UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

BITCOIN: L'EMBLEMA DI UN SISTEMA MONETARIO ALTERNATIVO

RELATORE:

CH.MO PROF. BASSETTI THOMAS

LAUREANDA: MARTELLATO LAURA

MATRICOLA N. 1090216

ANNO ACCADEMICO 2016 – 2017

INDICE

INTRODUZIONE

Il mutamento degli scenari economici ed in particolar modo la recente crisi finanziaria hanno evidenziato negli ultimi decenni la necessità di affiancare alle monete tradizionali altre tipologie di valute, le quali rispondono a sistemi e logiche completamente differenti. Il processo di creazione di valute private e indipendenti da autorità centrali è stato reso possibile grazie alle implementazioni e gli sviluppi nel campo dell'informatica, i quali hanno rappresentato un terreno fertile per idealizzare e sperimentare un nuovo sistema monetario. La crisi del 2007-2008 propagatasi dagli istituti di credito alle finanze pubbliche, già in squilibrio, e i danni arrecati all'economia sia durante lunghi periodi di deflazione che inflazione, hanno spinto molti studiosi a chiedersi se un sistema in cui la moneta sia decentralizzata e quindi non manipolabile, possa essere una soluzione più efficiente sotto il punto di vista della stabilità dei prezzi, della sicurezza dei pagamenti e dei costi degli stessi. A poco meno di dieci anni dalla nascita del protocollo Bitcoin,[1] i dubbi e le speranze rivolti a questa tecnologia sono attuali più che mai, dividendo la letteratura in sostenitori, che vedono il futuro di questa valuta destinata a soppiantare i tradizionali sistemi monetari e i critici, i quali individuano in questo fenomeno una bolla in procinto di scoppiare.

"Bitcoin è una collezione di concetti e tecnologie che formano le basi per un ecosistema di monete digitali" (Antonopoulos, tdr, 2014, p.1), la cui moneta si pone all'interno del contesto economico/sociale odierno come la valuta dell'informazione, dotata delle seguenti caratteristiche: è decentralizzata, non è sostenuta da alcun governo, è resistente alla censura, è a libero accesso, ha costi pressoché trascurabili e non conosce confini geografici. Per comprendere l'impatto di questo fenomeno nello scenario economico globale risulta necessario evidenziarne le dimensioni e le evoluzioni nel tempo. Nel periodo che va dal 2013 al 2017, la capitalizzazione di mercato è passata da 1 milione ad oltre 45 miliardi di dollari USA, con un tasso di cambio iniziale (2010) di $0.50 per BTC. A novembre 2013 il valore della moneta raggiunge i 1.000 dollari USA, per poi crollare in seguito a degli shock e ricominciare la sua ascesa, arrivando a toccare quasi i 3.000 dollari USA a giugno 2017. Sempre nel periodo 2013-2017 il numero di transazioni è aumentato da 20 milioni ad oltre 230 milioni.[2] Secondo le previsioni di Peter Smith, amministratore delegato di Blockchain e Jeremy Liew, primo investitore di Snapchat, "la rete degli utenti crescerà di 61 volte nei

[1] In questo elaborato sono utilizzate due nomenclature, "Bitcoin" (iniziale maiuscola) si riferisce al protocollo e alla tecnologia, mentre "bitcoin" si riferisce all'unità monetaria

[2] Si veda il sito Blockchain Luxembourg (https://blockchain.info/charts, consultato il 14/07/2017)

prossimi tredici anni e nel 2030 rappresenterà il 5% della popolazione mondiale",[3] stimando una capitalizzazione di mercato di 10 trilioni di dollari e un tasso di cambio BTC/USD pari a 500.000. Nonostante le stime possano sembrare ambiziose, i recenti incrementi di utilizzo e notorietà e conseguentemente di valore della valuta, aprono la strada a degli scenari poco prevedibili, che potrebbero determinare il successo o il fallimento di questa tecnologia.

Lo scopo di questo elaborato è quello di mettere in luce le origini, il funzionamento e le principali differenze tra questa criptovaluta e le valute a corso legale. Il primo capitolo ricerca nelle teorie sviluppate da alcuni esponenti della Scuola Austriaca, in particolar modo quelle degli economisti Ludwig von Mises e Friedrich von Hayek, le origini del Bitcoin attraverso lo studio del libero mercato e dell'intervento di enti governativi nella politica monetaria. Il secondo capitolo si concentra su una descrizione dettagliata di questa valuta digitale, dalla nascita del protocollo alla sua evoluzione, analizzando i processi che portano alla sua creazione. Il terzo capitolo, invece, analizza le funzioni della moneta, se il bitcoin le assolve o se è più corretto paragonarlo ad una commodity, in seguito sono messi in luce alcuni aspetti che differenziano questa criptovaluta dalla valute fiat, come la volatilità e la tendenza deflazionistica. Si conclude con alcune riflessioni sul futuro della tecnologia Blockchain, applicabile al sistema bancario e finanziario.

[3]Si veda il sito Business Insider (http://www.businessinsider.com/bitcoin-price-could-be-500000-by-2030-first-snapchat-investor-says-2017-3?IR=T, consultato il 14/07/2017)

Capitolo I
LE TEORIE ALLA BASE DEI SISTEMI VALUTARI CONCORRENZIALI

1.1 La Scuola Austriaca

Nonostante si tratti di un fenomeno apparentemente molto recente, l'idea alla base delle criptovalute non nasce negli anni 2000, bensì ha origini ben più lontane. Molti economisti del secolo scorso infatti, avevano individuato delle falle nei sistemi centralizzati, studiando i problemi derivanti dal controllo diretto dello Stato sull'emissione di moneta. Ludwig von Mises (1881-1973) e Friedrich August von Hayek (1899-1974) furono tra i maggiori esponenti della Scuola Austriaca, una corrente di pensiero che sostenne l'importanza dell'azione umana e delle interazioni tra individui alla base delle leggi economiche e della libertà commerciale, studiando temi come la legge della domanda e dell'offerta, le cause dell'inflazione, il funzionamento dei tassi di cambio e la natura soggettiva del valore economico.

1.2 Il contributo di Ludwig von Mises

Ludwig von Mises fu uno tra gli economisti di maggior rilievo della Scuola Austriaca, sostenitore della libertà economica e del libero mercato, in contrapposizione con gli ideali socialisti e la pianificazione centralizzata. Nel 1912 pubblicò "Theorie des Geldes und der Umlaufsmittel" in cui affrontò numerose tematiche tra cui: natura, definizione e determinazione del valore della moneta, la teoria della domanda e il processo di creazione dell'offerta di moneta e la critica all'intervento pubblico nel sistema monetario, infatti secondo Mises periodi di inflazione e di recessione non sono frutto di fluttuazioni congenite all'economia di mercato.

1.2.1 Lo Stato e la moneta

L'analisi di Mises (1912) parte dall'interrogativo sul motivo per cui lo Stato detenga la sovranità monetaria, se in origine il suo ruolo si limitava alla coniatura per rendere riconoscibile la moneta e assicurare il grado di purezza del metallo al suo interno, nel corso degli anni la sua influenza si è estesa. Anche se è soggetto alla legge di mercato, è in grado di causare forti perturbazioni legate all'influenza che esercita sulla domanda e sull'offerta, poiché è aumentata la sua importanza in quanto agente economico e l'influenza che può esercitare sulla scelta del mezzo di scambio da utilizzare nel commercio, grazie alla sua autorità legislativa. Nonostante ciò, secondo l'autore, il peso delle decisioni di politica

monetaria dello Stato sono sopravvalutate, infatti "solo l'uso commerciale può trasformare un bene in mezzo generale di scambio" (Von Mises, 1912, in Bellofiore, 1999, p.40), ovvero la creazione della moneta è frutto della pratica corrente di tutti gli agenti economici che operano sul mercato e non del potere coercitivo dell'ente governativo.

1.2.2 La politica monetaria

Proseguendo con l'analisi, Mises riconosce allo Stato in cui vige uno standard metallico (tipicamente oro o argento) la possibilità di influenzare il mercato sul tipo di moneta da utilizzare, mentre in uno in cui circola moneta segno, ovvero con valore intrinseco nullo, la possibilità di emettere o ritirare le quantità di contante che desidera, modificandone il valore di scambio oggettivo. La politica monetaria è rappresentata da un insieme di strumenti a capo dello Stato (ad oggi della Banca Centrale Europea), che gli permettono di modificare e indirizzare l'offerta di moneta col fine di raggiungere determinati obiettivi, in particolar modo la stabilità dei prezzi. Per far ciò, si avvale principalmente di due variabili: il tasso d'interesse e la quantità di moneta. Gli esponenti della Scuola Austriaca definiscono l'inflazione come un aumento della massa monetaria in circolazione (e non un aumento generalizzato dei prezzi), la quale fa perdere valore alla moneta e di conseguenza aumentano i prezzi. I vantaggi dichiarati da coloro che sostengono l'inflazione sarebbero: favorire i debitori a dispetto dei creditori, stimolare l'esportazione e svantaggiare l'importazione, incoraggiare la produzione e lo spirito imprenditoriale. Mises confuta queste teorie, in primo luogo affermando che i debitori traggono beneficio dall'inflazione solo nel caso in cui sia imprevista, in caso contrario i creditori cercherebbero di tutelarsi ricorrendo a valute ritenute più stabili o richiedendo tassi d'interesse più alti, in previsione della svalutazione.[4] In secondo luogo, gli agenti economici esteri sono incentivati ad acquistare in un Paese in cui è in corso l'inflazione, per il cambio più favorevole, fintantoché l'aggiustamento non tocca tutte le merci e i servizi, perché il livello assoluto del valore della valuta non ha significato per il commercio estero. Infine riconosce l'efficacia della svalutazione nell'aumento della produzione in casi del passato, ma non all'epoca in cui il capitalismo ha reso depositi bancari e obbligazioni gli strumenti

[4] Questa critica è il linea con le valutazioni esposte nel 1976 dall'economista Robert Lucas, secondo cui un modello econometrico stimato sulla base di dati passati (es. inflazione registrata l'anno precedente) non possa essere utilizzato per predire il comportamento degli agenti a seguito di una nuova politica economica. Un cambiamento di politica economica modifica il modo in cui si formano le aspettative (es. inflazione attesa) e ciò modifica alcuni dei parametri del modello oggetto di studio. Si passò perciò, da un approccio basato sulle aspettative adattive a uno basato sulle aspettative razionali. In un contesto in cui gli agenti economici svolgono un ruolo attivo, la credibilità di una politica monetaria è indispensabile affinché possa essere implementata in modo ottimale. Se le autorità di politica monetaria, come i governi, possono seguire comportamenti discrezionali ed opportunistici, la loro credibilità vacilla. Una soluzione per eliminare questo problema è la delega della politica monetaria ad autorità indipendenti come le Banche Centrali.

principali del risparmio, disincentivando l'accumulazione di capitale e di conseguenza del risparmio. L'inflazione è spesso adottata nei casi in cui un governo necessiti di fondi per scopi pubblici e non voglia aumentare la tassazione, per ragioni principalmente politiche, o accendere un nuovo prestito, i cui effetti sono spesso imprevedibili e indesiderati. Supponendo che un determinato settore benefici dell'emissione della moneta e produca un bene/servizio di cui non c'è richiesta da parte del mercato, ne consegue una distorsione, perché risorse come lavoro e capitale sono state mal assegnate, a cui farà seguito una recessione con lo scopo di correggere le allocazioni inefficienti. Un ulteriore elemento di instabilità del sistema è affrontato da Carbone (2012), il quale individua nel moltiplicatore del coefficiente di riserva (moltiplicatore monetario = 1/tasso di riserva frazionaria) un fattore scatenante, seppur indiretto, di bolle e crisi finanziarie. L'emissione di banconote e di certificati o l'emissione di depositi a vista senza copertura al 100%, generati dalla riserva frazionaria, portano allo stesso risultato perché tutti e tre rappresentano una reale offerta di moneta. Nonostante ciò in Inghilterra nel 1844 la legge Peel, vietò l'emissione di certificati e banconote senza copertura totale, tralasciando i depositi bancari, situazione che ancora oggi nei momenti di contrazione finanziaria, riduce le attività delle banche ad una frazione del valore che assumevano durante l'espansione, le passività restano invariate e il sistema finanziario si riversa in uno stato d'insolvenza. La deflazione invece, rappresenta una riduzione della quantità di moneta in circolazione, a cui segue un apprezzamento del valore e successivamente una riduzione generalizzata dei prezzi. Essa è attuata solitamente dopo un periodo inflativo, non è ben vista dall'opinione generale in quanto mette in luce le distorsioni e gli squilibri creati dall'immissione di moneta nel mercato, gli investimenti meno proficui devono essere iscritti in conto perdite, la bilancia commerciale si deteriora, prezzi e salari necessitano di aggiustamenti verso il basso. Risulta evidente il motivo per cui, in seguito a queste analisi Mises ritenga un sistema in cui lo Stato è in grado di influenzare il valore di scambio della moneta e di conseguenza la distribuzione del reddito, attraverso le politiche monetarie, non compatibile con il capitalismo e il libero mercato. Esso non può governare il mercato ed ogni qualvolta tenti di farlo, incorre in un risultato non prevedibile perché "i mezzi che il potere di influenzare la domanda e l'offerta mette a sua disposizione agiscono sul processo di formazione dei prezzi solo attraverso le valutazioni soggettive degli individui" (Von Mises, 1912, in Bellofiore, 1999, p.161), valutazioni che un monopolista non può captare appieno.

