UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

Il mercato del bitcoin: studio di una "moneta" alternativa

RELATORE:

CH.MO PROF. *Brunello Giorgio*

LAUREANDO/A: *Bragato Alberto*

MATRICOLA N. *1089953*

ANNO ACCADEMICO 2016 – 2017

INDICE

Premessa……..…….....7

1 Introduzione…..……...8

1.1 Cos'è il Bitcoin……..……8

1.2 Storia…….……...……..9

1.3 Hayek e la scuola austriaca……..……..…..15

1.4 Caratteristiche di Bitcoin…….16

1.5 Alternative coins……..18

2 Funzionamento…….……..…20

2.1 La blockchain…….....……..20

2.2 Come ottenere bitcoin……..…....21

2.3 Il mining……..…….22

2.4 Transazioni in Bitcoin……..……25

2.5 Il problema del double spending……..26

3 Profili economici…….……...……29

3.1 Bitcoin può essere definito moneta?.....……..…….29

3.2 Differenza con le valute legali…….…….31

3.3 Legale o illegale?.....32

3.4 Bitcoin e le banche…….……..35

4 Il futuro di Bitcoin……..……..37

4.1 Vantaggi……..……37

4.2 Svantaggi…….……42

4.3 Ipotesi future……..……..44

Conclusioni……..……47

Bibliografia…….……50

PREMESSA

Negli ultimi dieci anni sono stati fatti considerevoli passi avanti sia nel mondo della finanza in senso lato che nel mondo dell'informatica ma soprattutto è avvenuta (e sta avvenendo) una vera e propria rivoluzione nell'intersezione tra questi due macro-ambiti.

Si sta espandendo sempre più un processo di informatizzazione dei pagamenti che si presenta sotto varie forme: a partire dalle ormai comuni carte di credito, carte prepagate, bancomat, fino ad arrivare all'ancora poco diffuso *mobile payment*[1] e soprattutto a delle valute completamente virtuali chiamate appunto, criptovalute.

Oltre alla continua "informatizzazione" del concetto di moneta, un altro fattore che negli anni stimolò il sorgere di monete elettroniche è il fatto che il potere di acquisto di una qualunque moneta non è legato a nessun valore in senso fisico ormai da molto tempo: in origine, il valore della moneta era legato al valore dell'oro (epoca del *Gold Standard*) ma tale sistema aureo venne abbandonato definitivamente negli anni '30 del '900 quando si passò ad un sistema di cambi flessibili. (Schiaroli, 2012)

La grande rivoluzione introdotta dall' *Information & Communication Technology* (ICT) unita al cambiamento dello scenario economico globale sta portando grossi dubbi e ripensamenti sulla natura stessa della moneta. (Meggiato, 2014)

Questa tesi mira ad analizzare nel dettaglio la prima e più importante criptovaluta, il Bitcoin, prestando particolare attenzione alle opportunità, minacce e possibili sviluppi futuri legati a questo particolare sistema di pagamento.

Il testo si articola in 4 sezioni:

Nell'introduzione viene spiegato cos'è Bitcoin, come è nato e quali sono le sue caratteristiche fondamentali.

Il primo capitolo tratta il funzionamento dei meccanismi che stanno alla base del sistema di pagamento e che ne hanno permesso una diffusione così ampia.

Il capitolo successivo parla dei profili economici connessi a Bitcoin, soffermandosi sul concetto di moneta e sull'applicabilità di tale concetto alle criptovalute.

Nel capitolo finale si spiegano i vantaggi e gli svantaggi ricavati dalle informazioni sinora fornite e si tenta di ipotizzare possibili scenari futuri.

[1] Processo con cui è possibile effettuare pagamenti utilizzando dispositivi mobili come smartphone e tablet.

