UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in **Economia e Commercio**

Bitcoin e criptovalute

Bitcoin and cryptocurrencies

Relatrice:

Prof.ssa Giulia Bettin

Rapporto Finale di:

Alessia Kura

Anno Accademico 2019/2020

Alla mia famiglia,
che mi ha sostenuto in ogni occasione.

A Claudia,
che è sempre stata presente.

A Valerio,
che mi ha insegnato a non mollare mai.

A me stessa,
per aver compreso finalmente quanto valgo davvero.

INDICE

INTRODUZIONE

L'incontro tra finanza e informatica ha portato alla nascita di criptovalute, ossia nuove monete caratterizzate dalla presenza di crittografia, in grado di portare innumerevoli benefici ai soggetti che la utilizzano rispetto alle semplici valute legali. In particolare, il successo più grande all'interno del mercato è stato ottenuto da *Bitcoin* che ha portato ad un cambiamento nella concezione della moneta oltre che dei nostri sistemi di pagamento.

Il presente elaborato, dunque, è volto a comprendere i meccanismi di funzionamento delle criptovalute e in particolare ad analizzare tutte le peculiarità che le differenziano dalla moneta legale.

Ho scelto questa tematica per approfondire la conoscenza nell'ambito dell'economia monetaria e cercare di comprendere al meglio i processi economici in atto. Infatti, al giorno d'oggi, sono sempre di più gli utenti, le aziende e le attività commerciali che ricorrono all'uso delle criptovalute sfruttandone al massimo le potenzialità. Ecco il motivo per cui, a mio parere, si tratta di un argomento di attualità molto interessante soprattutto perché legato all'economia dei singoli paesi.

Inoltre, analizzando nel dettaglio le diverse tecniche e modalità attraverso cui si utilizzano *Bitcoin, Ethereum, Ripple, Tether e Bitcoin Cash* ho avuto modo di scoprire e imparare nuove funzionalità del web.

La tesi è articolata in tre capitoli. Nel primo viene fornita una panoramica sull'evoluzione e lo sviluppo della moneta, in particolare, tutte le fasi che hanno portato

all'introduzione di nuove valute. Fatta questa premessa verranno, inoltre, messi a confronto le diverse tipologie di moneta così da poter individuare i vantaggi di cui dispongono e le loro peculiarità.

Il secondo capitolo, invece, si occupa di dare delucidazione su come il sistema *Bitcoin* sia in grado di funzionare: analizzando la tecnologia sottostante che ne permette il funzionamento, l'attività di "estrazione" di *bitcoin* e le modalità di acquisto di questi ultimi. Verranno trattati anche i possibili rischi che possono comportare problematiche relative al *double spending* della valuta.

Nel terzo capitolo viene effettuato un resoconto delle tipologie di criptovalute che nel corso del tempo si sono affiancate ai *Bitcoin*, analizzandone i punti di forza. Infine, viene fatta menzione anche di un prossimo futuro in cui le Banche Centrali emetteranno una propria valuta digitale.

Capitolo 1

CARATTERISTICHE DEI BITCOIN

1.1 La moneta e la sua evoluzione

In origine per poter acquisire beni e servizi, l'uomo ricorreva al baratto, un sistema di commercio funzionante all'interno delle comunità in cui avvenivano poche transazioni. Tuttavia, l'intensificarsi dei commerci e la volontà di semplificare gli scambi hanno portato all'introduzione di un nuovo strumento di pagamento: la moneta, la quale è accettata da tutti ed è in grado di garantire la compravendita di beni e servizi. È bene, però, sottolineare che la sua natura è mutata nel tempo. Inizialmente circolava la "moneta-merce", caratterizzata da un proprio valore intrinseco e che permetteva di effettuare gli scambi. Subito dopo si affermò l'utilizzo dei metalli preziosi come l'oro e l'argento che garantivano notevoli vantaggi quali l'omogeneità, la riconoscibilità, la divisibilità e la conservabilità nel tempo. Nonostante le monete d'oro e d'argento furono usate per lungo tempo presentavano lo svantaggio di essere piuttosto pesanti, difficili da trasportare e da custodire; così per porre rimedio a tali inconvenienti, si arrivò alla nascita delle banconote che garantivano la convertibilità in oro, e per questo chiamate anche "moneta convertibile". Poiché erano caratterizzate da un valore intrinseco inferiore rispetto al valore nominale, si venne a creare il cosiddetto "signoraggio" ovvero il reddito monetario percepito dall'istituto che ha la facoltà di emettere moneta ad un costo irrisorio rispetto al valore nominale.

Fino al termine della prima Guerra Mondiale la moneta detenne la piena convertibilità in oro (*Gold Standard)*: ogni valuta possedeva una parità fissa con l'oro che permetteva la presenza di un sistema di tassi di cambi fissi con l'estero. Successivamente, con l'avvento del *Gold Exchange Standard* la convertibilità delle banconote in oro rimase garantita solo per i pagamenti tra le Banche Centrali limitatamente alle loro riserve auree, finché, con gli accordi di *Bretton Woods*, solo il dollaro mantenne la convertibilità in oro fino a scomparire del tutto nel 1971 quando Nixon dichiarò l'inconvertibilità anche del dollaro. Ecco che, quindi, si afferma la moneta fiduciaria (o moneta legale) il cui valore non dipende più dal valore intrinseco ma diviene puramente nominale; la sua convertibilità si esprime in termini di beni che si possono acquisire e dipende dal livello dei prezzi. La moneta legale viene emessa dalle Banche Centrali che si occupano di garantirne la credibilità e la stabilità nel tempo. Essa, infatti, viene accettata e utilizzata quotidianamente dai singoli operatori che agiscono all'interno del mercato.