1.3 Il contributo di Friedrich von Hayek

Grande oppositore di Keynes e delle politiche keynesiane, allievo di Ludwig von Mises da cui trasse ispirazione per molte delle sue opere e premio Nobel per l'economia nel 1974, Friedrich August von Hayek studiò e propose un sistema bancario in cui ci fosse competizione fra valute, teoria che è stata sicuramente una buona base di partenza per lo sviluppo dell'idea sottostante la nascita delle criptovalute, e in particolar modo del bitcoin. Nella sua opera "Denationalisation of Money" pubblicata nel 1976, anticipa di trent'anni un sistema monetario, seppur diverso nella forma dal suo, in cui non è lo Stato a detenere il monopolio della moneta ma è la collettività ad averne il controllo indiretto. Egli sostenne il pensiero alla base dell'individualismo metodologico, secondo cui sono le scelte dei singoli, in quanto apportatori di specifiche conoscenze, a determinare un indirizzo di politica economica, si tratta perciò di un approccio più microeconomico.

1.3.1 Il monopolio della moneta

Come il suo maestro, Hayek (1976) inizia la propria analisi chiedendosi il motivo per cui all'interno di un territorio circoscritto debba circolare un unico tipo di valuta (nonostante non si utilizzino più oro e argento come unici mezzi di scambio come nel passato) e conseguentemente perché il monopolio statale dell'emissione di moneta sia collettivamente riconosciuto come indispensabile. Nel corso della storia, dall'epoca dell'Impero romano al Medioevo, la prerogativa statale di emettere moneta coincise con il monopolio di conio, che rappresentò sia una fonte di guadagno che di potere. L'onere che inizialmente si attribuivano i governi era quello di garantire peso e purezza dei materiali attraverso una stampa, rappresentante l'autorità, per poi arrivare al periodo in cui cercarono di ridurre le quantità di oro/argento nelle unità monetarie e giustificarne il valore in quanto emesse dallo Stato e non per la quantità di metallo prezioso contenuto in esse. Fu da allora che il ruolo del governo cambiò, da garante del peso delle monete, a decisore delle quantità e del tipo di valuta da emettere. Le banconote in principio rappresentavano delle ricevute con controvalore in oro o argento, che i cittadini erano obbligati ad accettare, perché rilasciate dall'autorità in deficit di monete metalliche. Con l'affermarsi delle monete nominali, il controllo politico sull'intero sistema è aumentato, determinando un'inefficienza legata al tentativo di avvantaggiare ristretti gruppi d'interesse e non la collettività. Il giudizio secondo cui una moneta metallica sia più stabile di una cartacea è, a parere dell'autore, infondato, perché seppur politicamente difficile, è tecnicamente possibile controllare e conservare il potere d'acquisto della valuta nominale, introducendo una varietà di monete tra loro differenti e tra loro in competizione, la cui scelta e utilizzo è decisa unicamente dal popolo. Ciò che Hayek cerca di mettere in discussione è il

pensiero radicato del privilegio statale sull'emissione di moneta, che ha permesso allo Stato per più di duemila anni di sfruttare e depauperare la collettività, la quale ha subito continui periodi di inflazione (la riduzione di oro all'interno delle monete fa aumentare di conseguenza i prezzi) a solo beneficio dei governi. Nel 1694 il monopolio di emissione della banconote venne conferito dal governo alla Banca d'Inghilterra e da allora il compito delle autorità governative fu quello di assicurare che il potere della coniatura non fosse concesso a banche effettivamente indipendenti. Questo potere fu limitato finché rimase in vigore il sistema monetario aureo (gold standard), il quale obbligò le banche centrali a mantenere delle riserve auree in base alle quantità di moneta in circolazione e garantì una certa stabilità dal 1870 fino alla prima guerra mondiale. Successivamente i governi si resero conto che la convertibilità in oro era solo un modo per controllare la quantità di banconote e quindi il valore delle stesse, motivo per cui cercarono di abolirla. Hayek dedica una parte della sua opera ad analizzare la nozione di corso legale, ovvero la caratteristica di una moneta di non poter essere rifiutata per l'estinzione delle obbligazioni pecuniarie nello Stato in cui essa è emessa. Egli afferma che questo concetto è strettamente legato al monopolio sull'emissione di moneta perché permette allo Stato di decidere quale tipo di moneta debba essere utilizzata per l'estinzione dei debiti, ma ciò non giustifica l'idea secondo cui tutto il denaro dovrebbe essere di corso legale. Il denaro non è frutto dell'invenzione di uno Stato ma la conseguenza naturale di un processo di evoluzione sociale, infatti l'avvocato Lord Farrer (1895) sostenne: "il corso legale sostituisce alla libera azione di un contratto volontario [...] una interpretazione artificiale dei contratti che non sarebbe mai venuta in mente alle parti a meno che non fosse loro imposta da una legge arbitraria" e per questo motivo provoca incertezza nei rapporti commerciali.

1.3.2 Ipotesi di competizione tra banche private

Hayek non si limita solamente ad individuare le inefficienze del sistema monetario, avanza anche un'originale proposta che, a suo dire, è in grado di correggere questo malfunzionamento in corso da decenni. Il modello alla base della sua teoria è il seguente: esistono una serie di istituzioni, o meglio banche, le quali agiscono in concorrenza come in un normale mercato libero, col fine di emettere moneta che incontri la preferenza del pubblico, il quale sceglierà l'alternativa di più semplice utilizzo e che più soddisfi le sue richieste. Il processo avrebbe inizio annunciando al mercato l'emissione di un'unità valutaria con un proprio nome brevettato (es. "ducato") e sancendo l'intenzione di controllare la quantità di moneta in circolazione, in modo da mantenere più costante possibile il suo potere d'acquisto nel tempo. Il pubblico sarebbe inoltre informato del fatto che i "ducati" rimarrebbero in circolazione a patto di mantenere stabile il loro valore reale (con un limitato margine di

deviazione) e la banca si riserverebbe il diritto di modificare la composizione del paniere dei beni che funge come unità di riferimento a seconda delle preferenze della collettività. Nonostante ciò, non sarebbe di alcuna utilità vincolarsi legalmente ad uno standard di valutazione perché "l'esperienza su come il pubblico risponde alle offerte in competizione mostrerebbe, con gradualità, quale combinazione di beni costituisca il paniere più adatto in ogni circostanza e in ogni tempo" (Von Hayek, 1976, in Petroni, 2001, p.42). La concorrenza permetterebbe di raggiungere un livello di efficienza di gran lunga superiore rispetto al monopolio governativo, in quanto le banche sarebbero costrette a mantenere costante il valore delle proprie monete in termini di un determinato paniere di beni per non perdere clienti e di conseguenza uscire dal mercato. La fiducia sottostante a questo modello non differisce di molto da quella su cui poggiano le operazioni delle classiche banche, quest'ultime, infatti, dovrebbero gestire le proprie attività in modo da poter convertire in qualsiasi momento i depositi in liquidità, anche se così non è. In un sistema concorrenziale la fiducia è strettamente correlata con il rischio imprenditoriale, il volume di moneta da immettere in circolazione o da ritirare, non è più uno strumento di manipolazione dei prezzi, ma uno strumento per adattare le quantità ai mutamenti della domanda di moneta; mantenendo costante il valore, la banca soddisfa le aspettative delle persone e di conseguenza la probabilità che si affidino alle valute dei concorrenti si riducono. Si potrebbero assumere come certi i seguenti punti:

1. La domanda di una moneta che ha come obiettivo quello di mantenere più costante possibile il potere d'acquisto, sarà in continua ascesa, purché le persone siano libere di usarla.
2. Questa domanda in continua crescita deriva dalla capacità di una banca di mantenere il valore della moneta stabile, perciò farà in modo di perseguire questo risultato, a differenza di un monopolio che non sostiene alcun rischio se deprezza la sua moneta.
3. La banca di emissione mantiene il valore costante regolando la quantità della propria valuta.
4. Questo controllo della quantità delle varie monete in circolazione rappresenterebbe il migliore tra tutti i metodi per regolare la quantità di tutti i mezzi di scambio.

Gli istituti di emissione sarebbero in concorrenza tra loro sulla qualità delle valute offerte, le quali risponderebbero ai bisogni e alle esigenze delle persone, più di quanto non abbia mai fatto la moneta statale. L'introduzione e l'utilizzo di nuove monete, porterebbe ad una diminuzione della domanda di monete nazionali, se la quantità non fosse immediatamente ridotta, ne conseguirebbe il deprezzamento. Questo processo porterebbe alla scomparsa delle valute meno affidabili e per impedire che la sua non venga più utilizzata, lo Stato dovrebbe

riformare il modo in cui la gestisce, seguendo l'esempio delle banche private. Hayek asserisce inoltre che non esiste inflazione derivante da maggiori costi: né salari più alti, né prezzo del petrolio più alto, possono far aumentare il prezzo aggregato di tutti i beni, a meno che non sia somministrato maggiore denaro agli acquirenti. Si ipotizzi una situazione in cui il governo aumenti i salari o altri costi (prevedendo un successivo aumento della moneta in circolazione) col fine di incrementare la domanda di lavoro. Hayek definisce questo aumento di quantità di moneta "inflazione da costi", deciso dal governo per impedire la disoccupazione derivante dal precedente aumento dei salari o di altri costi, come quello del petrolio. L'aumento dei prezzi e dei salari imposti monopolisticamente (ad esempio da parte dei sindacati) ritarda l'effetto negativo sull'occupazione fintantoché il tasso d'inflazione, necessario a mantenere un determinato livello di occupazione, diventi insostenibile. Questo tipo di manipolazione crea non pochi problemi, nonostante per molti economisti un'inflazione blanda sia perfino benefica. "L'impulso iniziale generale impresso da un aumento della quantità di moneta è principalmente dovuto al fatto che i prezzi, e perciò i profitti, si rivelano superiori alle previsioni. Tutte le imprese hanno successo, comprese quelle che dovrebbero fallire. Ma questo può durare solo finché il continuo aumento dei prezzi non sia generalmente atteso. Una volta che la gente impari a tenerne conto, neanche un incremento continuo dei prezzi al medesimo tasso produrrà lo stesso impulso iniziale" (Von Hayek, 1976, in Petroni, 2001, pp.105-106). A questo punto la politica monetaria può seguire due strade: la prima consiste nell'aumentare il tasso d'inflazione e continuare a farlo ogni qualvolta la collettività incorpori nelle proprie aspettative il tasso d'inflazione corrente oppure può rallentare o fermare questo incremento, facendo sprofondare l'economia in una situazione peggiore di quella precedente. L'inflazione non solo nasconde i normali errori di valutazione, li accumula e indirizza la produzione in attività che senza l'aumento di moneta non sarebbero state intraprese; in altre parole l'inflazione crea un'illusione che non rispecchia la reale condizione dell'economia. È per questo motivo che Hayek rivede nelle politiche monetarie una causa delle depressioni piuttosto che un rimedio, l'origine dell'instabilità dell'economia nel corso dei decenni è riconducibile al fatto che la moneta non sia stata regolata dal mercato, nonostante sia il principale strumento regolatore del meccanismo di mercato. Un monopolista non ha sufficienti informazioni per regolare l'offerta di moneta per perseguire l'interesse generale, mentre una serie di banche in competizione tra loro sì, anche perseguendo obiettivi di profitto. In un libero mercato i prezzi forniscono informazioni necessarie affinché gli individui prendano decisioni e solamente il continuo controllo dei prezzi correnti dei beni permette di indirizzare la loro attività verso settori in cui conviene o no spendere denaro. Il corollario di

queste analisi è la consapevolezza di non avere una buona moneta perché ci si aspetta che lo Stato si comporti come un'entità benevola, ma così non è; per cui l'unica soluzione adottabile per risolvere le inefficienze sarebbe quella di permettere alle banche private di emettere moneta. Per i socialisti il ripresentarsi di periodi depressione e di disoccupazione di massa sono un difetto insito nel capitalismo, in realtà sarebbe l'intervento del governo nell'economia ad aver causato le frequenti crisi del passato e quelle che tuttora si ripresentano. Esso non ha permesso agli istituti di emissione di dotarsi di strumenti che permettessero loro di produrre un profitto per sé e procurare un beneficio all'intera collettività, anzi, il sistema monetario attualmente in vigore è inaffidabile, non rispecchia il libero mercato e arreca danni all'economia, colpendo le fasce di popolazione più deboli. Questa riforma proposta da Hayek di un ordine monetario competitivo, è stata il punto di partenza per lo sviluppo di correnti di cambiamento negli ultimi decenni, di cui si tratterà in seguito.

