Dipartimento di Impresa e Management

Cattedra in Macroeconomia e Politica Economica

"Bitcoin: moneta del futuro o fantasia del XXI secolo?"

Relatore: Prof. Salvatore Nisticò

Anno Accademico 2018/19

Candidato: Federico Monaco 205591

Indice

Introduzione

La scelta di trattare ed approfondire la tematica relativa ad i sistemi monetari è banalmente riconducibile al fatto che, il denaro, inteso come l'istituzione universale la cui genesi, come per il mercato, è difficilmente rintracciabile in un dato luogo o momento storico, è da sempre alla base dello svolgimento dell'attività economica e quotidiana della vita umana. Difatti, citando il celeberrimo Adam Smith, *"Whoever offers to another a bargain of any kind, proposes to do this. Give me that which I want, and you shall have this which you want*"[1]. Ovvero A. Smith sottolinea la normale propensione dell'uomo allo scambio intrinseca nella sua essenza, da non confondere con lo scambio utilitaristico che gli verrà in seguito criticato da Polanyi.

Il denaro, dunque, è stata l'invenzione che ha permesso all'uomo di superare la fase ed i limiti del baratto, aumentando il volume degli scambi e diventando un vero e proprio strumento di libertà per la sua astrattezza e neutralità.

Negli ultimi anni si sta assistendo ad una trasformazione definibile globale dell'intero sistema societario, comprendendo variabili non solo economiche, ma anche culturali ed istituzionali. Tale "rivoluzione" è facilmente attribuibile per gran parte all'evoluzione del mondo della tecnologia, intesa

[1] "*The Wealth of Nations", Adam Smith, 1776*

non con il suo vero significato derivante dal greco "*τέχνη*" e "*λόγος*"[2], ma come sviluppo nel campo dell'Information and Communication Technology (ICT). Il sistema monetario, dunque, è stato senza dubbio toccato da tale evoluzione tecnologica e le monete attuali rischiano di diventare uno strumento obsoleto, in favore di sistemi tecnologicamente più avanzati, dove la fisicità del denaro sembra muoversi verso la definitiva scomparsa. In particolare, analizzando l'evoluzione dei sistemi monetari, sembra ormai certo che si assisterà in un breve futuro alla nascita di una nuova fase, ovvero quella delle criptovalute e nello specifico del Bitcoin, considerata la criptovaluta per eccellenza e l'unica ad essere sopravvissuta a pieno nell'ambito nella genesi delle criptovalute.

La tesi, dunque, è finalizzata al tentativo di spiegare il funzionamento dei sistemi monetari basati sulle criptovalute ed in particolare la loro genesi, analizzare eventuali pro e contro di tali sistemi, confrontare una criptovaluta con una moneta d'uso comune attuale ed infine cercare di delineare un sistema economico in cui l'unica moneta in circolo sia il bitcoin e vederne le possibili conseguenze, cercando di rispondere a quesiti di ordine pragmatico, come ad esempio interrogarsi sul ruolo e sulle funzioni del sistema bancario in codesto scenario .

[2] *La traduzione reale sarebbe: "l'applicazione e l'uso di tutto ciò che può essere funzionale alla soluzione di problemi pratici, all'ottimizzazione delle procedure, alla scelta di strategie operative per raggiungere un determinato obiettivo".*

Capitolo 1

1. Introduzione alle criptovalute

1.1 Origini e sviluppi storici

La storia del denaro è difficilmente collocabile nel tempo e nel periodo storico, l'uomo è da sempre stato animale sociale ed ha da sempre posto in essere relazioni interpersonali e di fatto ha da sempre scambiato beni o servizi contro moneta nel mercato. Dunque, sembrerebbe davvero un tentativo azzardato cercare di dare una data o un luogo di genesi all'uso del denaro, inteso come concetto e non, come nell'immaginario comune attuale, come semplice banconota. Alternativamente, però, è possibile delineare un'evoluzione dello scambio e della moneta, seguendo una sorta di climax ascendente basato sulla tecnologia. È possibile dunque distinguere circa quattro fasi: una prima caratterizzata dal baratto primordiale, quest'ultimo tuttavia aveva sempre il limite di dover soddisfare la condizione della "doppia coincidenza dei bisogni". Successivamente l'individuo, in quanto limitato, imperfetto e fallibile[3] si è trovato davanti alla necessità di dover risolvere questo problema della doppia coincidenza, la soluzione è stata ricercare un mezzo che potesse essere forma di scambio con tutti gli altri

[3] *Karl R. Popper, La scienza, congetture e confutazioni, in Congetture e Confutazioni, trad. it., Bologna, Il Mulino*

beni. Si è individuato negli animali, e nello specifico la pecora[4], un mezzo di scambio che potesse essere appetibile per tutti, la pecora quindi diventa il mezzo di scambio che consente di superare questo problema. Successivamente, si evidenziarono i limiti degli animali, ovvero: difficilmente trasportabili e marcescibili. Quindi nel tempo si sono sostituiti agli animali ed alle pecore, dei beni che fossero più duraturi e che fossero più semplici da trasportare nel processo di scambio. Esempi principali furono: il sale (permetteva di conservare il cibo nel tempo), le conchiglie, i metalli (con cui sono sorte le prime coniazioni della moneta), la carta con le prime banconote ed infine anche la plastica. Dunque, in tutta la storia dell'evoluzione del denaro, quello che non è cambiato è la funzione del denaro che è sempre rimasta quella di essere un "mezzo di scambio", quello che, invece, è cambiato è il "materiale fisico su cui si appoggia il mezzo"[5]. Ad oggi però ci stiamo incamminando verso una strada in cui il supporto materiale sta scomparendo, ci si sta allontanando dal mezzo materiale. Questa è una delle cose che Simmel non era riuscito a immaginare, in quanto sosteneva che "il mezzo di scambio sarebbe sempre stato appoggiato a qualche materiale fisico". Nel XXI secolo, gran parte delle transazioni (scambi economici) avvengono online, quindi senza il passaggio di un mezzo materiale. Dunque, alla conclusione di tale evoluzione, si arriva al giorno d'oggi dove si stanno diffondendo sistemi monetari alternativi basati su criptovalute ed in particolare sul Bitcoin.

[4] *Dal lat. pecunia, der. di pecus -ŏris 'bestiame'*
[5] *Kurt H. Wolff The Sociology of G. Simmel, Glencoe, 1950*

1.2. Il Bitcoin

Il Bitcoin è considerata la criptovaluta per eccellenza e fu ideata e creata nel 2009 da un inventore anonimo il cui pseudonimo, usato online, era Satoshi Nakamoto, il quale già nel 2008 in un abstract online presentò la sua idea di sistema economico basato sulla sua criptovaluta.

A partire dalla pubblicazione dell'embrione del sistema la comunità di hacker è cresciuta in maniera esponenziale, attirando migliaia di users ed investors e difatti, nel 2012 si assiste alla nascita della Bitcoin Foundation, un'organizzazione creata con la finalità di consolidare pubblicamente il bitcoin e promuoverlo. Nel 2013 il fenomeno era già cresciuto talmente tanto da favorire lo sviluppo di alcuni ATM di Bitcoin, in particolare uno anche in Italia presso la Luiss Enlabs. Il consolidamento della moneta è cresciuto fino al 2017, quando si assiste ad una vera e propria "cryptocurrency bubble", difatti, come analizza il grafico sottostante, nei primi mesi del 2017 il sistema Bitcoin aveva attirato milioni di investors, causando un effetto domino e richiamando all'investimento anche investitori medi che pensavano di cavalcare l'onda della cryptocurrency, purtroppo dopo qualche mese la bolla "popped", causando perdite per decine di migliaia di euro, in quanto 1 Bitcoin era arrivato ad essere scambiato per circa 20k di dollari[6]. Adesso, dopo

[6] *https://bitcoincharts.com/charts/bitstampUSD#rg60ztgSzm1g10zm2g25zv*

l'esplosione della bolla, il prezzo è tornato ad una volatilità standard che lo attesta intorno ai 5k/6k USD.

Figure 1. Comparing of the three great price bubbles on bitcoin - 06/2011, 4/2013, 11/2013 with 2017

[7] *Source: http://www.kurzy.cz/zpravy/440516*

1.2.1. Il Bitcoin e le principali funzioni della moneta

In finanza, il bitcoin è ormai definito una moneta a tutti gli effetti, capace di soddisfare qualsiasi tipo di scambio di bene o servizio contro moneta e, infatti, può essere analizzato secondo le tre principali funzioni monetarie:

- Il bitcoin come *mezzo di scambio*: la moneta è ciò che si utilizza per acquistare beni e servizi. Ovvero la moneta dovrebbe fornirci la sicurezza che

[7] *Comparing of the three great price bubbles on bitcoin - 06/2011, 4/2013, 11/2013 with 2017,* consultabile all'indirizzo *http://www.kurzy.cz/zpravy/440516*

verrà accettata per qualsiasi scambio; attualmente il bitcoin non è considerabile al 100% come mezzo di scambio, però il numero di soggetti che accettano il bitcoin come pagamento sta crescendo in maniera esponenziale da quando i colossi come Amazon, Starbucks e Goldman Sachs hanno iniziato a trattare con il bitcoin. Difatti nel 2017 il volume delle transazioni in bitcoin attraverso la piattaforma sarebbe cresciuto del 328% sull'anno precedente.[8]

- Il bitcoin come *unità di conto*: la moneta rappresenta l'unità di misura con cui si esprimono i prezzi e si registrano i debiti ed è di fatto il metro con cui si misurano le transazioni economiche. Questo discorso è totalmente valido ed applicabile anche al bitcoin in quanto riesce a soddisfare come qualsiasi altra moneta corrente o passata tale condizione.
- Il bitcoin come *riserva di valore*: la moneta rappresenta un mezzo per trasferire potere d'acquisto dal presente al futuro. Anche in questo caso il bitcoin è totalmente valido, bisogna specificare anche che l'alta volatilità attuale del bitcoin non va ad inficiare con tale condizione in quanto la moneta è comunque una riserva di valore imperfetta: i prezzi sono comunque soggetti a cambiamenti, sia per il tasso d'inflazione, sia per altri motivi. Dunque, è impossibile avere una moneta il cui valore sia cristallizzato nel tempo perciò la volatilità del bitcoin non contraddice tale condizione.