1 INTRODUZIONE

1.1 COS'E' IL BITCOIN

Il bitcoin (BTC) è, come dice il nome, una "moneta" fatta di bit. Per essere più precisi è una criptovaluta ovvero una valuta regolata da algoritmi matematici. In questo testo si possono trovare altri sinonimi di criptovaluta tra cui "moneta elettronica" e "moneta matematica".
Le criptovalute per definizione sono valute digitali indipendenti da qualsiasi unità centrale, che utilizzano la crittografia per verificare le transazioni e regolare l'emissione di nuove unità di valuta. (Hanna Halaburda, 2016)
Già da questa breve definizione iniziale si può notare che le valute virtuali hanno caratteristiche completamente diverse rispetto alle monete tradizionali; infatti una criptovaluta per essere definita tale deve utilizzare la rete digitale e la crittografia per poter circolare e soprattutto deve essere indipendente dalle autorità centrali.
Queste sono solo due tra le peculiarità di Bitcoin che verranno approfondite dettagliatamente in seguito.
Nello specifico bitcoin non è una semplice criptovaluta ma è la prima e più famosa criptovaluta immessa nel mercato. Con la diffusione dei bitcoin ha avuto inizio un processo di radicale cambiamento sia fisico per quanto riguarda i sistemi di pagamento e le transazioni di denaro, sia concettuale con la messa in discussione dei fondamenti stessi della moneta.
Anzitutto una prima distinzione: con il termine "Bitcoin" (con la lettera "B" maiuscola) ci si riferisce alla tecnologia e alla rete di pagamento virtuale mentre con il termine "bitcoin" (con la lettera "b" minuscola) si intende la valuta in sé.
Il Bitcoin è quindi un sistema di pagamento virtuale basato su una rete di comunicazione *peer-to-peer*[2] il cui scopo è quello di rendere più semplici e veloci i pagamenti online eliminando la necessità di intermediari finanziari e garantendo allo stesso tempo alti livelli di sicurezza.

[2] Con il termine peer-to-peer si intende un tipo di architettura informatica composta da nodi che non sono soggetti a gerarchia e quindi non si presentano nella forma client-server ma sono nodi equivalenti che si possono comportare sia da client che da server (la forma è client-client).

1.2 STORIA

La nascita di Bitcoin è un fenomeno piuttosto recente ma per capirne fino in fondo le origini è necessario fare qualche passo indietro cominciando dalla storia della crittografia.
Inizialmente la crittografia era uno strumento utilizzato esclusivamente dalle istituzioni per mantenere la segretezza di piani o operazioni, ma negli anni '70 ci fu un cambiamento sostanziale in questo ambito: la crittografia diviene pubblica e alla portata di tutti.
Tale cambiamento è stato stimolato e sostenuto dalla rapida espansione dell'era digitale avvenuta in questi anni e, conseguentemente, dall'uso di apparecchi tecnologici che richiedevano un certo livello di privacy.
Una conseguenza del binomio disponibilità pubblica della crittografia e diffusione di dispositivi tecnologici fu inizialmente il miglioramento della privacy nei servizi di pagamento offerti dalle banche, e in un secondo momento, la nascita di sistemi di pagamento elettronici che usavano denaro virtuale.
Verso la fine degli anni '80 nacquero i *Cypherpunks* ovvero un gruppo di attivisti che diedero vita ad un movimento che prevedeva l'uso cospicuo della crittografia informatica come base per scatenare un percorso di rivolte sociali e politiche (ad esempio rendendo pubbliche verità che grazie all'informatica erano in grado di scovare). Questi esperti di crittografia discutevano e si organizzavano tramite una *mailing list* cioè una piattaforma online con lo scopo di condividere idee e progetti, di cui facevano parte nomi importanti tra cui Eric Hughes (uno dei fondatori), David Chaum e Wei Dai.
Il 9 Marzo 1993 proprio Eric Hughes in *"A Chyperpunk's Manifesto"* descrisse la *mission* e la *vision* dei Cypherpunks come: *"Privacy is necessary for an open society in the electronic age… privacy in an open society requires anonymous transaction systems… Privacy in an open society also requires cryptography… We must defend our own privacy… Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money."*.
(A Chyperpunk's Manifesto, 1993)
Tale movimento ebbe quindi il merito di riunire molti esperti in materia e di fungere da "incubatore di idee" dal quale nacquero progetti ad alto grado innovativo; per questo motivo può definirsi il precursore e la fonte di molti cambiamenti in ambito informatico ed economico dagli anni Novanta ad oggi (come appunto l'avvento di Bitcoin).
In realtà l'idea di una criptomoneta in sé stessa non risulta essere innovativa. Sin dagli albori di internet, infatti, ci sono stati movimenti volti alla creazione di una moneta virtuale, tuttavia non

si è mai riusciti a risolvere problematiche connesse alla natura intrinseca del dato informatico in quanto digitale e afflitto da fenomeni non autorizzati di copia. (Wayner, 2008)

Nel 1983 venne creato il primo sistema di pagamenti virtuali *"e-cash"* ad opera della *Digicash Inc.* fondata dal crittografo americano David Chaum.