1.4 Breve confronto tra Scuola Austriaca e teorie mainstream

Le teorie della Scuola Austriaca hanno svolto un ruolo marginale rispetto al più ampio spettro delle teorie economiche mainstream, solitamente ricondotte alla sfera delle teorie neoclassiche congiunte all'approccio keynesiano. Di seguito saranno confrontati alcuni aspetti delle teorie di Mises e Hayek, emersi nei precedenti paragrafi, con le teorie più diffuse ed accettate dal mondo economico. Gli economisti austriaci basano le loro teorie sull'individualismo metodologico, secondo il quale i fenomeni sociali sono frutto delle motivazioni e delle azioni degli individui e studiano come attività e decisioni di milioni di persone e aziende siano coordinate tra loro, infatti le singole decisioni degli individui permettono di ottenere informazioni che altrimenti non emergerebbero. Nel far affiorare ulteriori informazioni, anche sulle parti remote dell'economia all'attenzione dei singoli soggetti decisori, il sistema e i prezzi di mercato funzionano come un vasto sistema informatico e di comunicazione. Essi affermano che curve di domanda, preferenze e tecnologie non siano fruibili ai soggetti decisori e che queste entità emergono all'interno dei processi decisionali. Il lavoro empirico austriaco consiste principalmente in studi di casi storici, la cui unicità limita l'utilità di tale approccio. Gli economisti austriaci criticano l'alto livello di aggregazione necessario per la costruzione dei modelli neoclassici-keynesiani. I principali contenziosi tra le due correnti sono che gli economisti austriaci considerano erronea la dipendenza dalle relazioni tra variabili aggregate delle teorie economiche e affermano che le recessioni sono causate da fattori microeconomici piuttosto che macroeconomici. In secondo luogo sostengono che il modello IS-LM rappresentativo del pensiero di Keynes e formalizzato da Hicks semplifichi in

modo eccessivo gli eventi del mondo reale. Infine si oppongono alle politiche espansionistiche fiscali e monetarie per combattere le recessioni, poiché quello che appare come una temporanea spesa governativa solitamente diventa permanete e continua ad espandersi anche quando l'economia è in ripresa, con una con seguente soppressione del settore privato. Le teorie mainstream invece, cercano di determinare l'equilibrio economico in condizione note. Dal lato microeconomico, date preferenze, tecnologie e numero e varietà di beni, esse studiano una soluzione ben definita per il problema di allocazione delle risorse. Il comportamento dei singoli agenti è definito come il risultato di scelte razionali, utilizzando le azioni a propria disposizione per massimizzare la differenza tra costi e benefici personali e quindi la propria utilità. Dal lato macroeconomico, gli studi si basano su variabili aggregate col fine spiegare l'economia nel suo complesso e di ottenere consigli pratici sulle politiche da intraprendere. Le teorie mainstream infatti, non considerano i modelli matematici come una verità assoluta, ma riconoscono la loro utilità ed affermano che l'astrazione sia necessaria per rappresentare la realtà. Uno dei principali ruoli della politica monetaria è quello di garantire la stabilità dei prezzi e attraverso di essa (insieme alle politiche fiscali) in alcune circostanze è possibile aumentare l'occupazione e la produzione, stimolando la domanda aggregata. Il principale strumento di politica monetaria di una Banca Centrale è il tasso d'interesse a breve termine, determinato sul mercato interbancario, il quale influenza a sua volta il livello dei tassi d'interesse applicati dalle banche a famiglie e imprese. Attraverso l'applicazione della regola di crescita costante della moneta, la Banca Centrale regola i tassi d'interesse a breve in modo che la domanda di moneta produca un tasso di crescita costante della base monetaria. Nel 1960 Friedman affermò che un tasso di crescita costante dell'offerta di moneta assicuri il più alto livello di stabilità raggiungibile, in quanto implica un aumento stabile del reddito nominale complessivo. L'utilizzo di questa politica può risultare scorretto nel momento in cui i parametri della funzione di domanda di moneta cambino nel tempo e in modo imprevedibile, come è avvenuto durante la crisi del 2007-08, l'economista Taylor suggerì che la Banca Centrale dovesse regolare i tassi d'interesse a breve in reazione alle deviazioni osservate della produzione totale rispetto al suo livello potenziale e alle deviazioni del tasso d'interesse reale rispetto al livello obiettivo. I suoi studi hanno rappresentato una buona descrizione delle politiche sui tassi d'interesse attuate dalle banche centrali negli ultimi decenni. Inoltre, è importate ricordare che secondo gli economisti di impostazione neoclassica, nel medio periodo un aumento dello stock nominale di moneta in circolazione fa aumentare la produzione oltre al suo livello naturale, il livello effettivo dei prezzi è maggiore di quello atteso, perciò salari e prezzi aumentano; questo processo di aggiustamento si conclude nel

momento il cui la produzione torna al suo livello naturale e il livello dei prezzi eguaglia il livello atteso. Questa espansione monetaria non ha effetti sulla produzione o sul tasso d'interesse, ma si riflette interamente in un aumento proporzionale del livello dei prezzi, quindi nel medio periodo la moneta è neutrale e le variabili reali non sono influenzabili.

1.5 Le radici del Bitcoin nelle teorie di Mises e Hayek

Le critiche dei due economisti hanno permesso di far affiorare una serie di problematiche ed inefficienze del sistema che altrimenti non sarebbero state messe in discussione. Mises per primo, ha voluto porre l'attenzione sulla questione dell'emissione statale della moneta, che è sempre stata assunta per certa senza sottolineare gli effetti perversi che politiche economiche quali inflazione e deflazione hanno sul sistema economico. Hayek invece, affronta ancora più nel dettaglio queste tematiche ed arriva a proporre un sistema di competizione sull'emissione di moneta da parte delle banche, sistema che oggi come allora potrebbe risultare utopico, perché significherebbe per lo Stato rinunciare ad un importante strumento d'influenza e di potere. Il modello di Hayek risulta estremamente interessante nello studio del concetto di competizione tra valute, piuttosto che al mantenimento dei prezzi stabili da parte di banche in concorrenza tra loro, le criptovalute infatti, sono una serie di monete private che hanno permesso la competizione tra le stesse e le valute fiat. Nonostante le loro lucide analisi, i due economisti non poterono prevedere un sistema basato sull'uso preponderante di Internet e sulla crittografia, infatti sono stati proprio gli sviluppi senza eguali nel campo dell'Information and Communications Technology (ICT) a permettere la nascita delle criptovalute e in particolare del bitcoin. Le teorie di Hayek e Mises rappresentano un buona base di partenza per comprendere la natura del bitcoin, di cui si evidenzieranno le peculiarità nel corso del secondo capitolo.

1.6 Coesistenza tra valute e potere coercitivo dello Stato

È importante sottolineare il fatto che le teorie di Mises e Hayek sono utili per comprendere le motivazioni alla base dell'idea rivoluzionaria sottostante bitcoin, come la creazione di nuove valute decentralizzate e le proposte di modifica del sistema vigente, ma non possono spiegare un sistema in cui circolino già le criptovalute. In un'ottica attuale e futura il modello proposto da Hogan e Luther (2014) analizza i possibili stati realizzabili all'interno del sistema monetario e la capacità dello Stato di persuadere, sotto determinate condizioni, gli individui dall'uso del bitcoin. Dati una serie di agenti economici, suddivisi in diversi tipi quanti sono i beni prodotti, ognuno produce un determinato bene e consuma un sottoinsieme dei beni totali, ogni agente consuma lo stesso numero di beni ma beni diversi tra loro. In aggiunta, esistono

due tipi di moneta, valuta fiat e bitcoin. Al tempo zero una frazione di individui è dotata di valuta fiat, un'altra frazione è dotata di bitcoin e una terza non detiene alcuna ricchezza iniziale. In qualsiasi momento, un agente può decidere con chi negoziare e successivamente se concludere o no lo scambio, a patto che uno dei due agenti detenga ricchezza (valuta fiat o bitcoin) e l'altro nulla. Il modello evidenzia quattro possibili equilibri: il primo equilibrio è un equilibrio in cui la valuta fiat, ma non il bitcoin, è accettata nello scambio. La probabilità che un agente (senza dotazione iniziale di ricchezza) accetti valuta fiat è pari a zero se il valore atteso di detenere moneta fiat è negativo, è pari a 1 se il valore atteso di detenere moneta è positivo, se è pari a zero gli agenti sono indifferenti nell'accettare valuta fiat. Questa probabilità definita all'interno dell'intervallo [0,1] rappresenta la probabilità di soglia per accettare o no la valuta fiat. Il secondo equilibrio è un equilibrio in cui il bitcoin, ma non la valuta fiat, è accettato nello scambio e il procedimento è lo stesso utilizzato nel punto precedente. Il terzo equilibrio è un equilibrio di coesistenza, in cui sia la valuta fiat che il bitcoin sono accettati nello scambio. Il quarto equilibrio è un equilibrio non monetario e si ha nel momento in cui la frazione di agenti disposta ad accettare valuta fiat e la frazione di agenti disposta ad accettare bitcoin è inferiore alle relative probabilità di soglia di accettazione.

Il modello è implementato studiando la capacità dello Stato di prevenire l'uso del bitcoin, in un equilibrio in cui esso circola, perché la coesistenza di valute statali e criptovaluta potrebbero limitare le sue politiche monetarie, ridurre le rendite di signoraggio o favorire delle transazioni illecite. Gli agenti si suddividono ora in agenti privati, i quali accettano bitcoin, e agenti governativi, i quali si rifiutano di accettare bitcoin come mezzo di scambio. Nel caso in cui tutti gli agenti privati accettino bitcoin e nessun agente governativo li accetti, lo Stato è in grado di eliminare un equilibrio in cui i bitcoin circolano se e solo se la frazione di agenti governativi è superiore ad una determinata soglia. Il risultato mostra come lo Stato non sia in grado di precludere l'utilizzo generale del bitcoin come mezzo di scambio semplicemente rifiutandosi di accettarlo, anzi, se una consistente frazione di agenti preferisce la criptovaluta, ha la possibilità di ridurre il potere coercitivo statale non accettando la valuta fiat.

Capitolo II
CARATTERISTICHE E ANALISI DEL BITCOIN

2.1 Cos'è il bitcoin

Il bitcoin è in primis una valuta digitale e decentralizzata. L'innovazione non sta certo nell'intangibilità, in quanto il processo di dematerializzazione delle monete è un fenomeno che prosegue da molti anni e ha visto una progressiva riduzione della moneta cartacea per far posto a quella scritturale (depositi bancari) ed elettronica (carte di credito). Ciò che rende il bitcoin un'innovazione cosiddetta "disruptive" è il fatto che non sia sostenuto da alcun governo, né da alcun intermediario e permette per questo motivo transazioni quasi istantanee. Cambia il paradigma da moneta centralizzata a moneta decentralizzata e che racchiude in sé caratteristiche che possono essere studiate sinergicamente sotto il punto di vista della teoria dei giochi, della crittografia, delle telecomunicazioni e della teoria monetaria. Lo sviluppo della crittografia, cioè le "tecniche di rappresentazione di un messaggio in una forma tale che l'informazione in esso contenuta possa essere recepita solo dal destinatario",[5] già dalla fine degli anni '80 ha reso possibile la nascita di alcune valute private tra cui Liberty Dollar, E-gold, Ecash, Hashcash, B-money, Bit gold, ecc. Le prime due furono sostenute da metalli preziosi e si trattò di due esperimenti fallimentari perché utilizzavano camere di compensazione centrali per gestire le transazioni, come un normale sistema bancario e ciò li ha resi vulnerabili agli attacchi dei governi e degli hacker. Per camera di compensazione si intende un centro di clearing presso il quale si svolgono le attività di compensazione di rapporti di debito e credito. "Quando una banca riceve da parte dei propri correntisti la richiesta di accredito di assegni tratti su una delle altre banche associate, anziché entrare in contatto direttamente con ognuna di esse per l'incasso di ciascun assegno e per tutte le altre conseguenti operazioni che comportino l'effettivo trasferimento della moneta, si rivolge alla stanza di compensazione, alla quale ogni banca invia l'elenco degli assegni a credito tratti sulle altre banche; dalla differenza tra questi e gli assegni a debito verso le altre associate si calcola l'ammontare del dare e dell'avere in quel determinato giorno e solo le differenze eventualmente in essere vengono liquidate dalla stanza di compensazione".[6] Le altre valute invece, sono digitali e seppur più vulnerabili e qualitativamente inferiori, sono veri e propri precursori del bitcoin, il quale ad oggi rappresenta la valuta digitale di riferimento e il cui protocollo ha ispirato la nascita di numerose altre criptovalute. Ciò che accomuna tutte queste monete private, oltre la non-sponsorizzazione da parte del governo, è la caratteristica di non

[5] Definizione da treccani.it
[6] Definizione da treccani.it

essere a corso legale e quindi per poter essere accettate necessitano di essere riconosciute come utili da entrambe le controparti. Il bitcoin, in sunto, combina una serie di innovazioni, infatti si tratta di una valuta virtuale decentralizzata, non controllata da nessuna autorità governativa e da nessuna organizzazione ma nemmeno da singoli individui, che permette di eseguire transazioni peer-to-peer in un breve lasso di tempo, non necessita della fiducia di parti terze, la crittografia lo rende un sistema sicuro e con bassi costi di gestione. I bitcoin svolgono le stesse funzioni delle monete tradizionali, permettono di vendere e comprare beni, inviare denaro e fare credito, possono inoltre essere scambiati contro altre valute su particolari piattaforme di cambio. Si tratta di vere e proprie valute virtuali, perché non esistono monete fisiche né digitali in sé per sé, infatti è la transazione che conferisce valore dal mittente al ricevente ed è dalle transazioni che scaturisce la moneta.