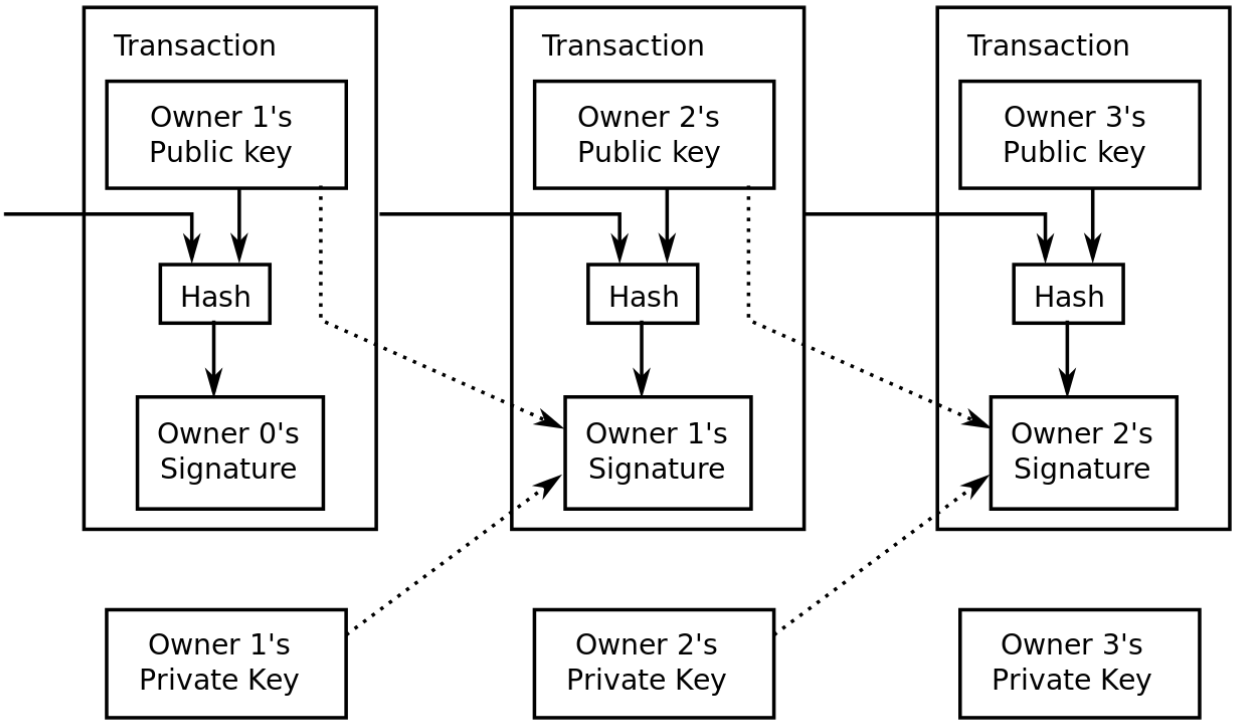
[8] *https://www.wired.it/economia/finanza/2018/06/27/shopping-pagamenti-bitcoin-criptovalute/*

1.2.2. Proprietà e caratteristiche

Bitcoin non è soltanto una moneta virtuale, bensì può essere considerato l'espressione della stessa comunità che si trova al suo fondamento e come innovazione tecnologica ha delle proprietà essenzialmente uniche e che lo contraddistinguono da tutti i tentativi di sistema monetari precedenti.

In primis si tratta di un sistema decentrato, nel quale non c'è assolutamente intervento di banche centrali, e dove la flessibilità e l'unicità fanno da motore. Infatti, è possibile avere movimenti di denaro e pagamenti con straordinaria velocità a livello globale, e dopo pochi minuti vedere la transazione registrata ed indelebile nella blockchain attraverso algoritmi avanzati. In conclusione, nel sistema è facilmente osservabile come l'intermediazione finanziaria di terzi sia completamente messa da parte, ovvero le transazioni avvengono tra soggetto e soggetto senza la necessità di istituzioni finanziarie che vadano ad approvare ed eseguire la transazione con costi elevati.

Figure 2. Schema semplificato di una catena di possesso



[9] *Source:* Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System (PDF),* ottobre 2008, in *www.bitcoin.org*.

In secondo luogo, il sistema Bitcoin garantisce l'anonimato della transazione peer to peer e soprattutto, può essere utilizzato sia come sistema di pagamento, sia come deposito di valore, in quanto il numero di emissioni di quest'ultimi è fisso e ciò dovrebbe evitare ed annientare il fenomeno dell'inflazione.

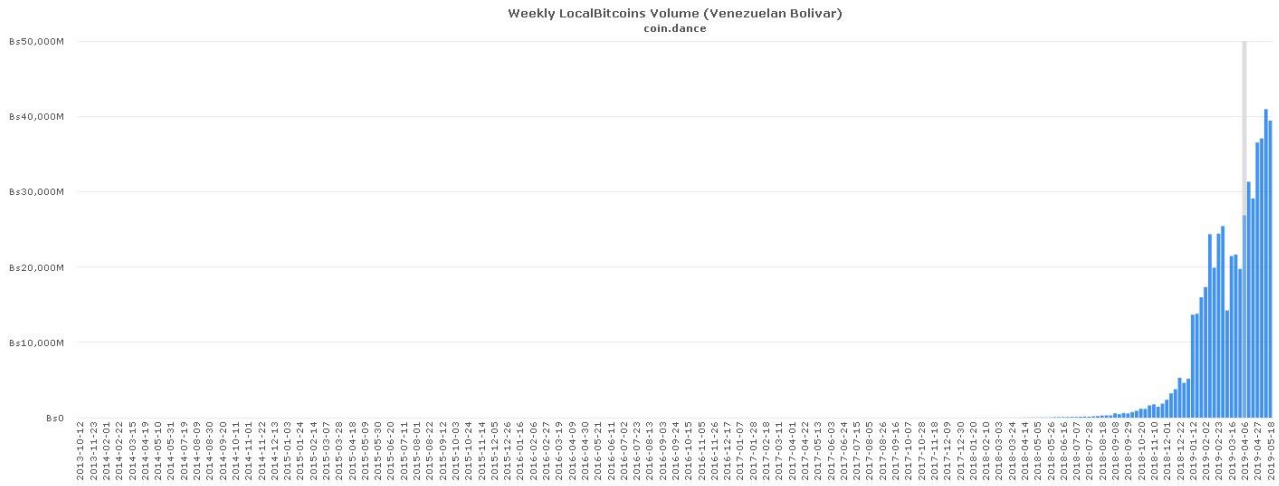
Ad oggi, è considerevole l'esempio dell'Argentina, dove una iperinflazione (quasi del 50%) ha portato in forte auge il bitcoin, considerato sempre molto

[9] Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System (PDF),* ottobre 2008, in *www.bitcoin.org*.

volatile, ma molto più solido come riserva di valore rispetto al peso argentino, l'interesse per la criptovaluta è testimoniato anche dal fatto che già 37 città del Paese hanno iniziato ad accettare il Bitcoin per il pagamento dei servizi di trasporto pubblico.[10]

Stesso discorso può essere posto in essere per la situazione venezuelana, dove gli scambi tra Bitcoin e bolivar venezuelani hanno superato i 6 milioni di euro, oltre il doppio rispetto all'ottobre del 2018.

[11] *Figure 3.*



Source: https://coin.dance/volume/localbitcoins/VES

1.3. Principali differenze rispetto alle valute tradizionali

Il bitcoin nasce, come menzionato precedentemente, come semplice token della blockchain, questo lo rende unico e senza dubbio migliore rispetto alle

[10] *https://www.wallstreetitalia.com/bitcoin-argentina/*
[11] *https://coin.dance/volume/localbitcoins/VES*

valute tradizionali dal punto di vista della sicurezza. Difatti, quest'ultimo non può essere assolutamente copiato o imitato, non può essere duplicato fisicamente, e dunque non può essere manipolato e forgiato in maniera illegale.

In particolare, esso si distingue dalle "Fiat Currencies" per diversi motivi, di cui alcuni già menzionati:

- Non è soggetto ad emissione da parte di un'autorità o banca centrale, a differenza di tutte le altre valute nazionali in circolo attualmente.
- È soggetto ad inflazione soltanto perché non sono ancora stati emessi tutti i bitcoin (circa 21 milioni)[12], si prevede che una volta raggiunto il limite non dovrebbe esserci più inflazione in quanto non ci sarà più aumento dell'offerta di moneta. Le valute correnti, invece, sono soggette ad inflazione o deflazione continua, dovuta agli andamenti macroeconomici dell'economia globale e di quella della loro nazione di emissione.
- Le transazioni bitcoin sono registrate nella blockchain e di fatto quest'ultima funge da immenso registro dove ogni transazione è conservata. Fenomeno che è difficile verificare con le valute tradizionali.
- Le transazioni bitcoin sono anche immutabili, ovvero non possono essere duplicate come accade per le transazioni attuali digitali.
- Durante una transazione bitcoin bisogna pagare una piccola "fee" ai miners, evento molto simile al pagamento di una tassazione statale (IVA in Italia),

[12] *www.bitcoin.org*

l'unica differenza risiede nel fatto che una tassazione statale attuale può essere evasa con metodi illegali, ma relativamente facili; mentre è molto difficile, e richiede capacità informatiche al momento poco reperibili, osservare una transazione nella blockchain senza il pagamento della "fee" ai miners.