L'innovazione introdotta da tale sistema era che il denaro virtuale veniva tenuto nel proprio computer e poteva essere speso per acquisti su Internet o nei negozi che lo accettavano, il tutto quindi senza passare attraverso le banche che si limitavano a controllare crittograficamente il denaro in questione.

Tuttavia le banche si dimostrarono ostili a questo sistema di pagamenti e in molte non lo accettarono, impedendo così ad *e-cash* di crescere e facendo fallire la *Digicash*. (Chaum, 1983)

Un altro esempio di un predecessore di Bitcoin è quello di *"e-gold"* una moneta digitale creata dalla società *Gold & Silver Reserve Inc.* ("GSR") nel 1996 e scambiata a fronte di depositi in oro o argento. Detenere questa valuta quindi significava detenere una certa quantità di metalli preziosi presso la GSR come riserva. (Synopsis of e-gold transactions, 1996)

E-gold poteva essere usata sia per trasferire denaro tra privati sia per gli acquisti on-line e questo comportò l'adozione di questa valuta da sempre più persone fino a che nel 1999 il mercato crebbe talmente tanto da provocare la nascita di piattaforme di *exchange*[3] indipendenti.

Nel 2007 *e-gold* venne accusato dal governo statunitense di permettere il riciclaggio del denaro provocando il definitivo blocco degli account e delle transazioni nel 2009.

La gran parte dei sistemi di pagamento virtuali esistenti fino a prima degli anni 2000, tra cui quelli appena descritti, erano sistemi centralizzati ovvero avevano come pilastro portante una banca o un'istituzione che ne regolava il funzionamento e ne garantiva le transazioni (o quantomeno si limitava a svolgere alcune funzioni che altrimenti non sarebbe stato possibile compiere).

La svolta dal punto di vista concettuale avvenne nel 1998 anno in cui il programmatore Wei Dai e il crittografo Nick Szabo propongono entrambi separatamente due diversi sistemi di pagamento decentralizzati.

Wei Dai creò una moneta chiamata *b-money* basata su alcune proprietà che si riscontrano tutt'ora in Bitcoin: la creazione di moneta si effettua tramite risoluzione di problemi grazie ad una certa potenza di calcolo (peculiarità cardine di Bitcoin come verrà approfondito in seguito), le transazioni avvengono mediante uso della firma digitale e infine gli utenti si registrano in un network anonimo tramite pseudonimi o nomi che non ne rivelino l'identità. (Dai, 1998)

[3] Gli exchange sono siti online in cui è possibile scambiare criptovalute (e non solo) con moneta legale e viceversa al tasso di cambio attuale.

Nick Szabo ideò nello stesso periodo di Wei Dai (ma separatamente da quest'ultimo) una criptomoneta (*bit-gold*) che a sua volta possedeva caratteri che contribuirono alla nascita di Bitcoin.

Anche nel caso di *bit-gold* la creazione di moneta avveniva grazie a calcoli effettuati da diversi processori proprio come previsto dall'idea di Wei Dai; nello specifico i calcolatori devono trovare la cosiddetta *"challenge string",* ovvero una stringa di bit tramite un processo definito *"proof-of-work"*[4]. Ogni *challenge string* è unica e può essere rilevata da un solo utente (il primo in ordine cronologico che riesce a trovarla) e solo una volta terminata la ricerca della stringa precedente si può passare alla successiva; l'utente che riesce a rintracciare per primo tale stringa la fa propria ed è di conseguenza autorizzato a spenderla: in questo modo nel sistema *bit-gold* viene generata "moneta". (Szabo, 2005)

Tutti i fenomeni e gli eventi appena descritti contribuirono in modi diversi alla nascita di Bitcoin. Nel Novembre del 2008 un certo Satoshi Nakamoto pubblicò su Internet un *paper* intitolato *"Bitcoin: A Peer-to-Peer Electronic Cash System"* (Nakamoto, 2008) il cui obiettivo era spiegare come fosse possibile il trasferimento di denaro digitale senza il tramite di istituzioni finanziarie o qualsiasi altro ente del genere.

