sarebbero stati impensabili e irraggiungibili, eppure Facebook è riuscita, nel tempo, a raggiungere questi risultati acquisendo nel mentre anche nuove piattaforme quali Instagram e Whatsapp rendendo ben più solida la base di utenti. Proprio le dimensioni esagerate di questa piattaforma hanno suscitato preoccupazione quando, a fine 2018, è stato annunciato il lancio del progetto Libra e dell'omonima criptovaluta.

  Questo progetto si configura come estremamente ambizioso e certamente il primo della specie, l'obiettivo è trasformare tutti gli account di Facebook in dei wallet attraverso i quali far circolare, facilmente, la criptovaluta Libra che potrà eseguire qualunque tipo di transazione tramite la Blockchain. Facebook si è però spinto oltre preoccupandosi di promettere elevata velocità di esecuzione delle transazioni e, soprattutto, stabilità delle quotazioni, Libra sarà infatti legata al dollaro e il suo valore verrà garantito da una serie di assets che la società andrà a detenere e che saranno in prevalenza costituiti da titoli di stato a breve termine. Libra dunque dovrebbe risolvere due limiti importanti della maggior parte delle criptovalute e inoltre potrà fare affidamento su una rete enorme di potenziali clienti, raggiungibili con un costo pressoché nullo per la società.

  Un altro punto a favore di Libra è sicuramente il suo potenziale di crescita che essa possiede ancor prima di nascere. Il lancio iniziale è programmato su

Facebook, che sicuramente è la piattaforma social più nota al mondo, questa, però, ha conosciuto negli ultimi anni una fase di crisi soprattutto tra i soggetti più giovani, i quali sempre più tendono a spostarsi verso nuove piattaforme come Instagram (Facebook ha infatti fatto registrare, negli ultimi anni, un vero e proprio invecchiamento della sua utenza per via di una riduzione degli account creati dai giovani ed un aumento di quelli realizzati dagli ultra cinquantenni). Anche quest'ultima piattaforma è di proprietà dell'azienda, per cui Libra avrà, ad un certo punto, la possibilità di essere implementata anche su di essa con dei risvolti positivi, non solo in termini di diffusione dello strumento, che, con molta probabilità, penetra molto più facilmente l'utenza per via dell'età media molto bassa, ma anche in termini di utilizzo in quanto Instagram ha già da tempo implementato un sistema di advertising che offre anche la possibilità di acquistare direttamente tramite la piattaforma i prodotti pubblicizzati, per cui non sarebbe strano se, il gruppo creato da Mark Zuckerberg, abbia intenzione semplicemente di sfruttare Facebook come banco di prova per questa criptovaluta per poi sfruttare la popolarità acquisita per effettuare l'implementazione del sistema di pagamento su una piattaforma molto più versatile, giovane e aperta alle innovazioni, come Instagram.

Per tutti questi motivi il progetto appare in grado di segnare la storia delle criptovalute poiché, qualora venisse adottata in massa, diventerebbe assolutamente impossibile da ignorare e i legislatori di tutto il mondo sarebbero chiamati, inevitabilmente, a regolamentare una situazione poco chiara prima che possa sfuggire completamente al controllo degli Stati. Il progetto dovrà certamente affrontare una grossa serie di problemi legati alle implicazioni in campo normativo che questo si troverà, inevitabilmente, a dover affrontare. Il lancio di una simile piattaforma andrebbe a rendere Facebook un vero e proprio intermediario finanziario, in quanto fornitore di servizi di pagamento, esso tenderebbe inoltre ad assomigliare ad una vera e propria banca in quanto gestore di flussi monetari da e verso gli utenti. Ciò darebbe vita a problemi normativi significativi poiché le banche, al fine di poter divenire tali, devono

necessariamente ottenere una serie di autorizzazioni delle quali Facebook sarebbe privo. In Italia, ad esempio, è possibile aprire una banca solo se si rispetta quanto stabilito dal Decreto Legislativo N.385 del 1993 Testo Unico Bancario e dalla Circolare della Banca D'Italia 285 del 2013. Nell'Unione Europea le banche possono infatti operare solo dopo che la Banca Centrale Europea, attraverso le Banche Nazionali (nel caso italiano, la Banca D'Italia), abbia effettuato tutta una serie di controlli e aver rilasciato delle autorizzazioni atte a far sì che la banca possa effettivamente operare sul territorio nazionale e comunitario.