Andando avanti nel tempo, l'avvento della tecnologia e del web ha portato alla nascita della "moneta elettronica" che introduce una novità, ossia la smaterializzazione della transazione. Infatti, i sistemi elettronici si caratterizzano per una completa centralizzazione del sistema e si basano sull'apertura di un deposito in cui si versa contante fisico in modo tale che, ogni volta che viene effettuato un acquisto, la cifra spesa online viene detratta dal conto.

Inoltre, con la crescita di internet, sono state introdotte all'interno di questa categoria valute alternative contraddistinte da un sistema di crittografia che ne permette la

rappresentazione digitale e prevede la sostituzione degli intermediari con soggetti privati che operano all'interno del web.

1.2 Che cos'è un *bitcoin*?

"*Bitcoin* è una criptovaluta e un sistema di pagamento mondiale[1]". Il suo ideatore, conosciuto con lo pseudonimo di Satoshi Nakamoto, ha dato vita alla prima moneta virtuale decentralizzata e alla tecnologia sottostante, ossia la *Blockchain*. Il suo obiettivo era quello di creare una moneta unica in grado di sostituire quella esistente e facilitare le transazioni all'interno del mercato.

Nonostante la pubblicazione del protocollo sia avvenuta nel novembre del 2008, la prima operazione è stata effettuata nel gennaio del 2009 con il seguente messaggio di Nakamoto all'interno del sistema: "*Chancellor on brink of second bailout for banks*"[2]. Molti studiosi hanno interpretato questa affermazione come una sfida lanciata per far fronte a quella che è la maggior crisi finanziaria del mondo; Nakamoto, infatti, con il lancio di questo progetto si era prefissato di superare il cosiddetto "*too big to fail*", cioè la presenza di istituzioni, troppo grandi per fallire, che attendono il salvataggio dello stato come prestatore di ultima istanza. Il suo intento, in altre parole, era quello di eliminare totalmente la presenza di intermediari.

Giunti a questo punto, bisogna fare una distinzione: con il termine *Bitcoin* (con la lettera "B" maiuscola) ci si riferisce al sistema di pagamento mentre con il termine

[1] Wikipedia, l'enciclopedia libera.
[2] Amato M. Fantacci L. (2018). Per un pugno di bitcoin: Rischi e opportunità delle monete virtuali, e-book: posizione 123 di 3132

bitcoin (con la lettera "b" minuscola) si intende la valuta. Il suo simbolo è ₿, nei mercati viene utilizzato anche BTC o XBT e la sua più piccola suddivisione possibile è il *satoshi*, pari a 10^{-8} *bitcoin*. La diffusione di questa criptovaluta è stata favorita dagli innumerevoli benefici che possiede, compresi quelli già presenti nella moneta elettronica e nel contante. Essa, infatti, permette di effettuare all'interno di internet trasferimenti e pagamenti tra gli operatori in tempo reale indipendentemente dalla posizione geografica, dall'importo e dal momento in cui si sta eseguendo l'operazione. Ciò implica una notevole libertà di pagamento favorita dalla mancanza di intermediari finanziari che autorizzino le transazioni, infatti questo sistema si basa su una tecnologia *peer to peer* che garantisce appunto a due o più dispositivi di scambiare informazioni reciprocamente senza la presenza di un server centrale che agisca come unità condivisa. Anche se ciò comporta da un lato una riduzione dei costi di transazione e quindi l'attrattività di questo tipo di moneta, dall'altro aumenta il rischio degli investitori che non possono più far fronte alla garanzia che veniva offerta dalle banche contro eventuali truffe o inconvenienti provenienti dal resto del mercato.

La rete *Bitcoin*, inoltre, punta a garantire l'esecuzione delle operazioni con una maggiore riservatezza senza la necessità di inserire dati personali che potrebbero portare all'identificazione anagrafica dell'operatore. Secondo recenti studio, questa caratteristica ha portato a far sì che l'utilizzo di tale criptovaluta si indirizzasse sul mercato nero (anche detto "*dark web*"), ossia il luogo in cui vengono svolte attività illegali. Molti studiosi, infatti, spiegano che circa metà delle transazioni in *Bitcoin* avvengono principalmente per acquistare droga, elementi legati alla pedopornografia o

addirittura anche armi; inoltre, spesso questa piattaforma diventa uno strumento per effettuare finanziamenti al terrorismo o alla criminalità e, oltre ciò, alcuni utenti fanno circolare e conservano fondi illeciti così da potersi sottrarre alla tassazione.

Tuttavia, *Bitcoin* non è totalmente anonimo dato che, nonostante permetta di nasconderci dietro l'utilizzo di pseudonimi, tutte le transazioni sono visibili, sin dalla prima, da chiunque osservi la *blockchain*; ciò lo differenzia dal contante, che permette invece ai singoli individui di svolgere le operazioni in piena privacy senza la possibilità di essere tracciati.

1. 3. Principali differenze tra le "criptovalute" e la moneta a corso legale

Analizzando tali considerazioni è opportuno capire nel dettaglio quali sono le principali differenze tra *bitcoin* e valute legali.

Come già anticipato, la moneta legale si caratterizza per un sistema centralizzato in cui la Banca centrale ha il monopolio sull'emissione di banconote che gestisce in base alle politiche monetarie che decide di adottare. Infatti, essa può intervenire in qualsiasi situazione andando ad incrementare o a diminuire l'offerta di moneta, ossia la quantità in circolazione, per poter garantire la stabilità macroeconomica di cui un paese necessita.

Eppure questa attività, in alcuni casi, può comportare una caduta del sistema all'interno di una fase particolare denominata "trappola della liquidità", rappresentata dalla presenza di tassi di interesse a livelli particolarmente bassi in cui la moneta emessa non circola, dato che i consumatori preferiscono detenere contanti piuttosto che

investirli; di conseguenza le politiche monetarie espansive cessano di avere effetti positivi sull'economia reale.