2.2 Nascita del bitcoin e protocollo peer-to-peer

Il bitcoin è apparso per la prima volta nel 2008, quando Satoshi Nakamoto (uno pseudonimo, infatti ancora oggi è ignota l'identità del/i creatore/i) pubblicò un paper scientifico intitolato "Bitcoin: A Peer-to-Peer Electronic Cash System". Egli prese spunto da valute digitali quali Hashcash e b-money per creare un sistema di contante elettronico completamente autonomo, che non dipendesse da alcuna autorità per l'emissione della moneta e la validazione delle transazioni. Nel gennaio 2009 Nakamoto distribuì la prima versione del software e continuò a sviluppare il progetto fino a metà 2010, quando si ritirò dal network Bitcoin. Al momento del rilascio del software, Nakamoto accennò le proprie motivazioni politiche: "Il problema alla base delle valute tradizionali è tutta la fiducia che è necessaria per farle funzionare. Le persone devono fidarsi della Banca Centrale affinché non svaluti la moneta, ma la storia delle valute fiat è piena di violazioni di questa fiducia"[7] e il protocollo Bitcoin emerse come possibile soluzione nel bel mezzo della crisi finanziaria, quando alle ingenti perdite registrate dalla banche, susseguirono i salvataggi delle stesse, con l'aumento del debito pubblico dei Paesi coinvolti, la conseguente crisi del debito sovrano e la grande recessione.

Questa unità monetaria immagazzina e trasmette valore tra gli utenti del network Bitcoin, i quali comunicano tra loro grazie al protocollo Bitcoin quasi esclusivamente attraverso internet. Questo protocollo è facilmente accessibile, è utilizzabile sulla maggior parte dei dispositivi digitali, quali cellulari e computer portatili, ed è disponibile come software free e open source, può perciò essere usato, copiato, modificato e redistribuito dagli utenti. Il punto principale che caratterizza il protocollo Bitcoin è l'esistenza di un registro pubblico delle

[7] Si veda il sito P2P Foundation (p2pfoundation.ning.com/forum/topics/bitcoin-open-source, consultato 1l 15/07/2017)

transazioni (“ledger” in inglese o “libro mastro” in italiano) distribuito e quindi condiviso attraverso la tecnologia peer-to-peer. A differenza delle prime modalità di “file sharing” come per esempio Emule o Napster, le quali prevedevano un server centrale che collegava tra loro i diversi “peer” del network e perciò li ha resi vulnerabili nei confronti delle autorità, protocolli come BitTorrent e successivamente anche Bitcoin, non hanno un server centrale e tutti i nodi della rete sono equivalenti, ovvero sono alla pari degli altri e non c’è alcuna gerarchia client-server. Questo significa che per poter chiudere un tale network, dovrebbero essere spenti tutti i nodi della rete. Tale registro permette il trasferimento di un gettone digitale univoco, il quale non può essere duplicato, caratteristica di fondamentale importanza, data la facilità di duplicazione di qualsiasi tipo di materiale digitale. Inoltre, il registro pubblico tiene traccia di qualunque transazione, nessuna esclusa, motivo per cui è potenzialmente in grado di rimpiazzare qualsiasi autorità centrale, il cui scopo è quello di gestire un registro centrale.

2.3 Chiavi, indirizzi e portafogli

La moneta non esiste fisicamente in sé per sé, ma solo come transazione documentata sul registro pubblico, non è una promessa di pagamento, ma uno strumento al portatore e quindi non ha intrinsecamente rischi di controparte. Un “wallet” o portafoglio è un software che raccoglie i propri indirizzi e le relative chiavi private, e può essere usato per conservare, inviare e ricevere bitcoin. Un indirizzo pubblico è una sequenza alfanumerica (può essere rappresentato anche sotto forma di QR code), assimilabile ad un indirizzo email, che può essere condiviso per ricevere bitcoin sul proprio portafoglio. Ogni indirizzo comincia con il numero 1 o 3 e possono essere creati senza limiti, anzi, è consigliabile utilizzare un diverso indirizzo per ogni transazione che si effettua, per motivi di sicurezza. La funzione del registro pubblico è quella di certificare quanti bitcoin sono associati a ciascun indirizzo e cliccando su di esso, come mostrato in figura 2.1, è possibile risalire all’intera storia di tutte le transazioni avvenute. La tecnologia sottostante è un sistema di crittografia asimmetrica a coppia di chiavi, una pubblica e una privata. Queste chiavi sono collegate tra loro matematicamente e svolgono due funzioni opposte: la chiave privata è segreta e genera una firma digitale, la quale costituisce una prova della transazione e impedisce l’alterazione della stessa. La chiave pubblica invece, è visibile a tutti e può essere utilizzata per verificare l’originalità della firma apposta dalla chiave privata collegata, oltre a mostrare se l’ammontare inviato è effettivamente posseduto dal mittente.

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

Sommario		Le transazioni	
Indirizzo	1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK	Nr. Transazioni	10
Hash 160	7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8	Totale Ricevuto	0.11870887 BTC
Utensili	Tag correlati - Uscite non spesi	consuntivo	0.10320887 BTC

Fig.2.1: https://blockchain.info/address/1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

L'indirizzo di un portafoglio rappresenta la chiave pubblica,[8] mentre la chiave privata è quella che permette di spendere le proprie monete ed entrambe conferiscono la proprietà delle transazioni. Se un utente perde le proprie chiavi private o non crea un backup, perde di conseguenza i propri bitcoin, come una qualsiasi persona che perda il proprio portafoglio con contante all'interno. L'unico modo per poterli spendere è possedere le chiavi, quindi ogni utente ha il totale controllo delle proprie monete, con i vantaggi e i rischi che ne derivano.

2.4 Transazioni

Una transazione è un pagamento da un indirizzo ad un altro, un trasferimento da una chiave pubblica a un'altra e comunica al network che il proprietario ha autorizzato il trasferimento di un ammontare di bitcoin a un altro. Il nuovo proprietario può spendere i bitcoin ricevuti e man mano si crea una catena di passaggi di proprietà. Qualsiasi nodo del network può in modo indipendente verificare attraverso la chiave pubblica del mittente se la disposizione di trasferimento è stata originata da egli stesso e se la transazione è legittima, ovvero se i fondi che vuole trasferire sono effettivamente a sua disposizione. Successivamente un nodo può registrare una determinata transazione in coda al registro pubblico e tutti i nodi della rete sono avvertiti dell'attuazione della transazione e che i bitcoin sono passati dalla chiave pubblica del mittente a quella del ricevente. Una transazione può essere immaginata come una scrittura contabile in partita doppia: gli "input" sono bitcoin ricevuti da transazioni precedenti, mentre gli "output" rappresentano i bitcoin spediti. La somma di queste due voci non andrà a

[8] In realtà l'indirizzo è derivato dalla chiave pubblica, ma per semplicità vengono associati

pareggio perché per ogni operazione si paga una commissione di transazione (c.d. "transaction fee"), la quale rappresenta una ricompensa affinché la transazione venga inclusa nel registro. L'ammontare della commissione solitamente è a discrezione di ciascun utente, tenendo in considerazione che maggiore è l'importo e maggiore sarà la velocità di conferma della transazione.

2.5 Blocchi e Blockchain

Le transazioni non sono iscritte singolarmente nel registro pubblico, vengono bensì raggruppate in blocchi di transazioni, i quali vengono agganciati in coda uno dopo l'altro, dando origine ad una vera e propria catena detta Blockchain, che tiene traccia di tutte le transazioni effettuate, dall'ultimo fino al primo blocco, chiamato "genesis block". Quando una transazione viene inclusa in un blocco, ha una conferma. Nel momento in cui un altro blocco viene validato, la transazione ha due conferme. Sei o più conferme sono considerate una prova sufficiente affinché la transazione non possa essere annullata. Ogni blocco viene validato in media ogni dieci minuti e ciò che permette di collegare in successione i vari blocchi è del lavoro computazionale, che lega due blocchi consecutivi. Maggiore è la quantità di lavoro computazionale utilizzata per unire due blocchi e minore è la possibilità di manomettere il legame tra i due. Questa potenza computazionale è misurata in hash/s (hash al secondo), la quale rappresenta l'operazione base necessaria per la validazione dei blocchi. La funzione di hash (è iniettiva e quindi non reversibile) è un algoritmo per cui un messaggio in entrata (dei dati come una sequenza di lettere di qualsiasi lunghezza) viene convertito in una stringa binaria di lunghezza fissa (chiamata valore di hash o "hash value") in modo da essere criptato. La funzione di hash applicata ad una stessa stringa genera lo stesso hash, mentre una minima modifica al file di partenza (come un'aggiunta di un carattere) genera un hash completamente diverso.[9] Dal dataset di input è possibile ricavare un "hash value", il quale è univoco per quel dato dataset, ma dal valore di hash non è possibile risalire al dataset di input. Bitcoin utilizza una funzione di hash chiamata SHA256 (SHA significa "Secure Hash Algorithm"), perché il suo output è di 256 bit. Ad esempio si potrebbe calcolare lo SHA256 della stringa "Hello, world" e si ottiene come risultato un numero esadecimale (per le prime dieci cifre si usano i numeri da 0 a 9, e per le successive sei cifre si usano le lettere da A alla F, per un totale di 16 simboli), utilizzando gli input a disposizione, è necessario aggiungere pezzi di informazione arbitrari affinché il risultato finale cominci con un determinato numero di zeri. I dati inclusi in un nuovo blocco, comprendono il valore di hash del blocco precedente

[9] Si veda il sito CoinDesk (https://www.coindesk.com/bitcoin-hash-functions-explained, consultato il 18/07/2017)

e le informazioni di tutte le transazioni che devono essere validate, a cui è necessario aggiungere un numero casuale, detto "nonce", graficamente rappresentabile come in figura 2.2, col fine di ottenere un "hash value" con un numero molto alto di zeri iniziali.

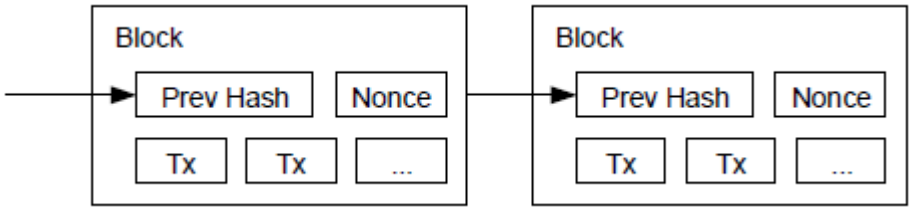

Fig.2.2: Satoshi Nakamoto paper "Bitcoin: A Peer-to-Peer Electronic Cash System"

Questo numero casuale può essere trovato solo procedendo a tentativi e chi lo trova per primo, trova la soluzione, e quindi valida il blocco. Per dare prova di ciò è sufficiente pubblicare il blocco e mostrare alla rete che calcolando il valore di hash con quel determinato "nonce" si ottiene un risultato con il desiderato numero di zeri iniziali, questo processo è definito "Proof-of-Work". I nodi investono in strumenti sempre più potenti per fare in modo di essere i primi a validare i blocchi ed ottenere come ricompensa nuovi bitcoin, infatti la difficoltà del problema è proporzionale al numero di zeri richiesti ed è adattata alla potenza computazionale del network per consentire in media la validazione di un blocco ogni dieci minuti. Il processo che si innesca è il seguente: chi risolve il problema ottiene nuovi bitcoin, si crea concorrenza, la potenza computazionale indispensabile aumenta, il legame tra due blocchi diventa più robusto perché per manipolarlo sarebbe necessario moltissimo lavoro computazionale e più robusta è la catena e più sicuro è il bitcoin, maggiore è il valore della ricompensa che i "miners" ottengono, maggiore sono gli investimenti in hardware e in potenza computazionale, creando una spirale che implementa in modo crescente la sicurezza e il valore del bitcoin stesso. La potenza computazionale della rete Bitcoin dal 2009 al 2017 è cambiata, aumentando esponenzialmente ed è all'incirca centinaia di migliaia di volte più performante dei top 500 computer più potenti al mondo, naturalmente solo nel compiere le operazioni di hashing, si tratta infatti di confrontare hardware altamente specializzato con hardware generico.