Sull'identità di Satoshi Nakamoto, il creatore di Bitcoin, si sa ben poco: si ritiene che tale nome sia in realtà uno pseudonimo che nasconde una persona (o un gruppo di persone) estremamente esperta (o esperte) di crittografia; l'unica cosa certa è che nel 2011 in una mail mandata alla comunità Bitcoin, Satoshi Nakamoto scrisse: *"Sono passato ad altro. È (*Bitcoin*) in buone mani con Gavin (*Andresen, uno dei primi programmatori a partecipare al progetto Bitcoin*) e tutti gli altri"* (Nakamoto, 2011) perciò si sa per certo che il suo creatore non fa più parte di tale programma.

Indipendentemente dal suo creatore, il fatto di notevole importanza storica ed economica è la nascita di un sistema di pagamento completamente elettronico, costruito sul concetto che la moneta è ogni oggetto e ogni sorta di dato che sia accettato come pagamento per beni e servizi in un dato paese o contesto socio-economico. (Schiaroli, 2012)

La data ufficiale in cui è stato emesso il primo blocco di bitcoin (*"blocco 0"* o *"genesis block"*) è il 3 Gennaio 2009 e il 12 Gennaio dello stesso anno venne registrata la prima transazione con cui Satoshi Nakamoto invia 10 BTC ad un esperto crittografo facente parte dei *Cypherpunks*.

Ovviamente nei primi mesi di vita dei bitcoin il loro valore era irrilevante e gli unici a possederne erano gli sviluppatori che li avevano generati; altrettanto ovvio è che inizialmente non esistevano nemmeno quelle piattaforme online che permettevano il cambio con la valuta

[4] Prova di lavoro, consiste nel far lavorare incessantemente i processori allo scopo di trovare la soluzione ad un problema preposto (nel caso specifico tracciare la *challenge string*).

tradizionale (i cosiddetti *"exchange"*) e quindi le compravendite avvenivano esclusivamente nel forum del progetto Bitcoin (bitcointalk.org). L'obiettivo principale degli sviluppatori e di questo forum era diffondere sia la conoscenza della criptovaluta che la criptovaluta stessa in modo da coinvolgere sempre più utenti e in modo da ingrandire il sistema Bitcoin; per raggiungere tale scopo vennero create transazioni di qualsiasi tipo tramite le quali i possessori di bitcoin acquistavano praticamente qualsiasi cosa al solo fine di diffondere informazioni: la più famosa di queste transazioni è avvenuta ad opera del programmatore Laszlo Hanyecz il quale offrì 10.000 Bitcoin (pari a circa 25$ all'epoca) per due pizze: tale operazione passò poi alla storia come la "pizza da 10.000 BTC". (Hanyecz, 2010)

Per comprendere l'entità della crescita di Bitcoin basti pensare che al tasso di cambio attuale (Giugno 2017) le due pizze sarebbero state acquistate per un controvalore di circa 25 milioni di dollari.

Nel 2010 vennero creati i primi *exchange* e ciò provocò una perdita di controllo sulle transazioni per gli sviluppatori, con gravi conseguenze: nell'agosto del 2010 venne scovato un punto debole nel sistema di sicurezza, ovvero le transazioni non venivano controllate in modo preciso ed esaustivo prima di venire registrate; ciò permise ad un gruppo di hacker anonimi di generare dal nulla un blocco del valore di 184 milioni di BTC e di spenderli in molteplici modi. In poco tempo gli sviluppatori intervennero correggendo il *bug* del sistema e annullando le transazioni fasulle. (Taras, 2016)

Negli anni successivi il valore di Bitcoin ha avuto un andamento generalmente positivo, con varie fluttuazioni di segno opposto ma il trend globale era di crescita sostenuta.