- Le transazioni bitcoin sono anonime, ma registrate attraverso indirizzi bitcoin, a differenza di molte transazioni monetarie che non passano assolutamente per nessun registro o notificazione.

In conclusione, la differenza principale tra un sistema monetario basato sul Bitcoin ed un sistema monetario tradizionale sta nella decentralizzazione del controllo dell'offerta di moneta. Charles Goodhart, nel suo celeberrimo paper "Two Concepts of Money" del 1998, afferma che gli stati hanno essenzialmente avuto sempre il pieno controllo sul sistema monetario ed ancora oggi è effettivamente così. Dunque, secondo il celebre economista britannico, bisogna porre l'attenzione del lettore sul fatto che gli stati hanno posto sempre forte fiducia nel signoraggio come fonte di "guadagno" e difficilmente tenderanno a cedere il dominio di tale risorsa ad una fonte privata di moneta.[13]

Inoltre, Goodhart afferma che la soluzione di affidare il sistema monetario ai privati, ha un sostegno storico poco affidabile, in quanto, quando si è provato ad effettuare scambi privatamente con un sistema basato sui metalli preziosi, le parti che scambiavano non riuscivano comunque ad avere una effettiva

[13] Goodhart C., *Two Concepts of Money,* 1998.

unità di conto su cui confidare. Difatti, Goodhart conclude affermando che solamente quando un'autorità centrale standardizza e riconosce il sistema monetario, quest'ultimo può essere diffuso e messo in pratica senza rischi e conseguenze nefaste.

1.4. Il Bitcoin dal 2009 ad oggi

Il tentativo di creare valore e scambiarselo digitalmente in assenza di un intermediario o di una controparte centrale è stato effettivamente realizzato grazie al genio di Satoshi Nakamoto. Tuttavia Bitcoin ha dei precursori chiamati ECash, HashCash, B-Money, Bit Gold, Anonymous Electronic Cash. Nonostante ciò, i precedenti esperimenti sono sempre stati bloccati o da problemi esogeni, ovvero governi che si sono opposti e hanno spento i server centrali, o endogeni, ovvero software con limiti strutturali che non potevano garantire a fondo il servizio promesso.

Adesso proveremo a ripercorrere le tappe fondamentali che hanno permesso al Bitcoin di sopravvivere rispetto alle concorrenti criptovalute e soprattutto, gli eventi che hanno permesso al Bitcoin di crescere e diventare sempre più solido.

Dopo la crisi di Wall Street nel 2008, il "famoso anonimo" Satoshi Nakamoto scrive ad una mailing list affermando di aver trovato un nuovo sistema monetario in grado di evitare l'intermediazione di terzi (intermediazione finanziaria), la spiegazione di tale sistema era riportata nel paper intitolato

"Bitcoin: A Peer-to-Peer Electronic Cash System"[14]. Tale sistema fu poi messo in pratica il 3 Gennaio 2019 con la nascita del primo blocco (blocco 0). Al momento della nascita,10000 BTC avevano una valenza di "poco più di una pizza da Papa John's"[15].

Un punto di svolta si ha nel Febbraio del 2011, quando il bitcoin raggiunge la parità col dollaro, quest'ultimo evento fu raggiunto grazie alla nascita dei primi Exchange dove era possibile negoziare bitcoin, il primo in particolare fu "Mt.Gox".

Dal 2011 in poi sempre più società ed exchange iniziarono a trattare ed accettare la nuova criptovaluta, tant'è vero che nel 2012 circa 1000 "merchants" accettavano pagamenti in bitcoin.

A cavallo tra il 2013 ed il 2014 diverse situazioni e circostanze hanno causato la prima crisi della criptovaluta, in primis la chiusura della piattaforma "Silk Road"(principale piattaforma di vendita di armi e droga dove il bitcoin era diventato moneta principale) aveva fatto creare nella mente delle persone l'associazione dell'illegalità al bitcoin, successivamente, nel dicembre del 2013, la banca centrale cinese emette un warning (allarme) destinato a tutte le istituzioni finanziarie, aziende e privati, affermando che qualsiasi operazione di compravendita con bitcoin verrà da quel momento considerata illegale. Un dato assolutamente rilevante considerando che in quel preciso momento l'80% delle transazioni venivano effettuate all'interno della

[14] Finley K., *"After 10 Years, Bitcoin Has Changed Everything—And Nothing"*, 31 October 2018.

[15] Wallace B., *"The Rise and Fall of Bitcoin"*, 23 November 2011.

Repubblica Popolare Cinese. Inoltre, il 19 Gennaio dell'anno seguente, Alibaba cancella i prezzi in bitcoin dal proprio portale e-commerce, facendo perdere alla moneta virtuale il suo principale mercato mondiale.

Agli inizi del 2014, invece, nello specifico, il 28 febbraio 2014 il maggiore exchange di bitcoin al mondo, Mt.Gox, dichiara bancarotta dopo aver subito un attacco hacker, nel corso del quale spariscono 750 mila bitcoin dei clienti e 100 mila della società.

Mt.Gox aveva già subito attacchi hacker in precedenza, ma quest'ultimo risultava fatale, decretando la chiusura definitiva del più grande exchange al mondo. La fiducia in bitcoin cala drasticamente portando il prezzo a perdere l'80% dai massimi toccati nell'anno precedente.

Alla fine del 2014, dunque, sembrerebbe che l'avventura bitcoin stava per arrivare agli sgoccioli, però, in realtà la tecnologia alla base del Bitcoin affascinava i maggiori esperti e difatti, avendo raggiunto un minimo storico iniziava ad attirare l'attenzione degli investitori istituzionali e privati. Tale movimento di capitali nel 2015 ha subito rapito l'attenzione mediatica che ha riportato in forte auge il bitcoin, creando una speculazione finanziaria di dimensioni bibliche. La crescita del valore continuò fino al 2017 quando la bolla finanziaria esplose riportando il prezzo del Bitcoin da circa 20000 dollari a 6000.

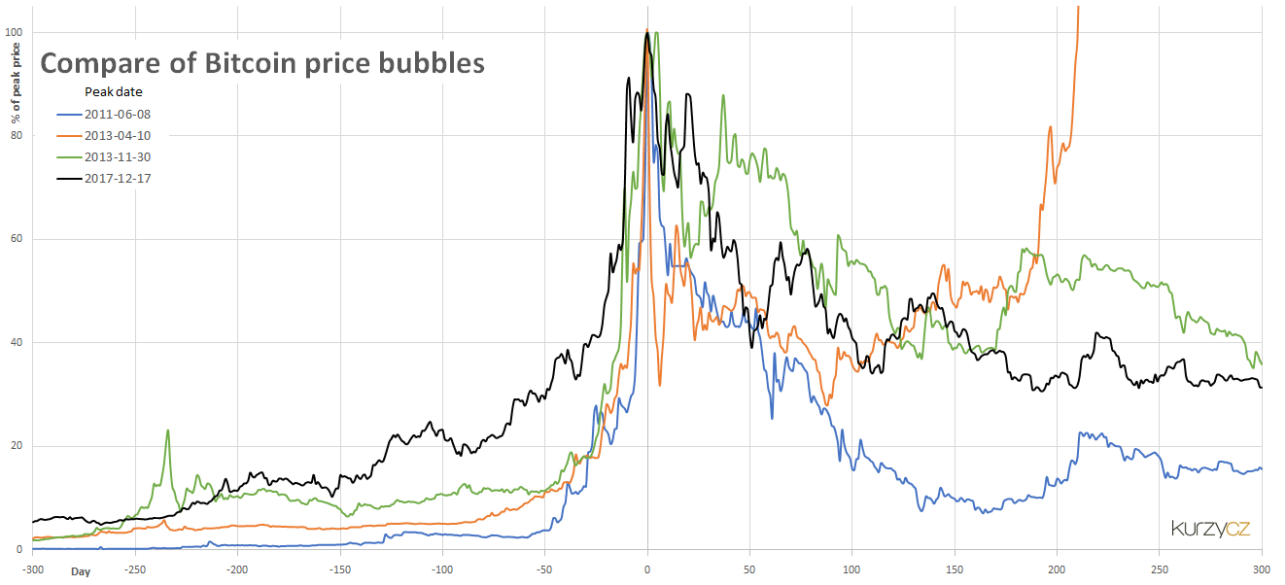
Figure 4. The price of a bitcoin (2012-2019)

[16] *Source: https://bitcoincharts.com/charts/bitstampUSD#a1gWMAzm1g5zm2g10zl*

Tale bolla ha causato forte perdite per la maggior parte degli investitori medi e soprattutto ha creato enorme sfiducia nell'immaginario collettivo verso la criptovaluta. Nell'ultimo anno tuttavia lo sviluppo del Bitcoin riprende la sua evoluzione, ed emerge l'interesse per la criptovaluta da parte di istituzioni e grandi investitori. Addirittura, NASDAQ annuncia che introdurrà un mercato di Future Bitcoin.

[16] *https://bitcoincharts.com/charts/bitstampUSD#a1gWMAzm1g5zm2g10zl*

Figure 5. Comparison between bitcoin bubbles since 2009



[17] *Source: http://www.kurzy.cz/zpravy/440516*

In conclusione, la storia dei primi 10 anni del Bitcoin ha visto momenti di florido sviluppo e momenti di amara crisi e purtroppo, solamente il futuro potrà rivelarci la validità di tale tecnologia e l'utilizzo che se ne farà globalmente di essa.