I *bitcoin*, al contrario, sono caratterizzati da un sistema decentralizzato in cui vi è la totale assenza di un istituto di emissione che si occupi di garantire e tutelare il suo valore. Quest'ultimo viene determinato in base all'incontro tra domanda e offerta all'interno del mercato, tant'è che gli operatori effettuano proposte di acquisto e di vendita ad un prezzo deciso da loro stessi dopo aver analizzato gli andamenti precedenti.

Tale criptovaluta all'interno del proprio sistema non permette il trasferimento di altre monete, come ad esempio euro o dollaro, ma soltanto di *bitcoin*. Ciò rimarca uno dei principali problemi su cui si concentra il mancato successo di questa moneta poiché, a differenza della valuta legale, per poterne usufruire è necessario non solo l'utilizzo della stessa criptovaluta ma anche che essa sia accettata dagli altri operatori. Inoltre, nonostante il *bitcoin* sia stato concepito come una moneta per l'acquisto di beni e servizi viene per lo più utilizzato per scopi speculativi, ossia per investimenti, anche rischiosi, al fine di ottenere un guadagno dalle fluttuazioni del mercato.

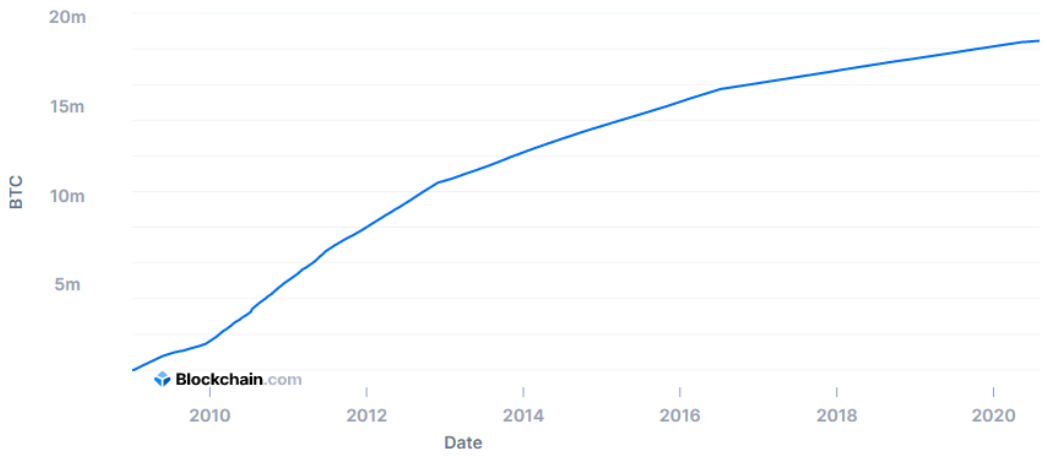
Un altro elemento che lo distingue dalle altre valute è il fatto che "*bitcoin* è un attivo di chi lo detiene senza essere al contempo il passivo di nessun altro"[3]; ciò implica che una quantità di *bitcoin* non può essere considerata come un credito in quanto non dà nessun diritto ad ottenere una somma di denaro. Diversamente, la valuta legale

[3] Amato M. Fantacci L. (2018). Per un pugno di bitcoin: Rischi e opportunità delle monete virtuali, e-book: posizione 169 di 3132

rappresenta un debito per le banche dal momento che devono garantirne la restituzione in contanti nel caso in cui gli operatori ne abbiano l'esigenza, ed è per questo che viene iscritta nel passivo del loro bilancio.

Possiamo dunque notare come, più che alla valuta legale, il *bitcoin* ricordi le qualità dell'oro in quanto chi ne è possessore gode di una forma di denaro che mantiene il suo potere di acquisto senza che risulti il passivo di nessun altro soggetto. Inoltre, *bitcoin* e oro possono essere accomunati da una caratteristica: la scarsità quantitativa; tuttavia mentre con l'oro ci riferiamo ad una scarsità dovuta all'esigua presenza in natura e alla grande difficoltà di estrazione, con il *bitcoin* sappiamo che si tratta da una carenza espressamente voluta dal suo ideatore, come si può capire analizzando il *White Paper* (il protocollo-statuto). Satoshi Nakamoto, infatti, sin dall'inizio del progetto ha stabilito una emissione massima di *bitcoin* di 21 milioni, e ha anche fissato il ritmo di produzione; raggiunto questo livello massimo nulla può essere aggiunto o modificato. La figura 1.1 mostra la crescita dei *bitcoin* dalla sua nascita fino ad oggi.

Figura 1.1: *Produzione bitcoin*



Fonte: *https://www.blockchain.com/charts/totalbitcoins*

Data la determinazione del quantitativo massimo di produzione, ogni quattro anni si verifica un evento di *halving* (dimezzamento). Ciò comporta anche una riduzione, a parità di sforzo, del 50% del premio in bitcoin che viene ottenuto da specifici soggetti che si occupano della loro estrazione, ma questo argomento verrà trattato nel dettaglio in seguito.

Capitolo 2

FUNZIONAMENTO DEI BITCOIN

2.1 La Blockchain

La Blockchain è una tecnologia, su cui si basa la rete *Bitcoin*, che prevede l'archiviazione e la gestione delle transazioni. Essa è una catena di blocchi che permette di memorizzare una grande quantità di informazioni e dati in maniera permanente e sicura. Elemento distintivo rispetto ai sistemi attuali è la decentralizzazione, che consente agli utenti di operare in maniera autonoma andando a contrastare l'oligopolio formato dalle Banche Centrali nella gestione del sistema dei pagamenti. Questa peculiarità va affiancata alla trasparenza totale dei dati; infatti, la blockchain viene paragonata ad un registro pubblico attraverso il quale chiunque può ricercare informazioni sulle attività presenti senza, però, la possibilità di manomissione o alterazione.