Nel caso di Facebook, questa, qualora dovesse completare e dare avvio al progetto Libra, si ritroverebbe ad operare in una moltitudine di paesi diversi come una qualsiasi altra banca senza essere passata per alcun tipo di controllo e senza essere assoggettata ad una qualsiasi autorità garante specializzata in materia. Sotto il profilo normativo, infatti, i problemi non si limiterebbero alle sole autorizzazioni ma sarebbe anche necessario che la società venga sottoposta, come tutte le banche a livello internazionale, alle normative sviluppate appositamente dal Comitato di Basilea per garantire la stabilità di questi enti. Inoltre le dimensioni di Facebook andrebbero a generare ulteriore confusione dovendo questa far fronte a normative diverse tra i paesi, poiché anche in tema di stabilità bancaria queste non risultano pienamente uniformate. In una situazione simile, la società si ritroverebbe quindi a navigare in una confusione giuridica che le consentirebbe di muoversi molto liberamente senza incappare in alcun tipo di sanzione.

Per questi motivi, non è da escludere che il progetto possa subire una battuta d'arresto significativa qualora gli Stati nazionali provvedessero a dichiarare illegale l'attività svolta da Facebook o andassero a sancire definitivamente l'illegalità delle criptovalute. A conferma di una possibile linea dura, i Ministri dell'economia di due paesi del G7, Francia e Italia, hanno recentemente espresso non poche perplessità in merito a questo progetto, con il francese, Bruno Le Maire, che ha parlato della pericolosità di Libra qualora questa

tentasse di imporsi come una nuova moneta sovrana, e di come il sistema sviluppato da Facebook potrebbe non far altro che incentivare attività criminali facilitando il riciclaggio di denaro ed il terrorismo internazionale; il Ministro uscente dell'economia italiano, Giovanni Tria, ha invece sottolineato come il progetto di Facebook preoccupi molti Stati e di come questo potrebbe portare, molto probabilmente, ad un intervento, senza però specificare il tipo di provvedimento e i termini, se positivi o negativi, di questo. Fatto sta che Facebook ha certamente attirato l'attenzione degli Stati con il suo annuncio e sicuramente in un futuro prossimo questi dovranno intervenire in maniera decisa optando per una delle possibili strade: un'estensione delle normative esistenti, una nuova normativa apposita o per una dichiarazione di illegalità delle attività o delle criptovalute. Tra tutte le possibilità certamente la soluzione ideale sarebbe la nascita di una nuova normativa che regoli queste nuove attività, dando la possibilità di far nascere nuove realtà aziendali e facilitando lo sviluppo e la diffusione di questa nuova tecnologia, certamente il tutto andrebbe effettuato tenendo comunque conto dei rischi economici alle quali queste società potrebbero esporci, si potrebbe dunque pensare ad una normativa che impedisca agli utenti di convertire cifre di denaro eccessivamente elevate, in modo da contenere gli eventuali danni o, in alternativa pensare ad un sistema di gestione obbligatorio per questi enti che andrebbero necessariamente a dover mantenere questo denaro sotto forma di titoli di Stato o di altri strumenti particolarmente "sicuri".

Al di là di questo enorme punto interrogativo circa lo sviluppo giuridico che seguirà la nascita di Libra, ci sono anche da analizzare alcuni "punti deboli" del progetto. Una prima criticità è certamente legata alla decentralizzazione, è ormai chiaro che una criptovaluta capace di garantire stabilità e velocità di esecuzione delle transazioni non sia, almeno per il momento, in grado di garantire anche una piena decentralizzazione. Infatti Libra, in prima battuta, non sarà completamente "permissionless", ossia non offrirà a tutti la possibilità di divenire un nodo convalidante all'interno del sistema, sarà infatti necessario

rispettare dei parametri e sottoporsi a una serie di controlli legali prima di poter effettivamente operare come tale. Per cui le operazioni di convalida saranno inizialmente gestite da alcune società che hanno già stipulato accordi con Facebook, tra le quali Vodafone, Iliad, Paypal, Uber, che forniranno supporto alla piattaforma nei primi anni di vita. Questo tipo di organizzazione dovrebbe però caratterizzare solo una fase iniziale, gli stessi realizzatori del progetto hanno infatti dichiarato di volere una piattaforma totalmente decentralizzata, ed è per questo che, nel giro di circa 5 anni, si impegneranno per convertire il sistema ad uno pienamente decentralizzato, così da poter soddisfare anche quella parte di utenza, per così dire "purista" della Blockchain, che richiede fortemente una struttura di questo tipo.