[17] *http://www.kurzy.cz/zpravy/440516*

Capitolo 2

2. La tecnologia Bitcoin

Il sistema Bitcoin è essenzialmente un sistema di pagamenti elettronici, decentralizzato e basato su una grande Rete. Tale rete Bitcoin consente il possesso e il trasferimento anonimo delle monete; i dati necessari a utilizzare i propri bitcoin possono essere salvati su uno o più personal computer sotto forma di "portafoglio" digitale, o mantenuti presso terze parti che svolgono funzioni simili a una banca. In ogni caso, i bitcoin possono essere trasferiti attraverso Internet verso chiunque disponga di un "indirizzo bitcoin". La struttura peer-to-peer della rete Bitcoin e la mancanza di un ente centrale rende impossibile a qualunque autorità, governativa o meno, il blocco dei trasferimenti, il sequestro di bitcoin senza il possesso delle relative chiavi o la svalutazione dovuta all'immissione di nuova moneta.

Nella realtà pratica chiunque con un indirizzo Bitcoin può accedere alla rete. Quando un utente si collega alla rete Bitcoin, l'utente è connesso a un insieme di altri utenti chiamati nodi[18]. Collegandosi alla rete l'utente scarica la blockchain, che è un registro pubblico di tutte le transazioni fatte fino a quel momento.

[18] *www.bitcoin.org*

Quando un utente crea una transazione, questa viene trasmessa a tutti gli altri nodi della rete.

Non molto dopo che la transazione sia stata trasmessa, l'intera rete è in grado di disporre delle informazioni relative alla transazione eseguita. Ogni dieci minuti, in media, tutte le operazioni vengono memorizzate in un blocco stabile che viene aggiunto al blockchain.

Il ruolo di quest'ultima risulta dunque fondamentale in quanto contiene l'intero registro pubblico delle transazioni avvenute tramite bitcoin.

La rete è progettata per rilasciare circa 21.000.000 di bitcoin, non tutti sono stati rilasciati immediatamente, ma ancora adesso attraverso funzioni matematiche specifiche vengono rilasciati con ogni blocco della blockchain e si prevede che con il raggiungimento del limite di bitcoin l'inflazione dovrebbe arrestarsi in quanto non ci sarebbe più aumento di moneta nel sistema economico.

Adesso procederemo con l'analisi più dettagliata di tutti gli elementi chiave della tecnologia Bitcoin, ovvero la crittografia, la blockchain, il fenomeno del mining e gli attori di tale meccanismo.

2.1. La crittografia

Nel protocollo Bitcoin per la generazione delle chiavi, ma soprattutto per la loro interazione a senso unico, è stato scelto l'algoritmo ECDSA, ovvero la Crittografia a Curva Ellittica, capace di concatenare facilmente le due chiavi

(pubblica e privata) con l'obiettivo però di rendere impossibile risalire alla chiave Privata a partire da quella Pubblica, rendendo il sistema univoco è quindi possibile operare nella sicurezza informatica sfruttando la crittografia. Dunque, la base della sicurezza del bitcoin si trova nel fenomeno della crittografia. Quest'ultima studia la branca della "crittologia" delle "scritture nascoste", ovvero un metodo per rendere un messaggio non decifrabile da terze persone.

2.1.1. Evoluzione crittografica

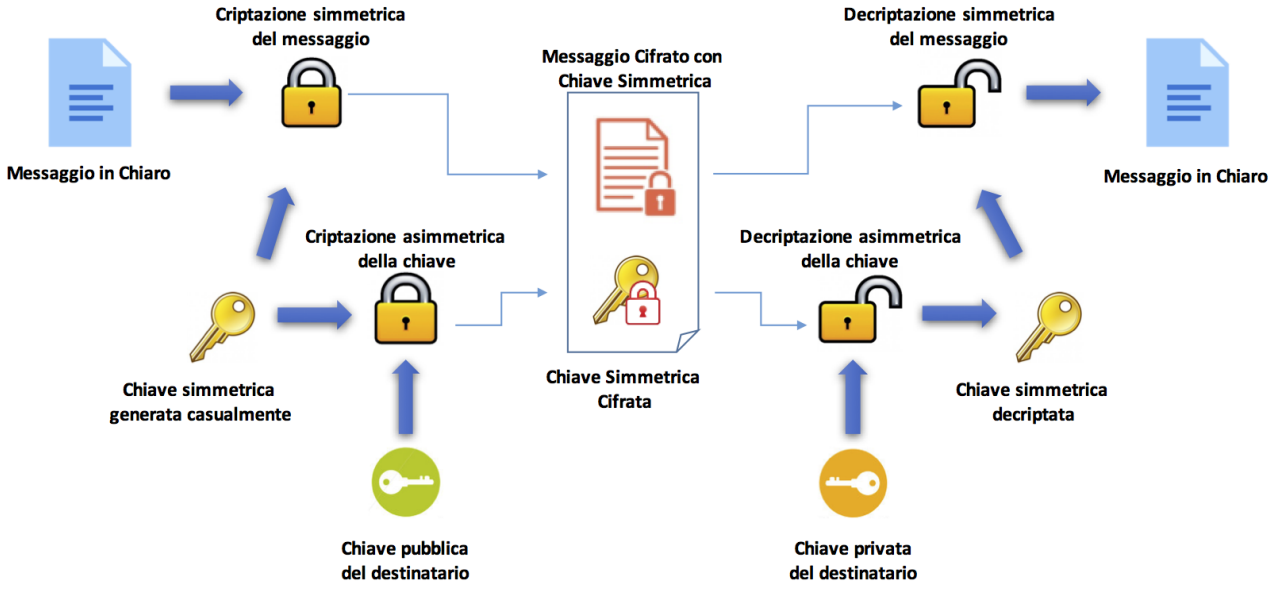
Tale sistema non nasce con l'avvento della tecnologia e dell'high tech, ma ha origini ben radicate nella storia. Le prime testimonianze di utilizzo della crittografia risalgono ad alcuni geroglifici egizi, successivamente a Gaio Giulio Cesare con il "cifrario di Cesare"[19], passando per il grande genio della crittografia Alan Turing, arrivando agli algoritmi specializzati dell'epoca contemporanea.

La macchina crittografica più famosa della storia è sicuro "Enigma", utilizzata dai nazisti durante la guerra per comunicare, quest'ultima si basava su un sistema di cifratura simmetrica, ad esempio la lettera A corrispondeva alla lettera I in una determinata posizione del testo e viceversa. Secondo i tedeschi tale macchina era inattaccabile, ma in realtà un gruppo di inglesi (tra cui Alan Turing) riuscì a decifrare l'algoritmo e sfruttare le debolezze di tale

[19] D'Agapeyeff A., *Codes and Ciphers - A History of Cryptography*.

macchina sin dall'inizio della guerra. Una delle debolezze dell'Enigma risiedeva proprio nella crittografia di tipo simmetrico, nella quale si ha una chiave, utile per criptare un messaggio che vogliamo recapitare a qualcuno rendendolo quindi incomprensibile, e contemporaneamente, sempre con la stessa chiave, per decriptarlo, renderlo quindi comprensibile al destinatario. Chiunque sia però in possesso di tale chiave può eseguire entrambe le procedure, rendendo di fatto la trasmissione insicura.

Figure 6. Schema crittografia simmetrica e asimmetrica



[20] *Source: https://www.javaboss.it/crittografia-in-java/?doing_wp_cron=1558462824.8484680652618408203125*

[20] *https://www.javaboss.it/crittografia-in-java/?doing_wp_cron=1558462824.8484680652618408203125*

Per superare tale limite si è pensato ad un altro tipo di crittografia, ovvero asimmetrica, dove, invece, si assiste all'adozione di due chiavi, anziché una sola, una per criptare il messaggio, ed una per decriptarlo, queste chiavi sono dette:

chiave privata, utilizzata per decriptare il messaggio e chiave pubblica, utilizzata per criptare il messaggio. Con questo sistema dunque, si implementa il meccanismo della "doppia firma" che risulta essere quasi inattaccabile dal punto di vista della sicurezza criptografica.

2.1.2. Crittografia e Bitcoin

Il sistema bitcoin si basa anche sulle funzioni di hash, capaci di rendere ancora più sicura la trasmissione delle transazioni. Tali funzioni si basano su una procedura che trasforma un messaggio di lunghezza arbitraria in un codice alfanumerico di lunghezza prefissata. La caratteristica principale di questo algoritmo è che è unidirezionale, ovvero è molto improbabile invertirla e quindi risalire al messaggio a cui è stato applicato, rendendolo di fatto perfetto per svariati utilizzi nella crittografia.

Bitcoin utilizza l'algoritmo Sha256 che, come si evince dal nome, prevede l'utilizzo di 256bit, pertanto se si volesse risalire al messaggio codificato con tale algoritmo si dovrebbe tirare ad indovinare per un numero di tentativi di 2^256. Questo numero è ridicolamente enorme: il canale YouTube

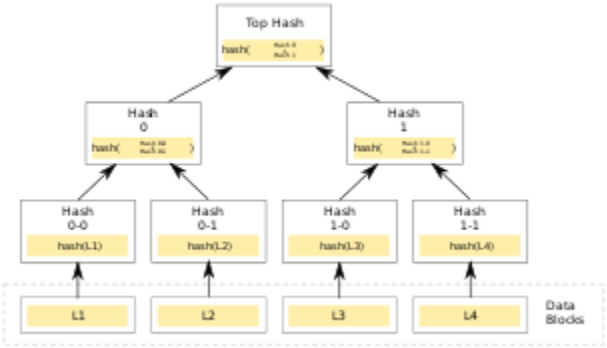
3Blue1Brown[21] ha reso in maniera molto chiara a quanto corrisponda, per farlo ipotizza di avere un computer in grado di generare 4 miliardi di hash al secondo, allo stesso tempo ipotizza di avere 4 miliardi di computer come questo, a questa strana unità di computer ipotizza che Google ne abbia 1000 unità per ognuna, e di dotare ogni persona della terra (circa 7,3 miliardi) di 1000 unità di questo «server», successivamente ipotizza che vi siano 4 miliardi di copie della terra dove ogni persona sia dotata di questo server da 1000 unità di cui ognuna ha 4 miliardi di computer ognuno dei quali genera 4 miliardi di hash al secondo, non contenti immaginiamo pure 4 miliardi di galassie con 4 miliardi di copie della terra al loro interno sempre con tutti quei «server», saremmo arrivati a 2^160 tentativi ogni secondo. Ancora lontani.