A Febbraio del 2011 il prezzo di un bitcoin arriva per la prima volta a quota 1$. Nel Giugno dello stesso anno si verifica la cosiddetta *"The Great Bubble of 2011",* termine con cui ci si riferisce all'aumento del prezzo del bitcoin da 10$ a 31,91$ in soli 4 giorni. (Buterin, 2012)

Il 2011 è l'anno in cui il mondo ha iniziato a rendersi conto dell'esistenza di Bitcoin, infatti il suo utilizzo crebbe rapidamente; molte associazioni iniziarono ad accettare tale criptovaluta per le donazioni e vennero aperti moltissimi siti web per scambiare bitcoin con prodotti di qualsiasi tipo.

Nel biennio 2012-2013 aumentò moltissimo il numero dei commercianti in grado di accettare pagamenti in bitcoin grazie soprattutto alla semplificazione dei processi di pagamento e all'attivazione di sistemi (ad esempio Bitpay, CoinBase e GoCoin) che permettono ai negozianti e alle imprese di convertire i bitcoin in valuta locale.

Il 27 Settembre 2012 venne creata la "Fondazione Bitcoin" con l'obiettivo di proteggere e promuovere tale valuta garantendo sicurezza agli utilizzatori e aumentando la loro fiducia verso questo sistema di pagamento.

Nell'Aprile del 2013 il prezzo di un bitcoin supera per la prima volta quota 100$ e a Novembre dello stesso anno raggiunge quota 1000$ registrando una crescita e un picco record. (DT, 2013)
Il 2014 è stato un anno che ha visto il prezzo di bitcoin decrescere progressivamente: a Gennaio un bitcoin era scambiato con circa 800$ con picchi sporadici fino a sfiorare i 900$; da Febbraio è iniziato un forte calo che, dopo una lieve ripresa nel mese di Luglio, ha visto il prezzo di Bitcoin chiudere a fine anno attorno ai 400$ con una perdita di circa il 52%.
Le cause che spiegano questo declino sono molteplici: la più importante e incisiva è stata sicuramente il fallimento di *Mtgox* nel Febbraio 2014 che in passato era una tra le principali e più utilizzate piattaforme di *exchange* a livello globale.
Mtgox si dimostrò insolvente a causa di numerosi attacchi hacker che provocarono una perdita stimata di circa 800.000 BTC con ingenti danni ai portafogli degli utenti. Questo fatto non solo fece perdere molti risparmi agli utenti di *Mtgox*, ma soprattutto contribuì a diminuire ulteriormente la già instabile fiducia nei confronti di Bitcoin. (Frediani, 2014)
Un'altra causa è stata la chiusura di *Silk Road 2.0* nel Novembre del 2014. *Silk Road* (poi definito "l'Amazon delle droghe") era un sito online nato nel 2011 per la compravendita di droghe, materiali pericolosi e altri prodotti illegali in cambio di bitcoin. Tale sito ebbe parecchio successo e tutti i suoi utilizzatori, costretti ad acquistare bitcoin per comprare quella merce, contribuirono in modo rilevante alla crescita e alla diffusione della criptovaluta.
La prima versione di *Silk Road* venne chiusa nell'Ottobre 2013 ma successivamente venne aperto *Silk Road 2.0*, una piattaforma ancora più grande e che attirò ancora più utenti con un circolo di bitcoin ancora maggiore; la sua chiusura provocò un calo negli acquisti della criptovaluta comportando un relativo calo anche nel suo prezzo. (Frediani, 2014)
A fare da contrappeso a questa tendenza al ribasso del prezzo unitario di BTC, alcune multinazionali tra cui Microsoft e Dell iniziarono ad accettare la criptovaluta come mezzo di pagamento contribuendo ad aumentarne la diffusione e soprattutto rivestendo di importanza e di sicurezze questa valuta ancora per molti sconosciuta.
Il 2015 è stato un anno complessivamente positivo per Bitcoin anche se ha subito alcuni traumi (il 19 Agosto il prezzo di bitcoin è sceso del 19% in appena 30 minuti a causa di un attacco hacker ai danni di un importante *exchange*, evento che prese il nome di *"Flash Crash"*) ma nonostante tutto in poco tempo è riuscito a risollevarsi e a fine Dicembre arriva a sfiorare la soglia dei 500$. (DOTSON, 2015)

Nel 2016 Bitcoin ha registrato crescite lente ma sostenute e continuative, confermando così il ruolo di criptovaluta leader del mercato e di investimento alternativo estremamente appetibile per qualsiasi tipo di investitore.