Tuttavia, c'è un quesito che molti utenti si pongono: come si fa ad avere la certezza che le operazioni all'interno di questo nuovo sistema siano sicure? La risposta è data dalla crittografia. L'etimologia del termine è data dall'unione di due parole greche: *kryptós*, ossia nascosto e *graphía*, vale a dire scrittura. Da ciò si può comprendere come l'obiettivo di questa tipologia di scrittura sia la creazione di un messaggio che può essere letto solo mediante una chiave che ne decodifichi il contenuto. Ad eseguire tale operazione sono i "*miners"*, figure specializzate di cui ci occuperemo più avanti.

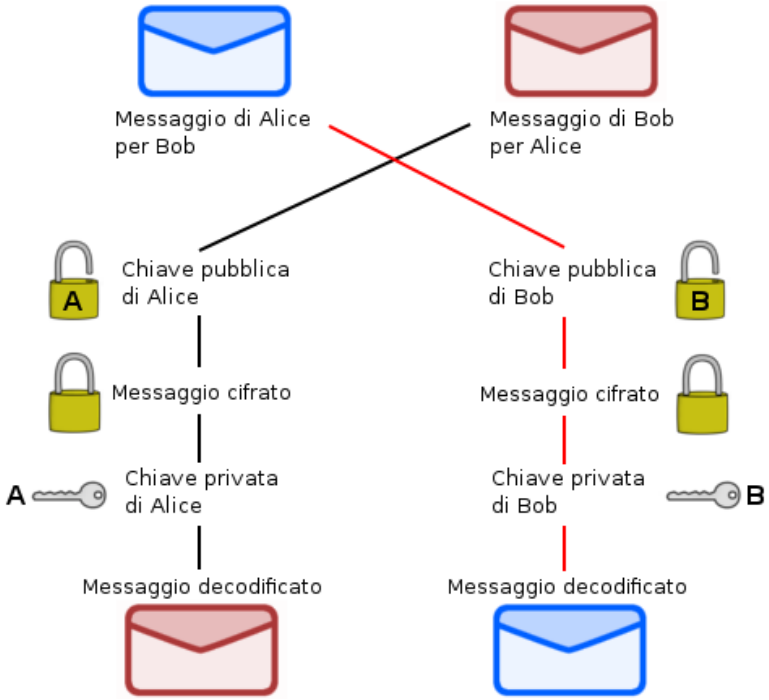
2.1.1 Come funziona realmente la blockchain e il sistema Bitcoin per un utente?

Il sistema Bitcoin non è altro che un programma che fornisce un portafoglio personale, chiamato *wallet,* che permette ai vari operatori di accumulare *bitcoin* acquisiti o di ricevere pagamenti.

L'utilizzo del *wallet* si basa sul possesso di specifiche chiavi di accesso: una pubblica e una privata (paragonabili ad una semplice password e username) legate da una relazione matematica che ci permette di ottenere la chiave pubblica con il solo possesso della privata. Mentre quest'ultima deve rimanere segreta ed essere utilizzata per poter confermare la transazione (come fosse una firma digitale), la chiave pubblica, dalla quale si ricava l'indirizzo (*bitcoin address*), rappresenta un codice, liberamente visibile agli altri clienti, utile per poter ricevere *bitcoin*. Le transazioni da un utente all'altro sono quindi molto semplici: basta digitare la chiave pubblica dell'utente a cui si vuole effettuare il trasferimento delle criptovalute, indicare l'importo e la transazione è completa.

Per meglio comprendere l'operazione, viene riportato di seguito nella Figura 2.1 un esempio pratico di come avviene il procedimento di decodificazione dei messaggi tra due utenti tramite l'utilizzo delle chiavi specifiche:

Figura 2.1: *Decodificazione messaggio*



Fonte: https://it.wikipedia.org/wiki/Crittografia_asimmetrica

2.1.2 Come acquisire i bitcoin?

Il crescente utilizzo delle criptovalute ha permesso la nascita di nuove modalità di acquisto:

- *exchange online*: siti che svolgono un servizio di intermediazione e che consentono di scambiare valuta virtuale con moneta legale. Permettono dunque non solo di trasformare *bitcoin* in euro e viceversa, ma anche di commutare altre valute virtuali come *Ethereum*. Inizialmente questi siti venivano percepiti come dannosi per il successo delle criptovalute dato che incentivavano a disfarsi delle

valute virtuali; ciò nonostante, gli operatori del mercato hanno iniziato a percepirle come una moneta meno pericolosa in quanto permette la conversione in valuta legale.

L'utilizzo degli *exchange online* è molto elementare: bisogna registrarsi all'interno della piattaforma ed inserire i dati personali. Tali siti svolgono il ruolo di *market maker*, una sorta di intermediario finanziario che fissa sia il prezzo di acquisto che di vendita delle valute con l'obiettivo di trarre un profitto. La tabella riportata nella Figura 2.2 mostra la classifica dei principali siti di *exchange online*, il volume di *bitcoin* scambiati con altre valute legali e la quota di mercato occupata:

Figura 2.2: *Bitcoin trading*

Exchange	Volume [BTC]	Market share ▾
coinbase	346k	23.92%
bit-x	251k	17.34%
kraken	247k	17.09%
bitstamp	224k	15.47%
bitflyer	113k	7.79%
bitfinex	105k	7.23%
bitbay	61.1k	4.22%
gemini	52.7k	3.64%
others	36.3k	2.50%
exmo	11.4k	0.79%

Fonte: http://data.*bitcoin*ity.org/markets/volume/30d?c=e&t=b

- *bitcoin* ATMs: sportelli automatici che, tramite l'utilizzo di bancomat, danno la possibilità di acquisire criptovaluta e in alcuni casi anche di venderla. Diversamente dagli sportelli tradizionali che si collegano ad un conto bancario, i *bitcoin* ATMs sono direttamente collegati ad internet e se ne trovano in minor quantità; la loro posizione è individuabile tramite l'apposito sito https://coinatmradar.com/;