2.2. La Blockchain

La blockchain è una lista in continuo aggiornamento di "records", definiti blocks, i quali sono correlati e collegati tra di loro attraverso meccanismi criptografici. Ogni blocco contiene informazioni riguardanti il blocco precedente, in particolare informazioni sulle funzioni di hash in grado di generare un ordine cronologico ed una data precisa, la struttura spesso viene definita "Merkle tree" (figura 22).

[21] *https://youtu.be/S9JGmA5_unY*

Figure 7.



[22] *Source*: Merkle R. C., *"A Digital Signature Based on a Conventional Encryption Function". Advances in Cryptology,* (1988)

Osservando la figura si può facilmente ricostruire il percorso fatto dai "nodi" e risalire alla transazione desiderata, ciascun blocco della catena contiene quindi diverse operazioni corrispondenti ai relativi trasferimenti di Bitcoin da un indirizzo all'altro, facendo riferimento al blocco precedente e a quello successivo. Pertanto, se si comincia dal primo blocco mai creato sulla blockchain e si procede attraverso i "successivi blocchi", la conseguenza sarà un passaggio obbligato per ogni blocco della rete Bitcoin.

Il funzionamento di una transazione in bitcoin segue un percorso ben preciso che risulta nel semplice passaggio di una certa quantità di bitcoin da un indirizzo Bitcoin ad un altro o più indirizzi. Nella realtà pratica di una transazione, un utente invia uno script al destinatario e quest'ultimo attraverso tale script può facilmente ritirare la somma di bitcoin scambiata.

[22] Merkle R. C., *"A Digital Signature Based on a Conventional Encryption Function". Advances in Cryptology,* (1988)

Tale transazione viene immediatamente registrata nella blockchain e confermata dagli altri utenti, e difatti, una volta registrata non può essere modificata in quanto per modificare tale transazione bisognerebbe alterare in maniera retroattiva tutti i dati dei blocchi collegati all'ultimo blocco creato.

La base, dunque, della blockchain è il blocco, quest'ultimo raggruppa le transazioni e può avere una lunghezza variabile in base alla lunghezza della transazione stessa. Il blocco può essere suddiviso in due "zone": un corpo ("body") e una testa ("header"), nel primo è contenuto l'insieme di transazioni, mentre nella seconda è possibile osservare sette caratteristiche identificative, simili alle basi azotate del Dna, che forniscono informazioni fondamentali per l'inserimento del blocco nella blockchain[23].

2.2.1. Il meccanismo del "blockchain consensus mechanisms"

In qualsiasi sistema centralizzato, un amministratore centrale ha l'autorità ed il potere di mantenere, conservare ed aggiornare il database, difatti, la facoltà di fare qualsiasi aggiornamento a quest'ultimo (aggiungere, eliminare, modificare ecc..) rimane nelle sole mani dell'autorità centrale.

Diverso è il discorso fattibile per una blockchain pubblica, in quanto il principio dominante è avverso ed è proprio la decentralizzazione, dove il sistema si autoregola su una scala globale senza l'intervento di

[23] *Blockchain,* su *www.blockchain.com*

nessun'autorità centrale. Il meccanismo coinvolge partecipazione da parte di centinaia di migliaia di partecipanti che lavorano sulla verifica e sull'autenticazione della transazione nella blockchain e sulle attività di mining sui blocchi.

In un sistema caratterizzato da tale dinamicità, i registri pubblici di tale importanza necessitano di un'efficiente, leale, funzionale e sicuro meccanismo che vada a certificare che tutte le transazioni contenute in esso siano veritiere e corrette e, soprattutto, che tutti i partecipanti abbiano raggiunto un consensus. Quest'ultimo viene raggiunto proprio dal "blockchain mechanism consensus", che rappresenta un insieme di regole che decidono sulla contribuzione di tutti i vari partecipanti della blockchain.

Sono stati rilevati due principali metodi di "consensus mechanism algorithms" che si basano su principi diversi: il primo è chiamato proof of work (POW), mentre il secondo proof of stake (POS).

Il POW è utilizzato dalle principali criptomonete, in particolare Bitcoin e Litecoin, esso prevede che un partecipante debba provare che il nodo precedente sia giusto e qualificabile come tale per ottenere il diritto ad aggiungere una nuova transazione nella blockchain. Questo sistema nel Bitcoin è definito Mining.

Il POS, invece, è utilizzato da Ethereum ed è considerato la versione "low-cost and low-energy" del POW algorithm, difatti, il partecipante si assume la responsabilità della qualifica della transazione solamente in proporzione al numero di criptovaluta che contiene.

Esistono altri consensus algorithms, ad esempio Proof of Capacity (POC), che si basano su altri principi e che non sono particolarmente diffusi nel sistema della criptovalute.

2.3. *Il mining e gli attori del sistema*

L'attività di mining risulta essenziale per il corretto sviluppo e funzionamento del sistema Bitcoin ed è anche l'unico metodo capace di immettere nuova moneta nel sistema. Attraverso l'attività di mining si assiste al processo di aggiunta di "transaction records" al registro pubblico delle transazioni, per tale motivo è considerato un'attività "resource intensive" e, soprattutto, molto difficile in modo da mantenere costante il numero di blocchi creati ogni dato intervallo temporale.

Il primo obiettivo del miner è quello di analizzare il blocco e confermare la cronologia di transazioni in modo da renderla impossibile da manipolare, modificare o eliminare da nessun altro soggetto. Dunque, il fine primario del mining riguarda la sicurezza del sistema, attraverso il proof of work contenuto nei blocchi. Per quanto riguarda l'immissione di nuova moneta, invece, quando un minatore risolve il problema del blocco e viene creato un nuovo blocco, il minatore si prende sia la ricompensa e sia gli additional fee sulle operazioni presenti nel blocco. A partire da questo momento i premi complessivi spettanti ai minatori cresceranno proporzionalmente con il valore monetario di Bitcoin e la quantità di transazioni.

Considerando che fee ulteriori potranno essere aggiunti ad una operazione, tanto più grande sarà la loro quota tanto maggiore sarà la velocità delle transazioni. La mancata aggiunta dei costi opzionali impedisce di garantire che una transazione entri a far parte della blockchain.

Dal momento che ogni singolo minatore ottiene dei premi o ricompense, qual dir si voglia, dall'attività di mining sono state create una serie di piscine minerarie, le cosiddette mining pools. Si tratta di una raccolta di diversi minatori che svolgono insieme l'attività di mining sui blocchi in maniera tale da aumentare la probabilità di eliminare un blocco, e quindi

ottenere la ricompensa in Bitcoin, nonché le commissioni aggiuntive.

Migliaia di computer, gestiti da minatori, sono in competizione per risolvere il problema matematico e la difficoltà di risolvere il quesito matematico è crescente o decrescente a seconda della potenza di hashing globale che cerca di risolverlo.

In media si può affermare che ciascun quesito matematico sia risolto ogni dieci minuti. Quando il problema è risolto viene creato un nuovo

blocco con la corrispondente assegnazione di un premio al minatore. La ricompensa era di 50 Bitcoin per i primi quattro anni successivi alla loro introduzione.

Attualmente tale cifra risulta dimezzata e circa 25 Bitcoin vengono rilasciati ogni qualvolta sia risolto un nuovo blocco e aggiunto al blockchain.

Inoltre, per ogni transazione, al momento dell'inoltro, una commissione opzionale può essere aggiunta alle operazioni, consentendo una maggiore celerità nell'esecuzione delle stesse. Le commissioni di transazione sono utilizzate come difesa da attacchi di utenti che cercano di dossare la rete inviando numerose transazioni. Non esiste ancora un modo standardizzato per le commissioni, non si basano su percentuali di transazione, né su somme fisse e perciò, non essendo legata alla quantità di bitcoin inviata, la commissione può sembrare estremamente bassa (0,0005 BTC per il trasferimento di 5000 BTC) o ingiustamente alta (0,005 BTC per un pagamento di 1 BTC).

La commissione è definita da attributi come la mole di dati della transazione ed il numero di indirizzi in cui è suddiviso l'importo da inviare.

Al momento dell'invio di una transazione nel sistema, essa è quasi immediatamente sottoposta a tutta la rete. Sono sufficienti pochi secondi perché una transazione possa essere riconosciuta dai nodi, ma ci vuole più tempo perché una transazione possa essere confermata.

Per le transazioni più grandi occorrono più firme. La prima conferma significa che la transazione è all'interno di un blocco, e ulteriori conferme indicano che altri blocchi sono stati aggiunti come prolungamento della catena. Dopo 6 conferme si ritiene che chiunque possa confidare nella buona fede della transazione attuata.

2.4. Le piattaforme ed i wallets

Un'importante limitazione di un sistema basato sul bitcoin potrebbe essere riconosciuta nel fatto che l'unico modo che si ha a disposizione per scambiare moneta è attraverso l'utilizzo di criptocurrency wallets[24].

Questi ultimi fungono da veri e propri wallets, ovvero servono per detenere moneta, come un conto in qualsiasi banca, e contengono dati segreti riguardanti le chiavi private o "seed" che servono per apporre la firma sulle transazioni e, dunque, forniscono la prova matematica che attesta che tale transazione ha coinvolto quel determinato wallet.