2.6 Il mining e il consenso

Alcuni nodi della rete, detti nodi di "mining", forniscono la potenza computazionale necessaria affinché le transazioni siano incluse nei blocchi e validate, inoltre garantiscono la sicurezza del network e sincronizzano tutti i nodi. I "miners" competono tra loro, con

l'obiettivo di trovare la soluzione, la "Proof-of-Work" per essere il nodo che per primo valida un blocco di transazioni, poiché il vincitore di questa competizione è ricompensato con l'emissione e la ricezione di nuovi bitcoin. Qualsiasi utente che partecipa al network Bitcoin può svolgere il ruolo del "miner", utilizzando la potenza di calcolo del proprio computer col fine di validare e registrare le transazioni effettuate. Ciò poteva ritenersi attuabile fintantoché le dimensioni della rete e la difficoltà nell'individuare un nuovo blocco, correlata alla potenza di "hashing" necessaria, fossero sostenibili da singoli computer con una discreta potenza di calcolo. Ad oggi i "miners" collaborano tra loro per formare delle "mining pools", unendo la loro potenza computazionale e dividendo i guadagni tra migliaia di partecipanti. Unire gli sforzi permette di avere guadagni più bassi ma più frequenti, di affrontare minore incertezza e investire in potentissime apparecchiature chiamate "Bitcoin ASIC (Application-Specific Integrated Circuit) Miner", cioè computer progettati specificamente per l'attività di "mining". Le "mining pools" possono essere immaginate come delle società, le quali si concentrano principalmente in Cina, ma sono presenti anche in Paesi quali Islanda, Giappone, Repubblica Ceca e India. Questa localizzazione non è casuale, infatti l'utilizzo di potenti computer costantemente accesi e al lavoro, comporta ingenti costi in termini di energia elettrica e per questo motivo le società si stanziano in Paesi in cui il costo delle corrente elettrica è relativamente basso. Satoshi Nakamoto sfruttò il concetto di rendite di signoraggio per coprire i costi del network, infatti per rendite di signoraggio si intende la ricchezza derivante dal potere di emettere moneta, ad esempio la Banca Centrale stampando una singola banconota dal valore di €500, dati i costi irrisori, ottiene un utile di gran lunga superiore. In un sistema come quello Bitcoin, queste rendite coprono i costi di energia elettrica necessaria, a beneficio dell'intera rete. L'impegnativo lavoro computazionale svolto dai nodi di "mining" è orientato a risolvere un problema informatico, chiamato Problema dei "Generali Bizantini", il quale consiste nel raggiungere un consenso da parte di alcuni generali, i quali devono decidere se assediare o no una città, ma non possono comunicare direttamente tra di loro, ma solo attraverso dei messaggi. Il successo è determinato dalla condivisione della stessa strategia da parte di tutti i generali e la teoria dimostra che con questi presupposti non si possa raggiungere il consenso. Un generale traditore, a cui arrivi il messaggio di non attaccare, propagherà il messaggio contrario e di conseguenza non si è in grado di distinguere tra messaggio onesto o disonesto. Specularmente in un network in cui esiste almeno un nodo malizioso o non affidabile non è possibile raggiungere il consenso, a maggior ragione in un network in cui si trasferisce valore, saranno infatti presenti nodi che attivamente tentano di sabotare il sistema a proprio vantaggio. L'invenzione di Satoshi Nakamoto invece rappresenta

una soluzione a questo problema perché permette di raggiungere il consenso grazie all'incentivo dei nodi di "mining" a comportarsi in modo onesto nonostante perseguano i propri interessi, attraverso la compensazione per la "Proof-of-Work" con l'emissione di nuovi bitcoin. Questo consenso viene definito emergente perché non è raggiunto esplicitamente ma attraverso l'interazione di migliaia di nodi indipendenti e senza l'ausilio di un'autorità centrale, la Blockchain rappresenta infatti il registro autoritativo di proprietà della valuta. Il consenso decentralizzato è raggiunto attraverso una serie di processi che avvengono indipendentemente sui nodi del network come: la verifica di ogni transazione, l'aggregazione delle transazioni in blocchi da parte dei "miners", la verifica degli stessi e la selezione da parte di ogni nodo della catena con il maggior numero di blocchi validati. Questo meccanismo di competizione globale rappresenta l'attuazione di un sistema completamente decentralizzato, in cui non è necessario un ente come una Banca Centrale per emettere valuta.

2.6.1 "Fork" della Blockchain

La struttura decentralizzata dei dati della Blockchain, può portare a delle situazioni in cui nel network sono presenti diverse copie di essa non identiche tra loro. I blocchi possono raggiungere i vari nodi in momenti temporali differenti, questo fa sì che i nodi abbiano diverse prospettive della Blockchain. Per risolvere questo problema, ogni nodo seleziona e cerca di estendere sempre la catena più lunga e con difficoltà computazionale cumulativa più alta. Nel momento in cui tutti i nodi selezionano la catena con difficoltà cumulativa più alta, la rete globale Bitcoin tende a convergere verso uno stato univoco. Le biforcazioni, chiamate "fork", rappresentano delle inconsistenze temporanee tra le varie versioni della Blockchain, le quali sono risolte da eventuali riconvergenze mano a mano che più blocchi sono aggiunti a uno dei rami. Si distinguono tre tipi di blocchi: quelli connessi alla Blockchain principale, quelli che formano rami che partono dalla Blockchain principale, dette catene secondarie, i quali restano validi senza far parte della catena principale. Se la catena secondaria accumula maggiore potenza computazionale, i nodi convergono su di essa, selezionandola come nuova catena principale. Infine, i blocchi che non hanno un genitore presente nelle catene conosciute sono denominati orfani e sono confinati in una "orphan block pool" fintantoché non vengono ricongiunti con i loro blocchi genitori. Nonostante queste possibili discrepanze temporali, risolvibili aumentando la "Proof-of-Work", tutti i nodi riescono a raggiungere un consenso condiviso dall'intero network.

2.6.2 Possibili attacchi al consenso

Un rischio in cui incorre, in via teorica, il meccanismo del consenso è un attacco da parte di più "miners", il cui scopo è quello di dirottare o distruggere il protocollo Bitcoin, con l'acquisizione di una potenza computazionale maggiore di quella dell'intero network. Qualsiasi tipo di attacco al consenso è comunque limitato al consenso futuro perché il registro pubblico diventa sempre più immutabile man mano che il tempo passa. Per riuscire a modificare la catena in profondità sarebbe necessaria un'enorme potenza computazionale, e in aggiunta, un attacco non può rubare, dirottare o cambiare la proprietà dei bitcoin, ma solamente colpire i blocchi più recenti e causare problemi legati alla creazione di nuovi blocchi. Un'ipotesi di attacco è il cosiddetto "attacco al 51%" in cui un gruppo di "miners", controllando più di metà del potere computazionale dell'intero network, colludono per attaccare la rete Bitcoin. Questo tipo di attacco avrebbe come scopo principale quello di distruggere il sistema, creando delle biforcazioni deliberate e la doppia spesa di alcune transazioni (utilizzabile solo per le transazioni degli stessi "miners" corrotti), per questo motivo un attacco con scopi di profitto risulterebbe svantaggioso, rispetto ad un utilizzo della potenza computazionale in modo onesto per l'attività di "mining". Nonostante il nome, è sufficiente una percentuale inferiore rispetto al 51% della potenza computazionale per attuare un attacco alla rete, è chiamato così perché con tale maggioranza un attacco è destinato ad andare certamente a buon fine.

2.7 Le proprietà del bitcoin

A differenza delle valute tradizionali il bitcoin può essere frazionato oltre la seconda cifra dopo la virgola fino a 1/100.000.000 di bitcoin, che è anche conosciuto come un "satoshi". Una caratteristica solitamente attribuita al bitcoin è quella dell'anonimato, un indirizzo (una chiave pubblica) può essere immaginato come un codice IBAN, il quale rappresenta un identificativo ma non comunica nulla del proprietario. Data la trasparenza delle transazioni nel registro pubblico, visibili a tutti e per sempre, è più corretto definire questa peculiarità come "pseudo anonimato".

Come precedentemente evidenziato, circa ogni dieci minuti un blocco viene validato e questo intervallo di tempo definisce la politica monetaria di Bitcoin. L'emissione di bitcoin è frutto della remunerazione di ogni blocco e in origine, nel 2009 venivano emessi 50 bitcoin ogni dieci minuti (nel 2017 sono 12,5 ogni dieci minuti). L'offerta di bitcoin è programmata e deterministica, ciò significa che il protocollo limita l'emissione e, circa ogni quattro anni, i bitcoin creati ad ogni validazione dei blocchi si dimezzano. Il numero massimo di unità

monetarie in circolazione sarà di 21 milioni e graficamente ciò è rappresentabile come una curva che tende asintoticamente a questo limite, che sarà raggiunto approssimativamente nell'anno 2140, come si evince in figura 2.3.

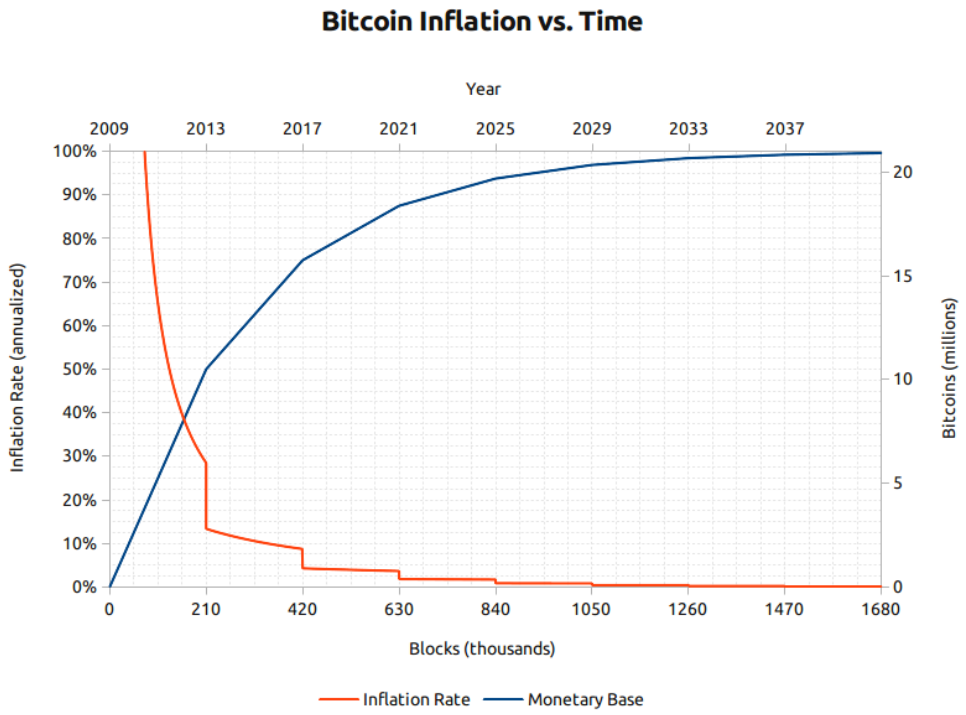

Fig.2.3: btctheory.com/2014/11/19/bitcoin-as-a-commodity-money

Questa politica monetaria imita idealmente la scarsità di un bene prezioso come l'oro, infatti i "miners" rappresenterebbero dei minatori, che svolgono l'attività di minare, scavare per trovare l'oro, la cui quantità è naturalmente limitata, motivo per cui questa valuta viene chiamata anche "digital gold". In un'ottica di lungo periodo emerge la natura deflazionaria del bitcoin, dato il tasso di emissione decrescente e l'offerta inelastica nel corso degli anni, non può subire svalutazioni derivanti dall'inflazione. Per moneta deflazionaria si intende l'apprezzamento del valore e del valore di scambio, frutto dello scostamento tra domanda e offerta, perciò la moneta aumenta la potenza d'acquisto nel corso del tempo.