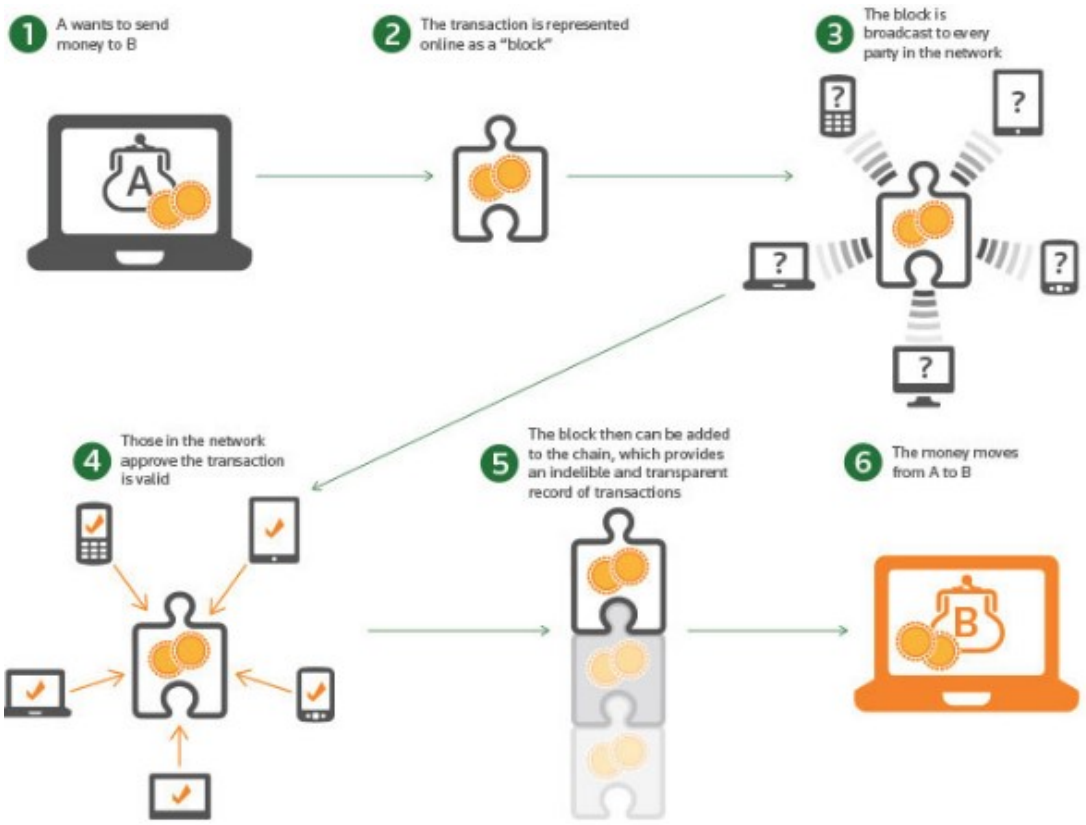
- vendere beni o servizi in cambio di *bitcoin*: modalità che si sta pian piano diffondendo, dal momento che sempre più attività commerciali, sia fisiche che online, accettano pagamenti tramite *bitcoin* oltre alle valute tradizionali;

- attività di mining: processo che permette di validare le transazioni di *bitcoin* e ottenere un guadagno.

2.2 Mining

Volendo approfondire il concetto di *mining,* esso rappresenta un processo di validazione delle transazioni: ogni scambio viene inserito all'interno di un blocco il quale, prima di essere aggiunto agli altri, viene certificato in modo da garantire la sicurezza e la stabilità della *blockchain*. Quindi, tale fase avviene tramite la risoluzione di complessi calcoli matematici svolti da soggetti chiamati *miners* (minatori). Nella Figura 2.3 viene riportato uno schema che spiega tutti i procedimenti relativi all'attività di *mining*:

Figura 2.3: *Funzionamento*



Fonte: https://www.codemotion.com/magazine/dev-hub/blockchain-dev/lightning-network-the-second-layer-of-blockchain-is-ready/

A questo punto è bene sottolineare che il *mining* è una attività remunerativa, vale a dire che il primo utente che riesce a risolvere il calcolo ottiene una ricompensa e le commissioni all'interno del blocco. Tuttavia, per poter raggiungere l'obiettivo, è

necessario dimostrare il lavoro computazionale svolto attraverso il cosiddetto *proof-of-work*[4].

Inoltre, una volta che si è deciso di intraprendere il percorso di *mining,* sarà necessario avere un computer, una connessione internet ed un *wallet* per *bitcoin*; quindi, sebbene da un lato questa attività rappresenti una fonte di guadagno, c'è da dire che solo pochi utenti decidono di ricorrervi. Ciò accade perché inizialmente ad ogni blocco risolto venivano assegnati 50 BTC ma nel momento in cui si raggiungono i 210.000 blocchi viene effettuato un dimezzamento; infatti nel 2012 questo valore ha raggiunto 25 BTC mentre da maggio 2020 il premio è sceso ulteriormente a 6,25 BTC. Nel momento in cui la produzione di *bitcoin* raggiungerà il suo limite massimo, la ricompensa non verrà più elargita e il guadagno sarà dato unicamente dalle commissioni delle transazioni stesse.

Per di più, accanto alla scarsità di guadagno, bisogna tener presente tutti gli eventuali costi che bisogna sostenere. Innanzitutto, come abbiamo detto, è necessario possedere computer specifici che possono essere acquistati anche sul web ma a prezzi molto elevati, e che consumano grandi quantitativi di energia elettrica anche solo per validare una singola transazione. Infatti, stando ai dati di *digiconomist.net*, per l'estrazione di *bitcoin* vengono spesi annualmente circa 62.97 *terawattora*[5] (TWh) di energia elettrica, paragonabili al consumo annuale di un paese come la Svizzera. Di

[4] Un sistema proof-of-work (POW) o protocollo proof-of-work, o funzione proof-of-work è una misura economica per scoraggiare attacchi denial of service (negazione di servizio) e altri abusi di servizio, come spam sulla rete, imponendo alcuni lavori dal richiedente del servizio, di solito intendendo tempo di elaborazione di un computer.
[5] È un'unità pratica di potenza usata soprattutto in elettrotecnica

conseguenza, queste attività vengono svolte principalmente all'interno di grandi capannoni situati nei paesi dove i costi per l'energia sono inferiori, come le zone rurali della Cina.