In conclusione, per l'utilizzo del sistema bitcoin, una volta appreso il funzionamento ed averne riconosciuto la validità, è necessario l'utilizzo di due strumenti: i wallets e le piattaforme di scambio (exchange).

I wallets possono essere di diversi tipi, distinti in base a diversi criteri di tecnologia:

per quanto riguarda la tecnologia, si differenziano digital apps da hardware based, ovvero se avere un rapporto diretto con l'user o utilizzare terze parti per conservare la chiave private; per quanto riguarda, invece, la firma, si distinguono multisignature wallets da quelli a firma singola, la differenza risiede nel grado di sicurezza che una multisignature può fornire alla transazione, in quanto è confermata e testimoniata da più soggetti; per quanto riguarda, infine, la determinazione della chiave, si differenziano portafogli

[24] Divine J., *"What's the Best Bitcoin Wallet?"*, 1 February 2019.

"deterministici" da "non deterministici", i primi sono caratterizzati da una "root key" che genera altre chiavi creando un vero e proprio "tree of key pairs" ed ovviamente tutte le chiavi secondarie generate hanno come risorsa di riferimento la root key, i secondi, invece, non hanno tale funzionamento, anzi, ogni chiave è generata in modo randomico senza l'utilizzo di una fonte comune.

È importante specificare, a questo punto, che i wallets non contengono bitcoin, ma solamente la coppia di chiavi pubbliche e private che permettono di risalire alle transazioni effettuate e dunque ad un bilancio dei bitcoin che, in realtà, rimangono nel registro pubblico (Blockchain).

Un altro ruolo fondamentale all'interno del meccanismo Bitcoin è svolto dalle piattaforme di scambio, chiamate Exchange; quest'ultimi rappresentano i "luoghi" dove è possibile scambiare bitcoin per altre valute e per svolgere l'attività di trading. Il sito ufficiale Bitcoin stesso evidenzia alcune delle migliori piattaforme autorizzate a svolgere tale funzione.

È possibile dunque riportare alcune delle più celebri e utilizzate piattaforme:

Il broker più utilizzato al mondo è Coinbase, che offre anche la funzionalità di "web wallet", con 6,5$ miliardi di capitalizzazione e circa 4 milioni di clienti, i punti di forza che hanno portato tale piattaforma a tale livello sono due: il design del sito e la facilità negli acquisti immediati, e la possibilità di assicurazioni attraverso partnership con diverse banche.

Successivamente, gli altri due broker più celebri possono essere considerati CEX.IO e Localbitcoins, il primo si basa sulla possibilità di acquistare e negoziare bitcoin anche con un profilo non verificato e soprattutto adotta una politica "zero tolerance" nei confronti del riciclaggio e tutte le attività ad esso connesse; il secondo, invece, è un P2P exchange, ovvero lascia ai privati la gestione del mercato e degli scambi, infatti, i termini e le condizioni degli scambi vengono stabiliti privatamente tra i due o più soggetti. La caratteristica che distingue localbitcoins dagli altri exchange è la facilità di effettuare scambi senza passare prima per lunghe verifiche identificative, difatti è possibile svolgere attività sulla piattaforma senza fornire informazioni personali.

Capitolo 3

3. Se il Bitcoin fosse l'unica moneta in circolazione?

Attualmente l'idea di sostituire totalmente tutte le valute tradizionali correnti sembrerebbe essere ancora un avvenimento di lontananza abnorme, tuttavia, in questo capitolo la tesi si proporrà di ipotizzare un sistema economico nel quale l'unica moneta utilizzata sia il Bitcoin, risultante unico sopravvissuto della concorrenza tra monete private. Di conseguenza, i quesiti ai quali si cercherà di ideare una risposta ipotetica riguarderanno la base monetaria, la teoria quantitativa della moneta e l'inflazione, la funzione delle banche ed

infine una trattazione sulla legislazione e regolamentazione della criptovaluta.

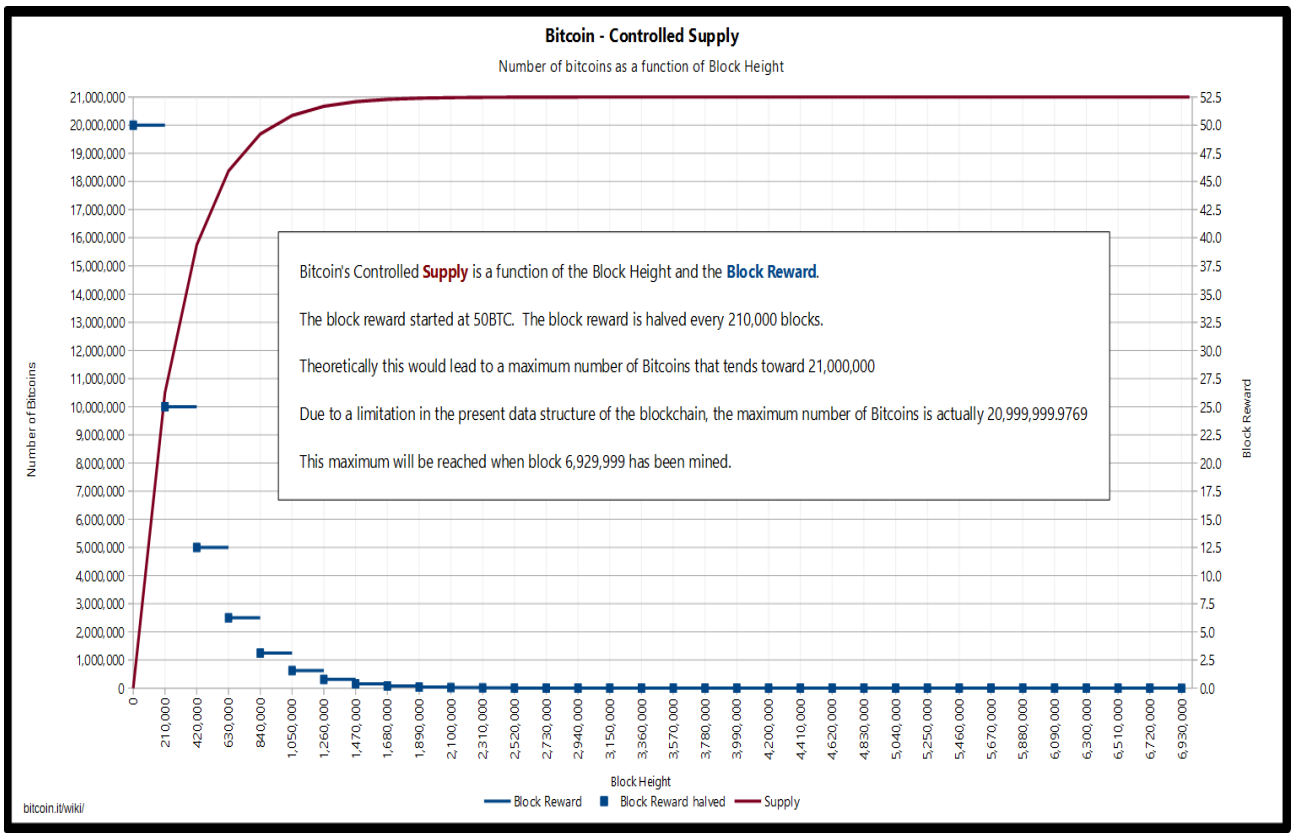
3.1. Bitcoin e offerta di moneta controllata

Nel suo celebre paper intitolato “Interest and Usury”, Bernard W. Dempsey, S.J. affermava che un’offerta di moneta fissa, o indicizzata ed ancorata a criteri matematici ben definiti e corretti, è la condizione necessaria per un prezzo reale e giusto della moneta.

Il sistema Bitcoin, come visto precedentemente, è decentralizzato, ovvero la valuta non è emessa da una banca centrale e non ha obiettivi di crescita, come ad esempio un tasso di crescita che sia pari all’aumento del volume di beni scambiati in modo da mantenere i prezzi stabili. La base monetaria in un sistema centralizzato è governata dalla banca centrale, in un sistema decentralizzato, invece, non è supervisionata e controllata da parte di nessun ente statale o sovranazionale. Tutta l’offerta di moneta è dunque generata e immessa del mercato dai nodi del sistema peer-to-peer attraverso un algoritmo ben definito, che prevede, già in partenza, la modalità e le tempistiche del rilascio di tutta la moneta fino al raggiungimento di un obiettivo fissato a priori.

In particolare, il Bitcoin prevede specifici tassi di creazione di moneta ed aumento di base monetaria, ovvero il tasso è modificato ogni 2016 blocchi creati, in modo da mantenere un tasso costante su base settimanale.