Nonostante tutti questi possibili scenari, non vi sono dubbi sulle potenzialità del progetto che potrebbe seriamente andare a sancire un definitivo passo in avanti nel campo delle criptovalute, rendendole uno strumento effettivamente utilizzabile da tutti, senza alcuno sforzo e nell'assoluta sicurezza di non veder ridurre i propri soldi da un giorno all'altro, per via della volatilità delle quotazioni. Sorvolando però tutti gli aspetti tecnici, che interessano a un ridotto numero di clienti potenziali, l'utilizzo di una piattaforma social come Facebook potrebbe rivelarsi una mossa vincente, anche solo sotto il profilo meramente divulgativo, in quanto è in grado di a raggiungere un numero molto ampio di persone, e potrebbe estendere, in maniera considerevole, la conoscenza della tecnologia. Facebook potrebbe definitivamente rompere quella barriera di ignoranza che ancora è presente intorno all'argomento permettendo una più ampia adozione di questi sistemi di pagamento, indipendentemente dall'effettivo successo di Libra. Facebook può garantire quella massificazione di cui la Blockchain ha bisogno e che le altre criptovalute non sono mai riuscite a raggiungere per via di un'incapacità di mostrarsi al mondo come qualcosa di semplice ed utile, piuttosto che come qualcosa di complicato e poco sicuro.

CONCLUSIONI

Dai primi studi sulle valute digitali, ai primi papers che teorizzavano la nascita di una valuta sicura e pienamente decentralizzata, alla realizzazione e al lancio di Bitcoin nel 2009, fino ad arrivare al previsto lancio di Libra nel 2020; senza dubbi la Blockchain si è evoluta e continua ad evolversi, nonostante durante il suo cammino abbia subito dure battute di arresto, a causa dei mercati finanziari che in più occasioni hanno mostrato poter dimezzare le quotazioni, ma anche per via degli Stati che, con il loro mancato intervento, hanno di fatto espresso una forte titubanza nei confronti di questa tecnologia e dell'idea di mondo che essa, in maniera implicita, esporta e diffonde. Ciò nonostante lo sviluppo di questa tecnologia prosegue e non si è mai effettivamente fermato, ha inizialmente atteso tempi migliori in cui lo sviluppo informatico garantisse delle solide basi sulle quali poggiarsi e ha poi atteso il momento opportuno per poter essere accolta come una vera e propria tecnologia rivoluzionaria, capace di stravolgere i sistemi tradizionali, oramai sempre più incapaci di soddisfare le esigenze degli operatori.

Eppure nonostante una serie di migliorie e accorgimenti, questa tecnologia ancora resta ai margini del panorama mondiale. Pur essendo nota ad un buon numero di persone ed aver iniziato ad affermarsi concretamente in alcune parti del mondo, essa risulta, nonostante i molti anni trascorsi dalla sua nascita, ancora sconosciuta ai più o comunque solo superficialmente nota. Questo è sicuramente un segno lampante di come essa non sia ancora giunta a quella "piena maturità" di cui necessita per potersi effettivamente e concretamente imporsi come standard nel campo dei pagamenti e della conservazione dei dati.

Per quanto siano presenti tutti i presupposti affinché essa possa realmente essere in grado di rinnovare un sistema antiquato, sembra essere sempre più difficile che questa possa effettivamente dar vita a quel sistema decentralizzato tanto desiderato, che ha fatto da base e supporto ideologico nel corso degli anni. Ciò è dovuto, in parte, a

motivi prettamente tecnologici ed economici ma, al tempo stesso, anche per una difficoltà nel fare a meno dei grandi enti centralizzati. Sono quest'ultimi, infatti, gli unici che, disponendo di enormi risorse finanziarie, possono effettivamente allocare in maniera efficace ed efficiente le risorse, sostenendo lo sviluppo delle imprese e delle economie dei Paesi.

Inoltre appare ancor più complicato il superamento dei vincoli giuridici che si porrebbero dinnanzi ad una rivoluzione di questo tipo, è dunque ben più probabile che questa tecnologia si imporrà in futuro, non tanto come tecnologia disruptive, quanto come una enabler capace di supportare imprese e banche. È ben più probabile un futuro pieno di aziende come Ripple, che si preoccuperanno di fornire servizi di trasferimento più rapidi e meno costosi di quelli attuali, piuttosto che uno in cui tutti saremo pienamente in grado di gestire i propri soldi trasferendoli senza alcuna sorta di vincolo.