2.8 Gli scandali e il crollo del prezzo

L'andamento del prezzo del bitcoin risulta uno strumento molto utile nell'analisi di questa valuta. Partendo da un valore di $1 nell'aprile 2011, ha subito numerosi apprezzamenti e deprezzamenti negli anni, raggiungendo quasi la soglia dei $3.000 a giugno 2017. Di seguito sono riportati tre avvenimenti che hanno causato importanti crolli nel prezzo e le relative conseguenze. Nell'ottobre 2013 fu arrestato Ross William Ulbricht, creatore del sito Silk

Road, un mercato del deep web in cui circolavano beni illegali quali droga e armi. L'acquisto della merce illegale in questo sito e in quelli creati successivamente, avveniva attraverso l'uso dei bitcoin, quale strumento non controllabile dalle forze dell'ordine. Nel dicembre 2013 "People's Bank of China", la Banca Centrale della Repubblica Popolare Cinese, vietò alle istituzioni finanziarie di comprare, vendere e detenere bitcoin perché rappresentava una commodity virtuale e non una vera e propria valuta.[10] Questo annuncio ebbe un profondo impatto poiché la Cina rappresentava il maggiore mercato di cambio del bitcoin (quasi l'80% delle transazioni) e nel gennaio 2014 Alibaba, il più grande online retailer del Paese, eliminò i prezzi in bitcoin. Nel febbraio 2014 Mt. Gox, la principale piattaforma di exchange USD/BTC, fallì e sparirono tutti i dollari e i bitcoin detenuti per conto dei clienti. Nel corso degli otto anni dalla sua creazione, questa criptovaluta senza l'appoggio di alcun governo, nonostante abbia perso il suo principale mercato (Cina), la sua principale istituzione finanziaria di riferimento (Mt. Gox) ed abbia la cattiva reputazione di moneta usata nei mercati illeciti, è ancora viva e performante. Per questa sua caratteristica di apparire inarrestabile ed inscalfibile, il bitcoin è definito resiliente.

2.9 L'utilizzo del bitcoin per scopi illeciti

In un report pubblicato nel 2016 dall'Europol, l'agenzia finalizzata alla lotta al crimine dell'Unione Europea, si evince quanto segue: "Le fonti di finanziamento dei terroristi all'interno dell'Unione Europea sono per lo più sconosciute. [...] Non c'è comunque evidenza dell'esistenza di network che finanzino l'ISIS. Nonostante le dichiarazioni di terze parti suggeriscano l'uso di valute anonime come bitcoin da parte dei terroristi per finanziare le loro attività, ciò non è stato confermato dalle forze dell'ordine" (Europol, 2015, p.7). In un ulteriore documento pubblicato dal ministero del tesoro del Regno Unito nel 2015 sul rischio nazionale di riciclaggio del denaro è possibile leggere: "Il rischio di riciclaggio del denaro associato alle valute digitali è basso, tuttavia se l'utilizzo delle valute digitali nel Paese dovesse aumentare, questo rischio potrebbe aumentare" (HM Treasury, 2015, p.79). Le informazioni ad oggi disponibili suggeriscono perciò una bassa, se non nulla, correlazione tra criptovalute da un lato e terrorismo e riciclaggio di denaro dall'altro, per cui prevale l'utilizzo del denaro contante. È importante sottolineare però che una maggiore diffusione del bitcoin, porterà ad un suo maggiore utilizzo anche per scopi criminosi, come qualsiasi altro mezzo di circolazione largamente diffuso ed accettato. Un problema apparentemente intrinseco alla natura delle criptovalute, è quello legato ai "cryptolockers", dei ransomware, o meglio, dei

[10] Si veda il sito The New York Times (http://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-using-bitcoin.html, consultato il 21/07/2017)

virus che bloccano l'accesso dei dati personali ai proprietari, criptandoli e chiedendo un riscatto per poterli decriptare. Due esempi di seri attacchi che sono stati propagati nel 2017 sono "WannaCry" e "Petya", per i quali è stato chiesto un riscatto in bitcoin, data la velocità e la bassa tracciabilità delle transazioni.[11]

2.10 Legislazione e Bitcoin

A livello legislativo le autorità centrali e di regolamentazione di tutto il mondo non hanno assunto una netta posizione nei confronti delle criptovalute, infatti l'approccio finora intrapreso sembrerebbe prudente e limitato a dei controlli normativi. I principali Paesi in cui bitcoin risulta legale sono: Stati Uniti, Canada, Australia ed Unione Europea. Negli Stati Uniti data la diffusa accettazione, sono stati istituite agenzie per prevenire l'utilizzo di bitcoin per scopi illeciti e dal 2013 è in atto un piano governativo per far conoscere questo strumento alla popolazione. In Canada l'agenzia federale per la tassazione classifica il bitcoin come "merce" e gli scambi devono essere registrati al Financial Transactions and Reports Analysis Centre, con lo scopo di controllare e segnalare eventuali operazioni sospette. In Australia, la tassazione sulla criptovaluta varia in base all'utilizzo che ne fanno gli utenti e all'interno dell'Unione Europea, le posizioni dei vari Paesi membri variano, seppur in linea di massima tutte permissive. Alcuni Paesi in cui l'utilizzo del bitcoin è proibito o con delle restrizioni sono: Bolivia, Ecuador, Vietnam, India, Russia e Cina. I primi due proibiscono l'utilizzo del bitcoin, il quale è stato decretato come illegale, mentre in Vietnam solamente le istituzioni finanziarie non possono effettuare transazioni in bitcoin. La posizione dell'India è ufficialmente contro l'uso della criptovaluta, senza aver però mai emanato leggi che la bandiscano. La Russia sembrerebbe in attesa di una legge che vieti le transazioni in bitcoin, ed infine, in Cina questa legge è valida per tutti gli istituti finanziari, comprese le banche, ma i singoli individui possono detenere criptomoneta.[12] In una relazione pubblicata nel 2015 dalla Banca Centrale Europea il fenomeno delle criptovalute viene descritto come un "sistema di moneta virtuale", in cui il bitcoin non possiede tutte le caratteristiche e i connotati giuridici necessari per poterlo definire moneta ed evidenzia tra i principali svantaggi: la ridotta base di accettazione sociale, la mancanza di trasparenza, l'elevata volatilità e l'assenza di garanzie giuridiche e controllo che ne disciplinino l'uso. Sotto il profilo della struttura funzionale come mezzo di pagamento la BCE afferma: "Alcuni elementi dello schema tecnologico dei sistemi

[11] Si veda il sito TheGuardian (https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20, consultato il 26/07/2017)
[12] Si veda il sito BitLegal (http://map.bitlegal.io, consultato il 26/07/2017)

di moneta virtuale potrebbero servire come ispirazione o persino come base, per i provider di pagamento tradizionali per offrire soluzioni innovative di pagamento".

2.11 Valute alternative

Nonostante bitcoin sia quella più diffusa e conosciuta (incide per il 40% sul mercato delle criptovalute), non è la sola criptomoneta in circolazione. La sua tecnologia rivoluzionaria, attraverso il meccanismo di consenso decentralizzato basato sulla "Proof-of-Work" ha aperto la strada a numerose innovazioni in diversi campi: valute, servizi finanziari, sistemi distribuiti e contratti. Le monete alternative, chiamate "alt coins", sono valute digitali create utilizzando lo stesso protocollo Bitcoin, ma con una Blockchain e una rete completamente diverse. Nonostante il numero totale si aggiri intorno al centinaio, le più conosciute e utilizzate sono: Litecoin, Peercoin, Ethereum, Ripple e Zcash. Litecoin è apparsa come la prima vera alternativa al bitcoin e nonostante non sia stata in grado di mantenere una posizione dominante, ad oggi rappresenta la seconda valuta più accettata ed utilizzata nei siti che accettano pagamenti con moneta virtuale. Ethereum invece, è la seconda criptovaluta per capitalizzazione (20 miliardi di dollari USA) e si è affermata come alternativa al Bitcoin all'inizio del 2016. La sua particolarità è legata al fatto che la Blockchain permette di eseguire delle applicazioni decentralizzate e quindi possono essere eseguiti diversi tipi di transazioni, a condizione che sia possibile codificarle all'interno della Blockchain stessa. Questi smart contracts facilitano, verificano o rinforzano la negoziazione o l'esecuzione di un contratto, oppure superano la necessità di una clausola contrattuale, avvalendosi di Ether, l'unità valutaria di Ethereum. In questo modo una serie di clausole contrattuali possono essere rese parzialmente o interamente automatizzate, eseguibili automaticamente, o entrambe le cose. Se il protocollo Bitcoin si propone come alternativa al sistema monetario esistente, il protocollo Ethereum si propone come alternativa decentrata al più generale sistema economico e sociale.

Capitolo III
DIFFERENZE SOSTANZIALI TRA BITCOIN E VALUTE FIAT

3.1 Le funzioni della moneta

La moneta, a differenza di un sistema basato sul baratto, assolve al problema della coincidenza dei bisogni, inoltre per poter essere classificato come moneta, uno strumento deve svolgere almeno tre funzioni:

1. Mezzo di pagamento: caratteristica intrinseca di un mezzo di poter essere scambiato in modo affidabile con qualcos'altro, eliminando le inefficienze di un'economia basata sul baratto.

Il bitcoin è uno strumento che permette di realizzare facilmente la vendita, l'acquisto e lo scambio di beni e servizi tra diversi soggetti, ma non gode di una base di utilizzatori sufficientemente ampia per poter figurare come vero e proprio mezzo di pagamento. Un motivo che dovrebbe spingere i commercianti ad usare questa criptovaluta sono i costi delle commissioni per ogni transazione, in media più bassi rispetto a qualsiasi altro sistema di pagamento (es. carte di credito). Nonostante ciò, le commissioni marginali si sono alzate di molto nell'ultimo anno, rendendo le microtransazioni impraticabili. L'aumento dell'utilizzo di Bitcoin e quindi del numero di transazioni, non è stato accompagnato da un aumento delle dimensioni dei blocchi (limite a 1 Megabyte), si tratta perciò di un punto su cui gli sviluppatori del software stanno lavorando. A causa del limite di dati per blocco, non solo sono aumentate le commissioni, ma sono stati causati ritardi nelle validazioni delle transazioni, passando da una media di dieci minuti a una media di un'ora.[13] È necessario sottolineare due svantaggi riguardo l'accettazione dei bitcoin come mezzo di pagamento: il primo è legato al tempo, infatti anche un'attesa di soli dieci minuti, rappresenta un rischio, seppur minimo, di non vedere una transazione andare a buon fine, mentre il secondo è legato all'elevata volatilità del prezzo. Ad oggi, chiunque usi criptovalute come mezzo di pagamento, converte nel giro di poco tempo i propri bitcoin in valuta fiat, con il fine di minimizzare il rischio legato alla volatilità del prezzo, specialmente i deprezzamenti. All'aumentare della base di accettazione, la volatilità dovrebbe diminuire, come i dati confermerebbero all'apparenza,[14] infatti nel corso degli anni le aziende che hanno permesso ai clienti di acquistare i propri beni/servizi in bitcoin sono aumentate e tra le più importanti

[13] Si veda il sito Blockchain Luxemburg (https://blockchain.info/charts/avg-confirmation-time, consultato il 04/08/2017)
[14] Si veda il sito Bitcoin Volatility Index (https://bitvol.info, consultato il 04/08/2017)

compaiono: Microsoft, Wikipedia, Dell, Expedia e Virgin Galactic.[15] Queste aziende, comunque, non accettano i bitcoin direttamente e si avvalgono di intermediari (es. Coinbase) che si occupano di convertire i bitcoin spesi dai clienti in dollari USA e accreditare l'ammontare in valuta fiat alle aziende. Nel momento in cui si ridurrà la volatilità e il problema del limite delle dimensioni dei blocchi sarà sistemato, il bitcoin potrà essere classificato come mezzo di pagamento a tutti gli effetti.

2. Unità di conto: beni e servizi sono valutati in termini di moneta. La moneta è l'unità di misura del valore e per questo dovrebbe essere stabile, in modo da poter garantire una valutazione stabile dei prezzi, fungibile, facilmente trasportabile, divisibile, riconoscibile e resistente alla contraffazione.

Ad oggi il ruolo del bitcoin come unità di conto dipende quasi esclusivamente dalla sua funzione di mezzo di pagamento e ciò è dovuto all'eccesso di volatilità, come precedentemente discusso. Ipotizzando il raggiungimento di una volatilità pari a quella delle altre valute fiat, potrebbe essere utilizzato senza alcun problema come unità di conto in tutti i Paesi. È divisibile, dato che può essere suddiviso fino ad otto cifre dopo la virgola, ma non è completamente fungibile, infatti non è facilmente sostituibile con altri beni che svolgono la medesima funzione economica. Inoltre è possibile che si verifichi una frammentazione dei prezzi tra diverse piattaforme di cambio e ciò viola la legge del prezzo perché le differenze tra prezzi creano delle opportunità di arbitraggio.