In sintesi, possiamo dire che i ricavi ottenuti dallo svolgimento del *mining* eguagliano i costi che i *miners* devono sostenere e dunque non viene offerto un grande margine di profitto.

L'attività di *mining* può essere svolta in tre modi differenti:

- individualmente: il minatore esegue l'attività di estrazione indipendentemente dalla presenza di soggetti terzi in modo tale da ottenere tutta la ricompensa. Tuttavia, questa specifica tipologia richiede un grande investimento iniziale in hardware dato che una maggiore potenza permette di anticipare la concorrenza nello svolgimento dei calcoli;
- *mining pool*: gruppi di minatori che cooperano tra di loro mettendo a disposizione le risorse che possiedono così da poter svolgere l'attività in maniera rapida e suddividere il premio ricevuto;
- *cloud-mining*: condivisione della rete al fine di eseguire il mining delle criptovalute senza la necessità di appositi hardware; tuttavia, tale attività comporta premi notevolmente inferiori rispetto alle opzioni precedenti.

2.3 Double spending

Data la natura globale della struttura dati su cui si basa *Bitcoin* e considerando il possibile scatenarsi di transazioni simultanee e in diverse parti del globo, un problema

che riguarda la moneta virtuale è quello del *double spending*. Tale attività consiste nella possibilità di poter copiare i dettagli di una transazione e ritrasmetterli in modo tale che un *bitcoin* possa essere utilizzato più volte dal proprietario. Ne deriva che, senza adeguate misure, un protocollo che non riesce a far fronte a questo problema risulta compromesso.

Diversamente dalle valute legali dotate di un sistema centralizzato in grado di tenere sotto controllo questo rischio, per la moneta virtuale ciò è molto più impegnativo. Infatti, quando un utente riceve la transazione, questa non viene immediatamente aggiunta alla blockchain ma deve essere prima validata dai *miners*; pertanto, finché non viene confermata, la transazione non è valida. Quindi per aggiornare la *Blockchain* ci vuole del tempo e in quel lasso temporale, seppure minimo, la stessa criptovaluta può essere spesa per più di una transazione tramite diverse tecniche. Un metodo è quello del "*51% attack"*, messo in atto quando una singola entità o gruppo riesce a controllare più del 50% del *mining power,* allo scopo di escludere o modificare le transazioni e poter effettuare una doppia spesa di *bitcoin*. Tuttavia, un simile attacco è molto improbabile poiché il network è vasto e la probabilità di ottenere tutto questo potere è molto bassa.

Invece, quando parliamo di "*race attack",* ci riferiamo alle situazioni in cui i commercianti accettano i pagamenti senza attendere l'eventuale validazione. In questo caso vengono create due transazioni in rapida successione e inviate a due negozi differenti di cui solo uno riceverà la somma di *bitcoin*.

Infine, è possibile eseguire anche un "*finney attack"* attraverso il quale il *miner* non trasmette immediatamente il blocco alla rete ma effettua la spesa prima di rilasciarlo. Se

il pagamento viene confermato, il nuovo blocco includerà una transazione a doppia spesa.

In conclusione possiamo dire che, per evitare o ridurre la possibilità di subire innumerevoli attacchi, è necessario che il commerciante si accerti della validazione della transazione.

Capitolo 3

LA NASCITA DI NUOVE CRIPTOVALUTE

3.1 Altcoin

L'avvento del *Bitcoin* ha portato allo sviluppo di molte altre criptovalute alternative, ciascuna delle quali con peculiarità specifiche in grado di attrarre l'attenzione di utenti differenti. Ad oggi, all'interno di *coinmarketcap.com* si possono individuare circa 6124 monete virtuali che circolano all'interno del mercato e che vengono soprannominate "*altcoin*". Questa sigla sta per "*alternative coin*" ad indicare tutte le criptovalute diverse rispetto ai *bitcoin*. Nella figura 3.1 di seguito riportata possiamo dare un rapido sguardo alle principali *altcoin* che andremo ad approfondire nello specifico.

Figura 3.1: Classifica criptovalute

Criptovalute | Scambi | Elenco di controllo | Filters | EUR | Prossimo 100 → | Guarda tutto

Rank	Nome	Cap. del mercato	Prezzo	Volume (24h)	Rifornimento circolante	Modificare (24h)	Grafico dei prezzi (7gg)
1	Bitcoin	€184.587.372.210	€10.002,70	€19.845.852.129	18.453.756 BTC	0,97%	
2	Ethereum	€37.520.108.942	€334,77	€9.486.760.758	112.078.748 ETH	-0,31%	
3	XRP	€11.677.935.562	€0,260304	€1.773.737.706	44.862.646.997 XRP *	2,19%	
4	Tether	€8.466.801.961	€0,846831	€28.300.933.464	9.998.221.723 USDT *	-0,14%	
5	Bitcoin Cash	€5.035.188.429	€272,42	€2.513.995.561	18.483.250 BCH	10,38%	

Fonte: coinmarketcap.com; data consultazione 07/08/2020

Dall'analisi di questo grafico possiamo notare come ci sia un notevole distacco tra i *bitcoin* e le altre criptovalute; questo perché, non solo il *bitcoin* ha preceduto tutte le altre in termini di tempo di creazione, ma anche perché delle centinaia di criptovalute che vengono lanciate nel mercato, solo una piccola parte riesce a guadagnare abbastanza interesse da parte degli utenti tale da garantirne la diffusione e quindi il relativo aumento di valore.