A fine anno il prezzo di un bitcoin stava per raggiungere quota 1000$.

Le vere crescite record e i veri picchi che dimostrarono il potenziale di Bitcoin si sono registrati proprio nel 2017, precisamente tra Marzo e Giugno: a inizio Marzo il valore di un bitcoin era appena sopra i 1000$ mentre il 12 Giugno 1 bitcoin poteva essere scambiato con quasi 3000$.

La principale causa di questa crescita esponenziale risiede in una delle caratteristiche principali di Bitcoin: la non tracciabilità. A Marzo 2017 c'è stato un attacco da parte di un gruppo di hacker russi che ha colpito moltissime tra le imprese più grandi del mondo (imprese del calibro di Renault che fu tra l'altro una tra quelle colpite più gravemente); questi hacker hanno chiesto un riscatto pari all'equivalente di 300$ in bitcoin (per non essere rintracciati) per ogni computer infettato dal loro virus. Ovviamente le imprese furono costrette ad acquistare bitcoin per pagare il riscatto, e in tempi rapidi oltretutto per non fermare la produzione e non perdere dati importanti; tale acquisto di massa fece esplodere il prezzo della criptovaluta.

La Figura 1 riassume tutti i valori annunciati finora.

Figura 1: *Grafico rappresentante il prezzo medio di un bitcoin (BTC) in dollari statunitensi (USD) da Gennaio 2009 (data di creazione di Bitcoin) ad Agosto 2017 (Blockchain.info, 2017)*

1.3 HAYEK E LA SCUOLA AUSTRIACA

Le radici del concetto alla base di Bitcoin (e di altre criptovalute) vengono comunemente individuate nel pensiero della scuola austriaca.

Infatti l'ideologia del Bitcoin presenta molte affinità con questa corrente di pensiero: le più rilevanti sono l'avversione ai governi e alle banche centrali, il giudizio negativo riguardo gli effetti dell'inflazione e il libertarianesimo insito in entrambe le concezioni.

Nonostante queste somiglianze Bitcoin e scuola austriaca non possono considerarsi del tutto compatibili; la più grande critica che i libertariani fanno al sistema Bitcoin è di non avere un valore intrinseco come l'oro, l'unico valore intrinseco associato alla criptovaluta è pari ai non indifferenti costi di produzione di tale "moneta".

Nel testo "La denazionalizzazione della moneta" di Hayek si cela una critica ai fondamenti che sostengono il Bitcoin. (Hayek, 1976)

La più grande critica che Hayek avrebbe fatto al Bitcoin è che quest'ultimo non può essere paragonato ad una moneta a causa della sua volatilità. La volatilità insita nel sistema Bitcoin proviene dal fatto che chi ha creato questa valuta digitale voleva contrastare l'inflazione togliendo potere alle banche centrali, ma ha ritenuto che irrigidire la creazione di moneta fosse l'unico sistema per ottenere questo fine.

Il premio Nobel per l'economia, avrebbe sostenuto che l'insieme dei meccanismi che sorreggono Bitcoin lo rendano fin troppo instabile e a questo non può essere affiancata una ferrea disciplina nella creazione di moneta. In circostanze come questa, nonostante la sua aversione alle autorità centrali, Hayek avrebbe teorizzato che delle ipotetiche banche avrebbero dovuto intervenire nel mercato, riducendo o aumentando la liquidità in circolazione con l'obiettivo di mantenere più stabili i prezzi.