Figure 8. Graph of Bitcoin's controlled supply, showing the supply as a function of the block height and the block reward

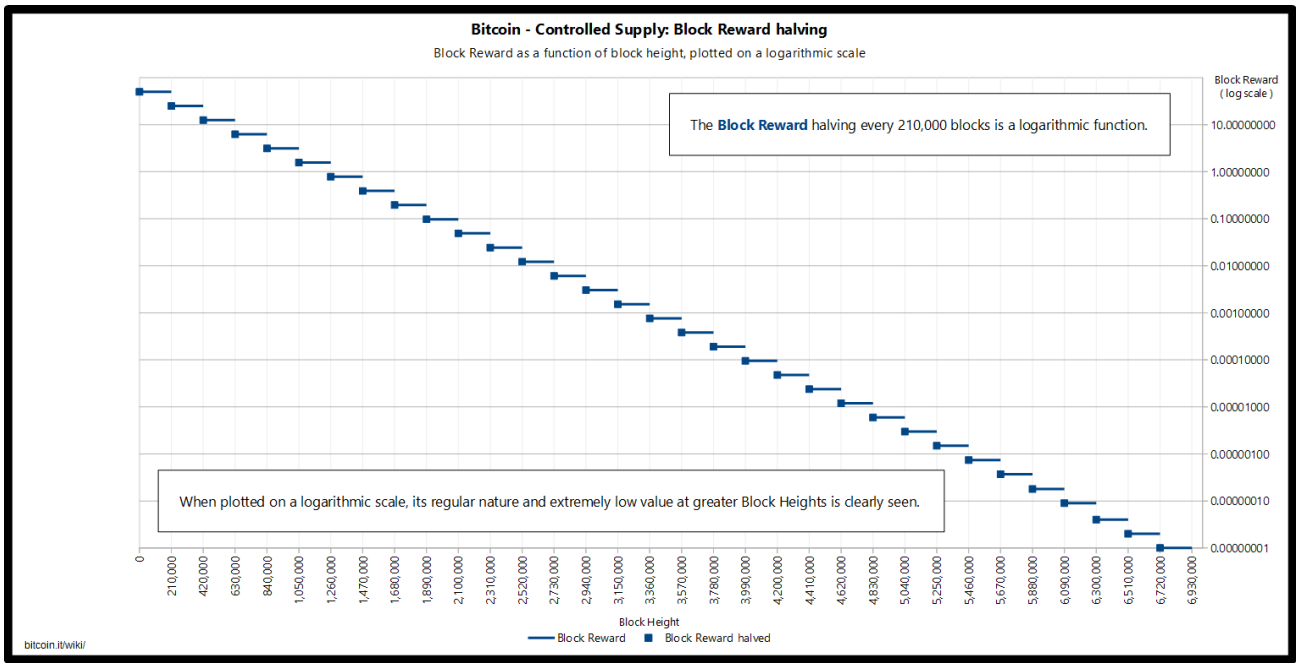


[25] Source: *https://bashco.github.io/*

La progressione del rilascio di Bitcoin è geometrica decrescente, difatti è prevista la diminuzione di circa il 50% ogni 200.000 blocchi; il risultato di tale algoritmo porta ad un totale finale di 21 milioni circa di bitcoin creati.[26]

[25] *https://bashco.github.io/*
[26] In realtà il numero preciso di Bitcoin emessi dovrebbe avere un asintoto al valore 20,999,999,9769.

Figure 9. Graph of the Block Reward halving schedule plotted against a logarithmic scale.



Source: https://bashco.github.io/

Si può facilmente concludere a questo punto che l'offerta di moneta nel sistema Bitcoin è caratterizzata da un andamento generalmente costante nel suo algoritmo, in sintesi, la differenza tra il tasso atteso ed il tasso realizzato dovrebbe tendere allo zero.

Un sistema con impostazione decentralizzata era già stato affrontato dal celebre studioso Hayek che, anche se con notevoli differenze nella tecnologia e nella modalità, lo considerava un modello perfetto, dove il principio fondamentale era la coesistenza di valute concorrenti private emesse da banche private. In questo contesto non era contemplata la possibilità di osservare una valuta emessa da una banca centrale o dal governo in quanto sarebbe andata a minare l'impostazione decentralizzata dell'ipotesi di Hayek. Dunque, quest'ultimo arrivò alle seguenti asserzioni conclusive:

- In primis, una valuta verrà classificata in base alla sua qualità che può essere osservata attraverso il potere d'acquisto e la stabilità. Tali caratteristiche andranno a determinare il calo della domanda delle monete non qualitativamente valide, portandole alla loro estinzione e alla sopravvivenza solo di una o poche valute.
- In secondo luogo, ogni banca privata cercherà di evitare il più possibile sia l'inflazione sia la deflazione, in modo da evitare qualsiasi incomprensione o alterazione del potere d'acquisto.
- Infine, Hayek poneva come presupposto all'osservazione, l'obiettivo da parte di ogni emittente privato di massimizzare la qualità della propria valuta, senza dunque avere tattiche strategiche diverse di speculazione o altro.

In conclusione, Hayek era convinto che fosse di necessaria importanza allontanare l'intero controllo dal governo e dalle banche centrali, poiché una sana competizione avrebbe potuto portare ad una valuta migliore. Difatti, il Bitcoin rappresenta un esempio della sua teoria e potrebbe creare una plausibile soluzione contro l'instabilità del mercato attuale per due principali motivi: il primo motivo si basa sul principio che prevede come favorevole alla stabilità un tasso predeterminato per l'emissione di nuova valuta bitcoin, il secondo, invece, è una conseguenza del primo e, infatti, delinea il fatto che la comunità Bitcoin non è in grado di controllare il valore della sua moneta, aumentando o diminuendo l'offerta di Bitcoin e di conseguenza, l'andamento economico non è manipolato da nessun ente, banca centrale o soggetto in particolare.

3.2. Bitcoin e la funzione delle banche

Di recente si è spesso affrontato il dibattito su quali sarebbero le conseguenze del rapporto tra Bitcoin e le banche centrali ed è stato possibile derivare due filoni di pensiero più evidenti:

- Il primo filone riconosce ancora l'importanza fondamentale del ruolo svolto dalle banche centrali. Gli obiettivi che quest'ultime si prefiggono sono stati considerati di forte ordine generale e benessere pubblico, infatti di solito la creazione o la distruzione di moneta è attuata per soddisfare dei fini come il mantenimento del pieno impiego, dei prezzi stabili; l'assicurare liquidità e sicurezza nel sistema finanziario; la stabilità in tempi non positivi del ciclo economico.

  È naturale affermare anche che il monopolio di potere affidato alle banche centrali abbia delle conseguenze in tutti gli ambiti, sia a livello nazionale, sia a livello internazionale, poiché una politica economica imperfetta o attuata col tempismo perfetto può creare forti sbalzi sull'economia generale ed avere un effetto diretto sul valore della valuta nazionale, causando disoccupazione, iperinflazione o altre conseguenze non considerabili positive.

- Il secondo filone, invece, si colloca nella prospettiva in cui la banca centrale non è più fondamentale e necessaria per lo sviluppo economico del paese. Infatti, la forte complessità associata alle economie nazionali e globali ha dato vita al pensiero che tali economie sono effettivamente imprevedibili e

dunque difficilmente governate dal tipo di manipolazione che le banche centrali cercano di attuare.

Questo pensiero è stato coniato e portato avanti già dagli esponenti della Scuola Austriaca ed è facilmente attuabile al discorso del Bitcoin. In aggiunta, molto frequentemente nell'epoca moderna le banche centrali sono state oggetto di forti critiche che hanno causato evidenti malcontenti nelle popolazioni nazionali. Difatti, una critica che è stata spesso mossa si regge sul concetto di monopolio di potere attribuito alle banche centrali che non viene pienamente concordato dalle persone e, soprattutto, sull'idea di un'entità esterna che ha effettivamente il libero potere di manipolare l'intera economia secondo i suoi canoni ed obiettivi. Di conseguenza, moltissimi studiosi (tra cui economisti, politici e sociologi) hanno posto l'attenzione dei lettori delle loro opere sulle conseguenze che un errore della banca centrale può portare sull'intera vita dei cittadini. I più noti problemi che una banca centrale può creare interpretando male la politica economica da effettuare sono:

- Aumento dell'offerta di moneta, creando forte inflazione e danneggiando il potere d'acquisto dei consumatori.
- Aumento dei tassi d'interesse, scoraggiando l'investimento e i prestiti.
- Adozione di un tasso di inflazione troppo basso, creando disoccupazione.
- Adozione di politiche con tassi di interesse non corretti e naturali, causando possibili sbalzi di alcuni settori del mercato che possono degenerare in vere e proprie bolle.

In conclusione, è molto utopistico immaginare un sistema economico senza la presenza delle banche, difatti, nell'ultimo periodo stiamo comunque assistendo al riconoscimento del Bitcoin per moltissime attività economiche ed anche le banche hanno dunque iniziato a riconoscerne il valore e la "minaccia". Alcune banche hanno cercato di far guerra a tale innovazione, altre si sono essenzialmente adeguate a quest'ultima. In particolare, si sta delineando una visione che contempla la coesistenza del Bitcoin e delle valute tradizionali fino a quando i governi non riconoscano il Bitcoin come una valuta legittima, ed in quel caso, ci sarebbe la possibilità di "uccidere" le banche centrali. Infine, per adesso le banche centrali stanno studiando Bitcoin, considerando anche che la creazione delle monete di metallo è un'attività costosa.

È necessario, a questo punto, analizzare quale sarebbe il ruolo delle banche comuni e non centrali all'interno di un sistema con Bitcoin legittimato.

Quest'ultime svolgerebbero lo stesso ruolo che si trovano a svolgere attualmente se il sistema bancario rimanesse a riserva frazionaria, ovvero andrebbero a creare moneta in base al rapporto riserve/depositi. Importante specificare anche che il sistema bancario andrebbe a creare moneta, senza generare ricchezza, ma solamente aumentando la liquidità del sistema economico fornendo prestiti ed attività attualmente diffuse.

3.3. Bitcoin e spirale deflazionistica

Un importante tema legato alla questione Bitcoin è rappresentato dal concetto della possibile "spirale deflazionistica"[27], dovuta alla natura stessa della valuta, infatti un tipo di moneta basato su un'offerta fissa e decrescente nel tempo, crea i presupposti per un sistema incline alla deflazione e resistente all'inflazione.

Tale concetto non deve essere analizzato ed immaginato solamente come un fenomeno di carattere negativo e che vada ad inficiare le capacità di sviluppo del sistema economico, anzi, secondo alcuni studiosi può portare addirittura ad un'efficienza più elevata. In sintesi, la spirale deflazionistica si genera quando in un periodo di deflazione gli attori economici tendono a rimandare spese ed investimenti ad un futuro ritende che quest'ultimo possa essere ancora più vantaggioso.