3.1.1 ETHEREUM

Ethereum è una piattaforma digitale aperta, lanciata sul mercato nel 2015, che permette ad ognuno di costruire e usare applicazioni decentralizzate, le quali vengono eseguite sulla tecnologia *blockchain*. Può essere quasi considerato come un grande computer condiviso che concede ai suoi utenti l'utilizzo di una grande potenza di calcolo ovunque e per sempre. All'interno di questa piattaforma vengono utilizzati gli *smart contract*, dei contratti intelligenti realizzati mediante un linguaggio di programmazione, caratterizzati da una totale autonomia nei confronti di qualsiasi intermediario e da una notevole sicurezza dato che i contenuti all'interno sono crittografati.

Tuttavia, questi tipi di contratti possono esistere solo grazie alla presenza di *Ether*, la valuta nativa di *Ethereum*, acquistata dai partecipanti della rete per poter pagare la potenza di calcolo messa a disposizione.

Mentre *Ethereum* si pone come obiettivo quello di sviluppare progetti tecnologici o favorire il lancio di nuove criptovalute, *Bitcoin* viene vista come una semplice

alternativa alla valuta legale che si occupa per lo più di transazione all'interno del mercato finanziario. Inoltre, nel caso di *Ethereum,* la creazione di un blocco avviene circa in 4-15 secondi, a differenza di *Bitcoin* che impiega oltre 10 minuti. Infine, uno degli elementi che distingue nettamente le due valute è l'offerta monetaria: mentre il limite massimo di *bitcoin* che possono essere prodotti è fissato a 21 milioni, il numero di *Ether* riproducibili è illimitato.

3.1.2 RIPPLE (XRP)

Ripple è la terza criptovaluta per capitalizzazione e rappresenta una valida alternativa a *Bitcoin* e ad *Ethereum.* Essa nasce nel 2013 con l'obiettivo di creare un sistema (denominato Ripple) e una valuta (XRP) che garantiscano la possibilità di effettuare trasferimenti di fondi in maniera sicura e soprattutto in tempo reale. Queste transazioni, a differenza di quelle eseguite con *Bitcoin* basate su un algoritmo di *proof of work* in seguito all'attività di *mining*, sono protette e verificate dai partecipanti del network attraverso un meccanismo di consenso specifico che viene raggiunto tramite un algoritmo noto come *Ripple Protocol Consensus Algorithm (RPCA)*.

Ripple supera quasi del tutto il sistema[6] precedente andando ad attrarre l'interesse delle banche e di grandi società che lo utilizzano per eseguire le proprie transazioni transfrontaliere in maniera più efficiente rispetto ai metodi tradizionali.

[6] "Society for Worldwide Interbank Financial Telecommunication (SWIFT)

Inoltre, ciò che distingue Bitcoin da Ripple è il fatto che nel primo caso parliamo di un sistema decentralizzato che non è di proprietà di nessuno e in cui le valute sono sparse per tutto il mondo, nel secondo caso sappiamo che è di proprietà della società Ripple Labs che detiene il possesso di circa il 60% di XRP ed è in grado di influenzarne il valore. Infine, mentre Bitcoin è stato creato come valuta da utilizzare all'interno dei processi di compravendita di beni e servizi, Ripple ha come unico scopo quello di digitalizzare le transazioni tra le banche che avvengono all'interno del sistema.

3.1.3 TETHER

Rispetto a tutte le valute virtuali presenti all'interno del mercato, *Tether* emerge per la sua stabilità. Questa valuta rientra all'interno della categoria delle *stablecoins,* vale a dire criptovalute appositamente progettate per ridurre al minimo la volatilità del prezzo grazie all' agganciamento alle monete tradizionali. Pertanto, possiamo dire che il valore di *tether* è legato a quello del dollaro statunitense e infatti ogni unità viene emessa soltanto se coperta da un dollaro presente nelle riserve della *Tether Limited*, una società delle Isole Vergini britanniche.

Tether viene utilizzata da molti utenti dato che, oltre ad utilizzare la blockchain di bitcoin che rende le transazioni sicure, permette di poter muovere i fondi più velocemente e sfruttare appieno tutte le eventuali offerte del mercato. Tuttavia, negli ultimi anni sono stati sollevati innumerevoli dubbi sul fatto che *tether* riesca a garantire la conversione in dollari e ciò ha inevitabilmente influenzato il pensiero degli utenti del

mercato che, timorosi di subire una grande perdita, hanno preferito sempre più affidarsi ad altre criptovalute.

3.1.4. BITCOIN CASH

Bitcoin cash è un *altcoin* nato dall'*hard fork* di *Bitcoin Classic* il primo agosto del 2017. L'espressione "*hard fork*" indica il fatto che la catena si è spezzata in due e di conseguenza all'interno della *blockchain* c'è un cambiamento del codice originario della valuta virtuale che permette così di ottenerne una nuova versione.

Il *Bitcoin cash* si pone come obiettivo quello di superare il limite dimensionale dei blocchi così da poter incrementare le transazioni elaborate e tener testa a servizi di pagamento come *Visa* o *Paypal*. In effetti, la dimensione dei blocchi in *Bitcoin* è pari a 1 *megabyte* con conseguenti rallentamenti per quanto riguarda l'elaborazione delle transazioni, invece in *Bitcoin Cash* la dimensione sale a 8 *megabyte*. Tuttavia, questo incremento viene affiancato da una maggiore potenza computazionale e da una crescita dei costi da sostenere che rischia di escludere i *miners* più piccoli e portare la concentrazione del potere solo nelle mani di pochi.

3.2 Se le Banche centrali emettessero criptovalute?

Negli ultimi anni la crescita esponenziale delle criptovalute ha minacciato l'autorità delle Banche Centrali. Ciò le ha portate ad ipotizzare l'emissione di una propria valuta virtuale che permetta di essere al passo con il sistema dei pagamenti e dunque soddisfare clienti alla ricerca di un sistema che faciliti le loro transazioni. Denominata

CBDC, ossia *Central Bank Digital Currency*, questa valuta al dettaglio rappresenta un futuro strumento in grado di affiancarsi alla valuta legale e al contante. Tuttavia è bene puntualizzare che le CBDC si trovano ancora in una fase sperimentale.