Tutte queste considerazioni sono il frutto di una situazione ancora piuttosto incerta e indefinita, sia sotto un profilo tecnologico che giuridico. Al momento della stesura non appaiono esservi i presupposti per l'effettiva nascita di un sistema decentralizzato, totalmente svincolato da qualunque autorità centralizzata. Ciò non toglie che in futuro potrebbe andarsi a creare un ambiente ben più adatto a questa tecnologia che, grazie al progresso informatico ed energetico, e ad un sistema giuridico più flessibile che abbia maturato una certa esperienza in questo campo, potrebbe essere in grado di esprimersi liberamente e garantire la realizzazione di quegli utopici sistemi teorizzati da quasi trent'anni. Del resto la storia ci ha insegnato che anche scoperte inizialmente poco utili o, comunque, non in grado di riscuotere immediatamente un certo tipo di successo, siano poi riuscite a divenire fenomeni di massa e a cambiare profondamente la vita quotidiana delle persone; se si pensa ai primi esperimenti sull'elettricità avvenuti a metà del diciottesimo secolo e che, a distanza di quasi tre secoli, diamo quasi per scontata l'esistenza di PC e altri innumerevoli elettrodomestici, possiamo facilmente intuire come anche una tecnologia che attualmente trova poco spazio o ci appaia poco utile, potrà poi, in

futuro, divenire qualcosa di assolutamente scontato. Nessuno è dunque capace di prevedere con certezza cosa accadrà a distanza di molti decenni o addirittura di secoli, per cui nulla vieta che questa tecnologia possa, prima o poi, imporsi nelle modalità in cui è stata teorizzata. Con sicurezza possiamo però certamente dire che alla luce degli elementi attuali, la Blockchain avrà un futuro certamente non facile, una qualsiasi azione coordinata degli Stati potrebbe infatti istantaneamente stroncarla, così come, l'insufficiente capacità produttiva di energia elettrica potrebbe impedirle di diffondersi rapidamente, ma di fatto nessuna buona idea o tecnologia nasce priva di difetti, né, tanto meno, incontra fin da subito il consenso pubblico. Per cui, a questo punto, appare superfluo concentrarsi sulla moltitudine di risvolti che questa tecnologia potrebbe seguire, piuttosto appare opportuno focalizzarsi su ciò che, nell'immediatezza dei prossimi anni, questa tecnologia sarà in grado di fornirci in maniera concreta. Con essa saremo proiettati in un mondo ancora più informatizzato, dove i processi verranno sempre più affidati a strutture informatiche e sempre meno alle persone, al fine di ridurre gli errori, velocizzare i processi e abbattere i costi. Tutto ciò avrà certamente delle ripercussioni giuridiche, sociali ed economiche, ma anch'esse col tempo verranno metabolizzate, assimilate e successivamente superate, poiché del resto il progresso è questo, un superare e sostituire il precedente, con la consapevolezza che ciò che è nuovo non è che il frutto di un processo e di un'evoluzione del vecchio.

Per cui dovremmo vedere la blockchain e le criptovalute come nient'altro che l'evoluzione dei vecchi metodi di pagamento: cosi come si è passati dal baratto alle monete d'oro, da queste alle banconote e infine alle carte di credito e ai servizi di pagamento online, le criptovalute potrebbero sancire un ulteriore passo in avanti, caratterizzato da nuove meccaniche e nuove possibilità di operare, ma la sostanza rimarrà sempre la stessa, benché nelle novità si cerchi sempre la tendenza a voler rivoluzionare l'esistente eliminando il precedente, nella realtà questo non sarà mai possibile.

Alla luce di questa analisi, appare necessario che gli Stati forniscano il loro apporto per lo sviluppo di questa tecnologia facilitandone la diffusione e non bloccandola, preoccupandosi di indirizzarla verso un ambiente regolamentato senza lasciarla in balia degli utenti, poiché si rischia di veder svanire quanto di buono questa tecnologia ha da offrire, in quanto appannata da utilizzi impropri e sbagliati alla quale essa inevitabilmente si presta.

BIBLIOGRAFIA

- David Chaum; *Blind signatures for untraceable payments*; 1983
- Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman; *Blockchain Technology: Beyond Bitcoin*; 2016
- Wei Dai; *B-money*; 1998
- Satoshi Nakamoto; *Bitcoin: A Peer-to-Peer Electronic Cash System*; 2008
- Team di sviluppo di Maker; *MakerDAO whitepaper*; 2017
- Alexandro Capogna, Leandro Peraino, Silvia Perugi, Marco Cecili, Giovanni Zborowski, Andrea Ruffo; *Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione*; 2015

SITOGRAFIA

- www.investopedia.com
- www.coindesk.com
- www.blockchain4innovation.it
- www.ilsole24ore.com
- www.wired.it
- ripple.com
- www.ethereum.org
- coinmarketcap.com
- makerdao.com
- www.terna.it
- github.com
- it.finance.yahoo.com
- www.bloomberg.com