Secondo la maggior parte degli economisti, nel caso del Bitcoin, la spirale deflazionistica si verrebbe a creare a causa della mancanza di liquidità e dell'offerta di moneta decrescente; questo processo porterebbe sia ad un aumento del valore del bitcoin, sia ad una diminuzione dei prezzi di beni e servizi, generando una riduzione anche dei salari e della produzione, e dunque, della domanda di beni e servizi che causerebbe poi ad un'ulteriore deflazione, portando in vita un vero e proprio circolo vizioso.

Altri economisti, invece, credono fortemente che la deflazione del sistema Bitcoin debba essere distinta da una generica di una moneta tradizionale, in

[27] BITMEX RESEARCH, *Bitcoin Economics – Deflationary Debt Spiral.*

quanto l'offerta della moneta è già delineata e scritta, dunque, non è generata da un collasso della domanda di moneta. In questo caso, si ipotizza che il superamento di una deflazione del genere possa essere effettuato tramite un'applicazione di sconti tali da invogliare gli attori economici a spendere nonostante il loro istinto ad attendere e risparmiare. [28]

3.4. Conclusioni ed implicazioni sulla regolamentazione

In conclusione, l'elaborato si è posto come obiettivo quello di effettuare un'analisi abbastanza multilaterale e completa del fenomeno Bitcoin che è ancora largamente sconosciuto alle menti non del settore.

Come si è potuto notare il sistema Bitcoin rappresenta un'interpretazione ideologica e definibile quasi filosofica di un sistema economico che cerca di ribaltare completamente tutte le certezze interiorizzate negli ultimi secoli dalla società attuale. Difatti, quest'ultimo ha destato molto stupore e ha suscitato l'attenzione e la necessità di una regolamentazione corretta. Per tale motivo, il Bitcoin risulta essere molto volatile attualmente, in particolare, perché non è ancora stato legittimato e molto frequentemente ed in diversi paesi si è cercato di regolamentare in maniera discorde e sotto diversi aspetti tale criptovaluta, non creando un'armonizzazione nei suoi confronti.

Si pensa spesso che le criptovalute operino al di fuori della portata dei regolamenti nazionali, tuttavia le loro quotazioni, i volumi delle transazioni

[28] Antonopoulos, tdr, 2014, p.176

e i loro bacini di utenza sono fortemente influenzati dalle notizie riguardanti gli interventi regolamentari.

Le notizie riguardanti divieti generici imposti alle criptovalute o il loro trattamento nell'ambito delle legislazioni sui valori mobiliari producono il maggior effetto negativo sulle quotazioni, seguite da quelle sulla lotta al

riciclaggio di denaro e al finanziamento del terrorismo e da quelle sulla restrizione dell'interoperabilità delle criptovalute con i mercati regolamentati. Le notizie riguardanti l'adozione di un quadro normativo incentrato sulle criptovalute e sulle initial coin offering (ICO) coincidono con forti rialzi sui mercati.

Dato che le criptovalute si affidano a istituzioni finanziarie regolamentate per operare e che i mercati sono (ancora) segmentati tra le giurisdizioni, esse rientrano nell'ambito dei regolamenti nazionali.

Le autorità di regolamentazione dispongono di diversi strumenti per raggiungere questi obiettivi.

In primo luogo, per contrastare gli usi illeciti, ci si può concentrare sulle società che forniscono accesso alle criptovalute. La maggior parte dei consumatori e degli investitori non possiede e non scambia direttamente criptovalute bensì utilizza crypto-wallet o altri intermediari che detengono attività per suo conto. Molti regolamenti in materia potrebbero già riferirsi a questi fornitori di criptoinfrastrutture; allo stesso modo, le norme e i

meccanismi di attuazione esistenti possono essere adattati in modo da rispondere a questioni specifiche. Per esempio, le norme già

esistenti sul riciclaggio di denaro e il finanziamento del terrorismo possono essere estese in diversi casi alle criptovalute. E le leggi e i regolamenti attuali relativi alla tutela dei consumatori e degli investitori possono essere applicati o adattati.

In secondo luogo, le regolamentazioni possono concentrarsi sull'interoperabilità delle criptovalute con entità finanziarie regolamentate, come banche commerciali, società che gestiscono carte di credito e piattaforme di scambio. Queste entità regolamentate permettono a soggetti singoli di convertire valute sovrane in criptovalute e viceversa. È possibile inoltre sviluppare e applicare norme sull'ammissibilità delle criptovalute e dei prodotti ad esse connessi (come derivati o exchange traded fund (ETF)) sulle borse regolamentate.

E i regolamenti possono definire se e in quali modalità le banche sono autorizzate a operare con attività legate alle criptovalute per i loro clienti o per conto proprio e, se la contrattazione è permessa, quali sono le implicazioni a livello fiscale.

In terzo luogo, le autorità possono fornire una definizione più chiara dello status giuridico delle criptovalute. Ciò solleva questioni relative alla tutela dei consumatori (ad esempio, come comportarsi in materia di diritti di proprietà, furto e vendita fraudolenta) e all'uso al dettaglio (ad esempio, definire chi può essere legittimato a scambiare criptovalute e a quali

condizioni). Un altro aspetto chiave relativo allo status giuridico è determinare se le criptovalute devono essere trattate come titoli

– ovvero strumenti negoziabili usati per raccogliere fondi tramite una promessa di pagamento nel futuro – e di conseguenza ricadere nell'ambito di una regolamentazione e di una sorveglianza più stringenti. In alternativa, potrebbero essere considerate come attività generiche (ovvero elementi tangibili o intangibili che è possibile possedere o controllare, come case, materie prime, brevetti), il che significa che possono essere detenute e scambiate, anche su mercati organizzati, senza dover necessariamente sottostare alle rigide norme a cui sono soggetti i mercati mobiliari e sottoporsi alla sorveglianza associatavi.

Il futuro di questa valuta è comunque molto incerto e difficilmente prevedibile, la sua introduzione ha rappresentato un primo passo nella sperimentazione di sistemi monetari alternativi, mettendo anche in discussione le attuali politiche di gestione della moneta.

L'unica certezza è che questa innovazione ha contribuito a sviluppare la tecnologia Blockchain (o altri registri pubblici condivisi), la quale potrebbe rivelarsi come la principale innovazione nel campo dei servizi finanziari dei prossimi anni, visto l'interesse che ha suscitato e gli ingenti investimenti attuati dalle principali istituzioni finanziarie a livello globale.

4. Riferimenti bibliografici

Smith A., *The Wealth of Nations*, 1776

Popper K. R., *La scienza, congetture e confutazioni, in Congetture e Confutazioni, trad. it.*, Bologna, Il Mulino

Wolff K. H., *The Sociology of G. Simmel*, Glencoe, 1950

Comparing of the three great price bubbles on bitcoin - 06/2011, 4/2013, 11/2013 with 2017, consultabile all'indirizzo *http://www.kurzy.cz/zpravy/440516*.

https://www.wired.it/economia/finanza/2018/06/27/shopping-pagamenti-bitcoin-criptovalute/

https://www.wallstreetitalia.com/bitcoin-argentina/

https://coin.dance/volume/localbitcoins/VES

Goodhart C., *Two Concepts of Money*, 1998.

Finley K., *"After 10 Years, Bitcoin Has Changed Everything — And Nothing"*, 31 October 2018.

Wallace B., *"The Rise and Fall of Bitcoin"*, 23 November 2011.

D'Agapeyeff A., *Codes and Ciphers - A History of Cryptography*.

https://www.javaboss.it/crittografia-in-java/?doing_wp_cron=1558462824.8484680652618408203125

https://youtu.be/S9JGmA5_unY

Merkle R. C., *"A Digital Signature Based on a Conventional Encryption Function". Advances in Cryptology, (1988)*

Blockchain, su *www.blockchain.com*

Divine J., *"What's the Best Bitcoin Wallet?", 1 February 2019.*

https://bashco.github.io/

BITMEX RESEARCH, *Bitcoin Economics – Deflationary Debt Spiral.*

Antonopoulos, tdr, 2014, p.176

Social Science Research Network (SSRN), *A History of Bitcoin*.

Bitcoin, ecco perché non è una moneta. (https://www.ilsole24ore.com/art/finanza-e-mercati/2018-01-15/bitcoin-perche-non-e-moneta-vero-valore-blockchain-155334.shtml)

Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System (PDF)*, ottobre 2008, in *www.bitcoin.org*.

An Assessment of Blockchain Consensus Protocols for the Internet of Things., IINTEC 2018

Turing A., *Treatise on the Enigma*.

Bitcoin Charts

Needham, R. M.; Schroeder, M. D., *Using encryption for authentication in large networks of computers*, 1978

Soltas E., *Bitcoin Really Is an Existential Threat to the Modern Liberal State*, in *Bloomberg*.

Paech P., *The Governance of Blockchain Financial Networks*

Houben R; Snyers A., *Cryptocurrencies and blockchain*, University of Antwerp, Research Group Business & Law, Belgium

Blumen R., *Lo spauracchio della spirale deflazionistica, su www.mises.org*

Fr. Bernard W; Dempsey S.J., *Interest and Usury*.

Partington R., *Bitcoin: after 10 wild years, what next for cryptocurrencies?*

Mills B., *What Is Cryptocurrency: 21st-Century Unicorn – Or The Money Of The Future?*

Roubini N., *Why central bank digital currencies will destroy bitcoin*

Bitcoin and Cryptos, the Friendly Mates Most Banks Fear, in *www.medium.com*

Auer R.; Claessens S., *Regolamentazione delle criptovalute: valutazione delle reazioni dei mercati*

Smith A., *The Wealth of Nations*, 1776