3. Riserva di valore: uno strumento può essere risparmiato in modo sicuro e deve conservare il suo valore nel corso del tempo. Non deve essere deperibile e i costi di conservazione devono essere bassi.

Per poter mantenere la sua riserva di valore, il bitcoin deve fare affidamento sull'aspettativa che gli altri siano disposti ad accettarlo in futuro. Avendo valore intrinseco nullo, il suo valore dipende dalla disponibilità degli altri di continuare ad usarlo. Come l'oro, ha una quantità limitata, è facilmente trasportabile, divisibile e non è contraffabile. Gode dei vantaggi del "first-mover", tra cui la popolarità, gli investimenti attuati e la fiducia, in quanto si è affermato come prima criptovaluta in circolazione. Nonostante oggi siano presenti un centinaio di criptovalute alternative, nessuna è ancora riuscita a prevalere sul bitcoin. Se la collettività ha delle prospettive positive nei confronti del protocollo Bitcoin, è possibile che in futuro possa svolgere la funzione di riserva di valore, ma al momento non gode di una stabilità sufficiente per poter assolvere questo compito.

[15] Si veda il sito ZeroHedge (http://www.zerohedge.com/news/2017-05-28/who-accepts-bitcoins-payment-list-companies-stores-shops, consultato il 04/08/2017)

3.2 Moneta oppure oro digitale

In base alle riflessioni appena riportate, il bitcoin difficilmente può essere ricondotto ad una moneta vera e propria, quanto piuttosto ad una commodity, come l'oro. Secondo il Morgan Stanley commodity Book: "Le commodity sono materie prime, ma più in generale si tratta di materiali destinati alla creazione di altri prodotti. Spesso le commodity sono dei beni fisici, ma non sempre è così: tra quelle meno tangibili si ricordano l'energia elettrica e le emissioni di carbonio. Le commodity negoziabili possono offrire agli investitori opportunità interessanti e diversificate. [...] Investendo in prodotti strutturati come le note e i certificati, gli investitori possono beneficiare dei movimenti dei prezzi delle commodity senza bisogno di doverle possedere fisicamente" (2007, p.1). Buona parte degli utilizzatori di bitcoin sfruttano la sua volatilità per ottenere guadagni dalla speculazione finanziaria, a differenza delle altre valute fiat, per cui le possibilità di arbitraggio sono nettamente inferiori. L'oro è stato fin dall'antichità adottato da tutte le civiltà come primo mezzo di pagamento perché possiede caratteristiche quali la scarsità, la lucentezza, la malleabilità ed è relativamente facile verificarne la purezza. Anche se successivamente il potere di coniatura è stato attribuito alle autorità locali, inizialmente la sua adozione è avvenuta senza una pianificazione centralizzata, situazione speculare a quella del bitcoin oggi, per cui un numero sempre maggiore di persone rivede un'utilità in questo strumento e quindi lo adotta di propria spontanea volontà. Come l'oro è stato per anni la miglior forma di moneta, da cui sono scaturiti tutti i sistemi monetari conosciuti più avanzati, senza però renderlo obsoleto; così oggi il bitcoin rappresenta la migliore criptomoneta in circolazione, che ha innescato la nascita di nuovi sistemi monetari e potrebbe essere sorpassato da criptovalute alternative, senza diventare necessariamente obsoleto.

3.3 Volatilità

La volatilità descrive la variazione nel tempo di un prezzo di cambio, e maggiore è la variazione di prezzo, tanto più ampia è la volatilità, a cui è associato un maggiore rischio. Essa rappresenta, come è stato evidenziato precedentemente, il più grande ostacolo del bitcoin per poter essere utilizzato come moneta. In un'analisi comparativa[16] effettuata da Baur e Dimpfl, sintetizzata in figura 3.1, si evince che la volatilità del bitcoin è di gran lunga superiore alla volatilità del tasso di cambio USD/EUR. I dati mostrano che la volatilità giornaliera del bitcoin è normalmente intorno al 10% (a luglio 2017 si attesta intorno al 5%), con picchi occasionali che possono arrivare al 30% contro lo 0,05% di quella del tasso di cambio

[16] Serie storiche di dati raccolti da gennaio 2014 a gennaio 2017

USD/EUR. Ciò significa che in caso d'acquisto di un bene dal valore di 1.000 dollari USA, il costo può variare in eccesso o in difetto di 100 dollari in un breve lasso di tempo.

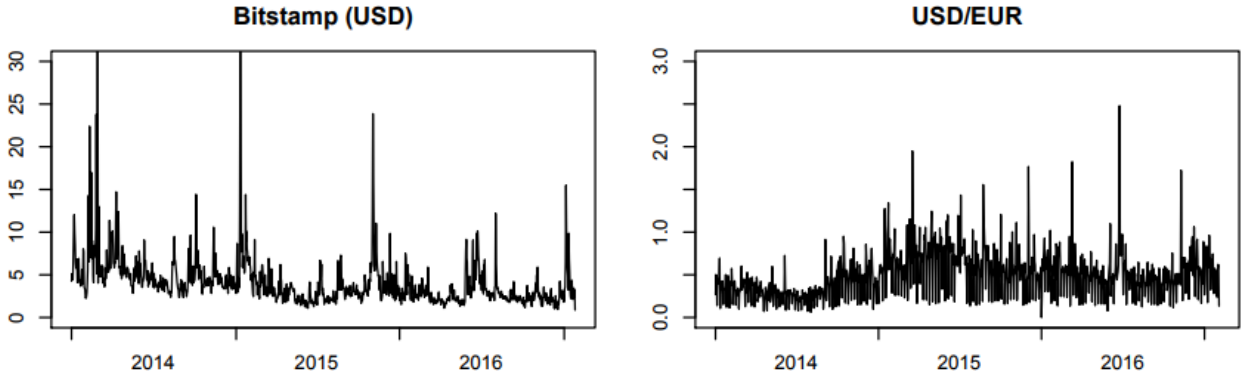

Fig.3.1: Baur e Dimpf paper "Realized Bitcoin Volatility"

Data la bassa capitalizzazione di mercato (45 miliardi di dollari USA), il prezzo del bitcoin è vulnerabile a consistenti ordini di acquisto o vendita e data la corrente natura speculativa, la volatilità del prezzo è per lo più influenzata da eventi esterni. Una serie di eventi negativi (es. un annuncio di default di una delle maggiori piattaforme di scambio) o positivi (es. legalizzazione come mezzo di pagamento da parte di uno Stato) possono innescare negli investitori reazioni di vendita o acquisto di massa. Le fluttuazioni sono causate principalmente da interventi improvvisi quali: la regolamentazione da parte di un governo, le violazioni sulla sicurezza di portafogli detenuti da aziende che offrono servizi di deposito o deprezzamenti di valute fiat. Un evento interno che riduce la volatilità, è la politica di dimezzamento dei bitcoin emessi, infatti all'aumentare del volume di quelli in circolazione nel corso del tempo, la volatilità ha subito un trend verso il basso.

3.3.1 Rischio bolla speculativa

La situazione in cui riversa il bitcoin è di un'apparente bolla, anche graficamente l'andamento del prezzo assume una forma parabolica, indice di una possibile euforia del mercato, la quale non giustifica il livello dei prezzi raggiunti. Di seguito saranno analizzate le possibili cause, che hanno portato ad un aumento della domanda e di un, forse eccessivo, ottimismo sul futuro della criptovaluta. Secondo Garrick Hileman, esperto in Bitcoin al "Cambridge Centre for Alternative Finance": "Ad oggi ci sono delle evidenze che il principale uso delle criptovalute è quello speculativo. [...] I volumi globali di trading del bitcoin sono stati significativamente più alti rispetto ai volumi di transazioni all'interno del network" (2017, p.26), quindi la

maggior parte degli utenti compra e vende per motivi volti al conseguimento di un profitto, piuttosto che per comprare beni/servizi e inviare denaro ad altri utenti. Uno dei fattori che ha spinto la domanda verso l'alto è la legalizzazione del bitcoin da parte del governo giapponese nell'aprile 2017, in quanto il Giappone rappresenta una tra le maggiori potenze economiche in Asia. Un secondo fattore che potrebbe aver incrementato l'attenzione pubblica nei confronti del bitcoin, è legata alla propagazione di alcuni ransomware, di cui si è discusso precedentemente. Gli autori di questi virus chiedono riscatti in bitcoin e nonostante ciò non produca un'immagine positiva nei loro confronti, la maggiore attenzione rivolta al tema da parte dei media può aver fatto crescere la domanda, portando molti utenti ad informarsi a riguardo ed acquistare la criptovaluta. Questi eventi hanno contribuito al generale incremento di domanda di bitcoin, la quale è stata guidata da motivi speculativi, piuttosto che da un incremento nell'uso pratico della valuta. Sempre più utenti sono convinti di un aumento del prezzo nel lungo periodo e ciò può aver innescato delle aspettative che si autoavverano, definite per la prima volta da Merton (1948). In un mercato finanziario per aspettative che si autoavverano si intende un comportamento sociale per cui una convinzione (o una profezia) si verifica per il solo fatto che è stata espressa ed è proprio il/la timore/sicurezza che si avveri che contribuisce alla sua realizzazione. Se il bitcoin dovesse diventare di fatto un mezzo di pagamento utilizzato in tutto il mondo, è possibile che queste aspettative ottimistiche non siano sbagliate. Se invece i recenti aumenti del prezzo dovessero rivelarsi una mera bolla speculativa, ad un certo punto si innescherà il processo opposto, causando panico ed una conseguente vendita di massa e diminuzione del prezzo.

3.4 Spirale deflazionistica

Un'ulteriore peculiarità che contraddistingue il bitcoin dalle valute tradizionali è la sua natura deflazionaria, infatti un'offerta fissa e in diminuzione nel tempo, determina un sistema monetario resistente all'inflazione. In un periodo di deflazione rapida, gli individui e le imprese tendono rimandare spese ed investimenti, sperando in una futura caduta dei prezzi. Di seguito saranno analizzate due posizioni contrastanti tra loro, da un lato chi sostiene l'efficienza e dall'altro chi evidenzia le problematiche che tale sistema comporterebbe. I maggiori esperti di bitcoin affermano che la deflazione non è in sé per sé un effetto negativo, perché quella più studiata, è normalmente associata a un collasso della domanda. In Paese in cui vige valuta fiat ed è possibile emetterla pressoché discrezionalmente, è difficile entrare in una spirale deflazionistica a meno che non ci sia un completo collasso della domanda e non

sia stampata nuova moneta a sufficienza.[17] La deflazione in Bitcoin invece, non è causata da un collasso della domanda ma da un'offerta di moneta sempre prevedibile. L'istinto di risparmiare moneta causato da una valuta deflazionaria "potrebbe essere superato tramite l'applicazione di sconti da parte dei venditori, fino a che lo sconto superi l'istinto di accumulare moneta del compratore. Dato che il venditore è anch'egli motivato ad accumulare, lo sconto diviene il prezzo d'equilibrio al quale i due istinti di accumulo combaciano. Con sconti del 30% sul prezzo in bitcoin, molti venditori non hanno difficoltà contro l'istinto di accumulare e generare guadagni" (Antonopoulos, tdr, 2014, p.176). Altri economisti invece, ritengono che un'economia deflazionistica dovrebbe essere evitata, specialmente se associata ad una bassa crescita e un'elevata incertezza del ciclo economico. Il processo deflazionistico del bitcoin potrebbe essere innescato da una mancanza di liquidità, dovuta ad un aumento della domanda ad una velocità superiore a quella necessaria per emettere nuove criptomonete attraverso il "mining". Questo processo porterebbe sia ad un aumento del valore del bitcoin, che ad una diminuzione dei prezzi di beni e servizi. Quest'ultima causerebbe una riduzione della produzione e dei salari, con una diminuzione della domanda di beni/servizi e dei prezzi a loro volta, provocando un circolo vizioso il cui risultato finale sono disoccupazione e distruzione della ricchezza. Ciò potrebbe portare all'abbandono dell'uso del bitcoin a causa del panico generatosi nel mercato. Dati questi presupposti e osservando la situazione odierna, i bitcoin sono utilizzati più come un investimento piuttosto che come mezzo di pagamento, già nel 2013 un terzo dei bitcoin era detenuto da investitori, i quali li acquisivano ma non li utilizzavano per effettuare transazioni.