Mentre oggi solo le banche commerciali hanno il permesso di accedere ai conti delle banche centrali, con l'introduzione delle CBDC questa possibilità verrà estesa anche al pubblico, senza la necessità di un conto bancario.

Innanzitutto, come per la moneta legale, le Banche centrali avrebbero il pieno controllo dell'offerta di moneta (oltre che del volume e della velocità di produzione) che porterebbe ad una totale perdita del sistema decentralizzato presente all'interno del sistema Bitcoin. Inoltre, dal momento che le CBDC rappresenterebbero passività all'interno dei bilanci delle Banche Centrali (compensate nell'attivo da titoli e finanziamenti alle banche), l'introduzione di questa valuta virtuale porterebbe ad una maggiore stabilità della moneta rispetto alle attuali criptovalute.

Per quanto riguarda le caratteristiche in comune con le criptovalute possiamo notare che ci sono benefici che daranno la possibilità di rendere i pagamenti più efficienti, riducendo i tempi di trasferimento e di approvazione delle transazioni; inoltre le CBDC, essendo rintracciabili, andrebbero a risolvere anche il problema della contraffazione di monete e banconote. Nonostante gli innumerevoli vantaggi, però, c'è da tener presente che l'utilizzo di questa criptovaluta gestita dalle Banche Centrali all'interno del mercato è ancora distante. Ciò accade in quanto molti non desiderano che la loro banca centrale tenga conto di tutte le transazioni che vengono effettuate; infatti l'anonimato previsto

all'interno del sistema *Bitcoin* verrebbe eliminato e proprio per questo i consumatori sarebbero più orientati all'utilizzo del contante.

Attualmente circa 15 banche centrali si stanno affacciando nel mondo delle CBDC; tra queste la Cina è quella che può considerarsi maggiormente pronta per l'introduzione di tale valuta all'interno del mercato. Non a caso, a partire dall'anno 2020, nelle città di Shenzhen, Suzhou, Chengdu, e Xiong'an è iniziata la sperimentazione dello "*yuan*" digitale, tramite test interni, in modo tale da poterla utilizzare nelle olimpiadi invernali del 2022. Per di più la banca centrale cinese è in trattativa con varie aziende private con l'obiettivo di facilitare l'utilizzo e il consumo di tale valuta.

In conclusione, l'introduzione delle CBDC potrebbe comportare un notevole impatto all'interno del sistema finanziario e dovrà di conseguenza essere sostenuta da un'adeguata tecnologia sottostante.

CONCLUSIONI

Con il presente elaborato ci si è posti l'obiettivo di analizzare il mondo delle criptovalute e comprendere gli elementi distintivi rispetto alle valute legali. In particolare, ci si è focalizzati sulla comprensione delle basi tecnologiche che hanno permesso il funzionamento del sistema *Bitcoin*, ossia la *Blockchain* la quale, tramite l'utilizzo della crittografia all'interno dei propri processi, ha permesso il successo di tale valuta.

Questo sistema, infatti, ha dato vita non solo al *Bitcoin* ma anche a tutte le criptovalute presenti nel mercato che hanno integrato la tecnologia della *Blockchain* e l'hanno adattata ai propri obiettivi.

Inoltre, sebbene più volte sia stato annunciato il fallimento di BTC, ciò non è mai avvenuto, anzi, la diffusione di tale valuta, accanto alle altre, continua a crescere a dismisura. Tale affermazione può essere compresa analizzando il sistema attuale; le Banche Centrali, infatti, si sono poste l'obiettivo di lanciare una propria valuta digitale che può essere comunemente utilizzata come moneta per l'acquisto di beni e servizi. Tuttavia, a causa della mancanza di affidabilità da parte degli utenti e l'incertezza relativa alle normative da applicare in tema di criptovalute, queste ultime non sono ancora state adottate in tutto il mondo e addirittura alcuni stati ne hanno limitato l'utilizzo.

Se quanto detto finora sul *Bitcoin* e sulle criptovalute è vero, bisogna anche fare una considerazione su quello che potrebbe accadere in futuro; questo perché l'uso intenso

della *Blockchain* e degli algoritmi crittografici potrebbe essere messo a dura prova dall'introduzione e dalla realizzazione dei computer quantistici. Questi ultimi sono una nuova categoria di calcolatori che sfruttano i fenomeni della meccanica quantistica per elaborare le informazioni e sono attualmente in fase di sviluppo nelle più grandi aziende informatiche. Essi saranno in grado di rompere gli algoritmi crittografici alla base della *Blockchain* e quindi di ottenere le chiavi private degli utenti, assicurandosi così tutti i loro *bitcoin*.

Una futura ricerca sulle criptovalute dovrebbe, dunque, valutare quanto detto, andando ad approfondire tali criticità e proponendo alcune possibili soluzioni in grado di risolvere questo eventuale problema.

BIBLIOGRAFIA

Amato M., Fantacci L. (2018). *Per un pugno di bitcoin: Rischi e opportunità delle monete virtuali*, Egea, Università Bocconi Editore: Milano.

Banca d'Italia (2015), *Avvertenza sull'utilizzo delle cosiddette valute virtuali,* Banca d'Italia, Roma

Bank of England (2020), *Central Bank Digital Currency*, Discussion Paper, Bank of England, Londra.

De Bonis R., Vangelisti M.I. (2019). *Moneta: Dai buoi di Omero ai Bitcoin*, Il Mulino, Bologna.

SITOGRAFIA

www.bancaditalia.it

http://data.bitcoinity.org/

https://www.youtube.com/: What is Bitcoin?

https://www.blockchain.com/

https://www.blockchain4innovation.it/

www.digiconomist.net

https://www.bankofengland.co.uk/

www.money.it

https://www.cybersecurity360.it/