3.4.1 Ipotesi di offerta elastica

L'instabilità dei prezzi dovuta all'offerta inelastica di bitcoin, potrebbe essere risolta introducendo una modifica al protocollo che renda l'offerta elastica. La deflazione crea instabilità nei prezzi ed aggrava il problema della volatilità, allontanando questo sistema monetario da quello proposto da Hayek sulla concorrenza tra valute, il cui primo obiettivo era quello della stabilità dei prezzi. La soluzione proposta da Ametrano in "Hayek Money: the Cryptocurrency Price Stability Solution" consiste nell'emettere un cospicuo ammontare di valuta, la quale si adatta elasticamente e in modo non discrezionale ai cambiamenti della domanda, attraverso un algoritmo completamente automatico. Un modello simile risolverebbe gli effetti negativi della deflazione senza rinunciare all'indipendenza da qualsiasi autorità centrale. A marzo 2014 il numero totale di bitcoin in circolazione era di 12,5 milioni e

[17] Situazione verificatasi in Giappone dopo lo scoppio nel 1991 di una bolla finanziaria, a cui seguì un lungo periodo di deflazione, noto come "decennio perduto"

sarebbe stato sufficiente aumentarlo di 500 volte, per non creare alcun impatto reale sui portafogli. Questo incremento di base monetaria (distribuendo i bitcoin pro-quota e in modo equo ad ogni portafoglio) avrebbe permesso di detenere in modo equivalente un bitcoin ad aprile 2011 od a marzo 2014.

3.5 Blockchain e fiducia

Dell'intero protocollo Bitcoin l'innovazione non riguarda tanto la moneta in sé, quanto piuttosto la sua tecnologia. La Blockchain, definita in The Economist "una macchina che crea fiducia",[18] permette a persone non in confidenza tra loro di collaborare senza alcun intermediario come un'autorità centrale che assicuri neutralità. Essa, a differenza di qualsiasi altro sistema monetario governato da una Banca Centrale, è un registro pubblico e condiviso, che tutti possono vedere e nessuno può controllare singolarmente, evitando la doppia spesa e tenendo traccia di tutte le transazioni effettuate. Anche se il bitcoin non dovesse riscuotere successo in futuro, la tecnologia sottostante permette di garantire transazioni affidabili, la quale rappresenta una necessità applicabile a qualsiasi tipo di transazione in qualsiasi campo. Dal 2014 molte tra le maggiori istituzioni finanziarie hanno effettuato ingenti investimenti in startup che si occupano di Bitcoin e Blockchain (sia quella di Bitcoin sia altri registri pubblici di creazione propria). Come mostrato in figura 3.2, l'apice degli investimenti è stato raggiunto nell'agosto 2015 per un miliardo di dollari USA, i quali sono continuati nel 2016 e 2017. Tra le società di maggior rilievo si evidenziano: Visa, MasterCard, J.P. Morgan, Goldman Sachs, Deloitte, Axa, BNP Paribas e molte altre. Alcuni esempi dell'applicazione di questa tecnologia potrebbero essere registri catastali pubblici, economici, a prova di manomissione; oppure registri che attestino la proprietà di beni di lusso od opere d'arte attraverso l'inserimento dei dati all'interno di una Blockchain senza ricorrere a notai che facciano da garanti; o ancora, in ambito bancario, registri che limitino l'intermediazione negli scambi e che garantiscano conformità e tracciabilità delle transazioni, senza la necessità che queste vengano verificate per poter andare a buon fine, permettendo di velocizzare le tempistiche e minimizzare i costi. È proprio in questo campo che potrebbe essere applicata maggiormente la tecnologia Blockchain, infatti dal 2015 è stato istituito il consorzio R3,[19] il quale riunisce oltre ottanta istituti finanziari, con l'obiettivo di sviluppare "Corda", un registro distribuito progettato specificamente per i servizi finanziari.

[18] Si veda il sito TheEconomist (https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine, consultato il 11/08/2017)
[19] Si veda il sito R3 (https://www.r3.com/about, consultato il 12/08/2017)

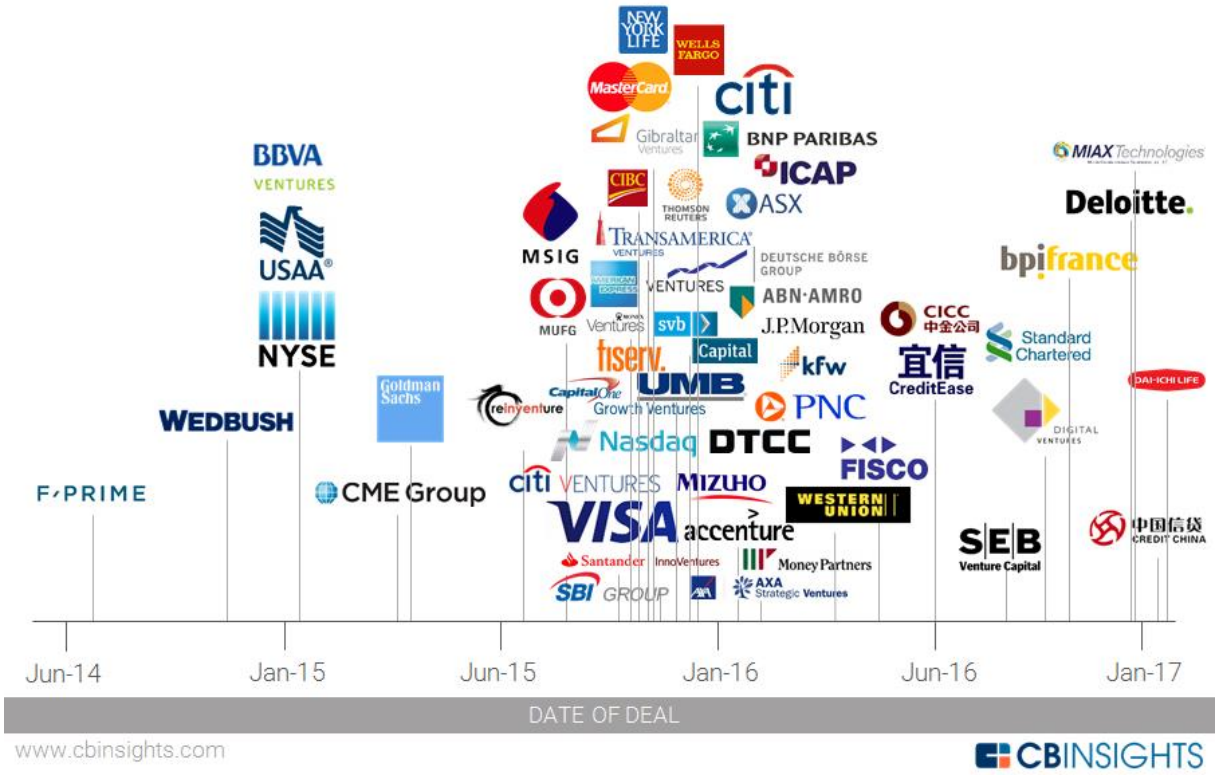

Fig.3.2: Investimenti in Bitcoin e Blockchain effettuati delle principali società di servizi finanziari

CONCLUSIONI

L'elaborato si è posto come obiettivo quello di fornire un'analisi completa di un fenomeno, ancora oggi, sconosciuto a gran parte della collettività, ma che sta assumendo negli anni maggiore rilevanza. I difetti e le potenzialità del bitcoin sono stati studiati partendo da molto tempo prima che fosse inventato, dalle teorie degli economisti Mises e Hayek, i quali ritenevano sbagliata la manipolazione della moneta da parte di un ente centrale e auspicavano la creazione di un libero mercato. Mises per primo critica la sovranità monetaria, in quanto lo Stato è in grado di influenzarne il valore di scambio attraverso politiche inflazionistiche o deflazionistiche ma non per questo è in grado di governare il mercato. Anche Hayek contesta il monopolio statale dell'emissione di moneta, ripercorrendo il processo storico che ha permesso di giungere al sistema odierno e avanza la proposta di un modello in cui le banche agiscono in concorrenza col fine di emettere moneta più affidabile e che risponda alle esigenze degli individui. Il bitcoin nasce nel 2009 e sebbene possa sembrare distante dalle teorie dei due economisti, si pone come soluzione alternativa al sistema monetario vigente, la cui caratteristica fondamentale è quella di rappresentare una valuta completamente decentralizzata e quindi non dipendente da alcuna autorità centrale. L'elaborato prosegue con una descrizione completa dell'intero sistema Bitcoin per comprendere a fondo la natura e le peculiarità di tale innovazione definita "disruptive" e che permette a diversi attori di perseguire contemporaneamente sia i propri interessi sia il benessere comune. In seguito, nell'effettuare una serie comparazioni si giunge alla conclusione che il bitcoin non può essere, ad oggi, paragonato ad una valuta fiat perché sotto il profilo strettamente giuridico esso non possiede una base di accettazione sufficientemente ampia da favorirne una diffusione capillare e non gode di un apparato normativo che lo regolamenti come mezzo di pagamento. Sotto il profilo empirico-economico, invece, il suo maggior ostacolo è costituito dalla volatilità, che lo associa più ad uno strumento finanziario speculativo piuttosto che ad una moneta, infatti per poter svolgere le funzioni di mezzo di pagamento, unità di conto e riserva di valore deve essere più stabile possibile. Anche la sua natura deflazionaria rappresenta un problema, in quanto potrebbe spingere gli individui a detenerlo come bene rifugio e non come mezzo di adempimento delle obbligazioni pecuniarie. Per queste ragioni spesso il bitcoin viene definito come oro digitale piuttosto che moneta, perché gode di proprietà che lo renderebbero più simile ad una commodity e il cui ruolo è riconducibile a quello dell'oro all'epoca del passaggio da un'economia di baratto ad un'economia monetaria. Il futuro di questa valuta è 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.

Bibliografia e sitografia

AMETRANO, F., 2016. Hayek Money: the Cryptocurrency Price Stability Solution. SSRN papers. Disponibile su <https://ssrn.com/abstract=2425270> (consultato il 09/08/2017)

ANTONOPOULOS, A., 2014. Mastering Bitcoin. 1° ed. Sebastopol (California): O'Reilly.

BAUR D., DIMPFL, T., 2017. Realized Bitcoin Volatility. ResearchGate. Disponibile su <https://www.researchgate.net/publication/317994265_Realized_Bitcoin_Volatility> (consultato il 07/08/2017)

BÖHME, R., CHRISTIN, N., EDELMAN, B., MOORE, T., 2015. Bitcoin: Economics, Technology, and Governance. Journal of Economic Perspective, American Economic Association, 29 (2), pp.213-238

CARBONE, F., 2012. A scuola di economia. Lezioni del professor Jesùs Huerta de Soto liberamente trascritte e rielaborate. 1° ed. Livorno: Usemlab, pp.141-146

EUROPEAN CENTRAL BANK, 2015. Virtual currency schemes – a further analysis. Disponibile su <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> (consultato il 26/07/2017)

EUROPOL, 2015. Changes in modus operandi of Islamic State terrorist attacks – Report. Disponibile su <https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-terrorist-attacks> (consultato il 24/07/2017)

HAYEK, F.V., a cura di PETRONI A., 2001. La denazionalizzazione della moneta. 1° ed. Italiana. Milano: Etas.

HENDRICKSON, J., HOGAN, T., LUTHER, W., 2015. The Political Economy of Bitcoin. Economic Inquiry, Western Economic Association International, 54 (2), pp.925-939

HILEMAN, G., RAUCHS, M., 2017. Global Cryptocurrency Benchmarking Study. Cambridge Centre for Alternative Finance, University of Cambridge. Disponibile su

<https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf> (consultato il 07/08/2017)

HM TREASURY – Dipartimento governativo del Regno Unito, 2015. UK national risk assessment of money laundering and terrorist financing – Report. Disponibile su <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf> (consultato il 24/07/2017)

KATSIAMPA, P., 2017. Volatility estimation for Bitcoin: A comparison of GARCH models. Economics Letters, Elsevier, 158, pp.3-6

MISES, L.V., a cura di BELLOFIORE R., 1999. Teoria della moneta e dei mezzi di circolazione. 1° ed. Italiana. Napoli: Edizioni Scientifiche Italiane.

MORGAN STANLEY IQ, 2007. Commodity Book. Disponibile su <http://www.morganstanleyiq.it/pdf/downloads/82_Commodity%20Book_Sett07.pdf> (consultato il 04/08/2017)

NAKAMOTO, S., 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin Project. Disponibile su <https://bitcoin.org/bitcoin.pdf> (consultato il 29/06/2017)

ROSEN, S., 1997. Austrian and Neoclassical Economics: Any Gains From Trade? Journal of Economic Perspective, American Economic Association, 11 (4), pp.139-152

SELGIN, G., 2014. Synthetic commodity money. Journal of Financial Stability, Elsevier, 17, pp.92-99

SØRENSEN, P., WHITTA JACOBSEN, H., 2010. Introducing advanced macroeconomics: growth and business cycles. 2° ed. Maidenhead (Berkshire): McGraw-Hill Education.

WHITE, L., 2015. The Market for Cryptocurrencies. Cato Journal, Cato Institute, 35 (2), pp.383-402

YEAGER, L., 1997. Austrian Economics, Neoclassicism, and the Market Test. Journal of Economic Perspective, American Economic Association, 11 (4), pp.153-165