Solo così facendo Bitcoin avrebbe potuto essere accostato a ciò che consideriamo moneta. (R.A., 2014)

Un elemento che gli aderenti alla scuola austriaca avrebbero apprezzato di Bitcoin è che grazie alla sua innovazione ha dato vita ad un mercato (quello delle criptovalute) che magari in futuro potrà portare alla concorrenza di valute private. Essi ipotizzavano che una situazione del genere avrebbe portato verso la stabilità monetaria: avrebbe abbattuto il monopolio statale nell'emissione di moneta e avrebbe lasciato da parte tutte le valute instabili in quanto non accettate dagli utenti (tutto questo però, con il presupposto che Bitcoin avesse adottato meccanismi per ridurre la volatilità). (Matonis, 2011)

Sicuramente al momento non si può parlare di concorrenza poiché nonostante la presenza di molte altre criptovalute diverse da Bitcoin, è quest'ultimo a possedere la maggiore quota di mercato in quanto le altre valute digitali non sono sufficientemente diffuse.
In conclusione possiamo ipotizzare che, nonostante i punti in comune tra l'ideologia di Satoshi Nakamoto e quella di Hayek e della scuola austriaca, questi ultimi non avrebbero apprezzato la criptovaluta a causa della sua volatilità e della rigidità nell'offerta di bitcoin.

1.4 CARATTERISTICHE DI BITCOIN

Come già accennato, il successo di Bitcoin è dovuto ad alcune sue caratteristiche estremamente innovative e rivoluzionarie tali da permettere la forte espansione di questi anni.

- **Anonimato delle transazioni**: questa è probabilmente la caratteristica più iconica del sistema e prevede che i bitcoin siano detenuti in *wallet* virtuali a cui si può accedere tramite un *username* (completamente fittizio e slegato dal vero nome del possessore) e una *password*. Le transazioni in bitcoin utilizzano *l'username* e non un nome vero e proprio, quindi chiunque lo voglia può tenere segreta la sua identità. Questa prima caratteristica ha enormemente avvantaggiato gli scambi illegali in cui ovviamente meno informazioni circolano e meglio è.

- **Non tracciabilità**: Le transazioni sono tutte registrate dal sistema in un apposito registro chiamato *blockchain* (verrà spiegata dettagliatamente in seguito) ma, essendo anonime, non è possibile risalire al mittente o al destinatario di queste ultime rendendole a tutti gli effetti non tracciabili.

- **Gestione peer-to-peer**: con questo si intende che il sistema è soggetto non ad un'architettura *server-client* ma ad un'architettura *client-client* in cui tutti i nodi sono allo stesso livello e le informazioni sono equamente distribuite tra di essi, senza dipendere da alcun nodo centrale.

- **Decentralizzazione**: Bitcoin non prevede alcuna banca o istituzione che ne regoli il funzionamento o ne controlli i movimenti ed è oltretutto completamente indipendente da qualsiasi ente già esistente, per questo motivo è detto un sistema decentralizzato. Il corretto svolgimento delle transazioni è garantito da tante entità indipendenti (persone o gruppi di persone) che, mettendo a disposizione del sistema la potenza di calcolo dei loro calcolatori, fanno in modo che gli scambi di bitcoin procedano nel verso giusto.

- **Trasparenza**: ogni transazione viene registrata nella *blockchain* che agisce come una sorta di registro aperto al pubblico che ogni utente è libero di consultare. Nella *blockchain* è possibile constatare quali sono state le transazioni avvenute e per quale importo ed è perfino possibile appurare di quanti bitcoin sia in possesso un determinato indirizzo in un preciso istante temporale. Ovviamente la trasparenza non è in contrasto con l'anonimato delle transazioni e questo perché ogni azione viene compiuta tramite un *username* (che è noto a tutti) dal quale però è impossibile risalire alla vera identità del soggetto.

- **Impossibilità** (o estrema difficoltà) **di falsificazione**: le proprietà della crittografia garantiscono che non è possibile spendere una moneta per più di una volta, e quindi truffare gli altri utilizzatori.

- **Scarsità:** l'offerta di bitcoin è prestabilita dal protocollo e limitata a 21 milioni di unità (somma che si prevede raggiungere nel 2140 circa) e di conseguenza sono considerati un bene scarso.

- **Facilità di scambio**: i pagamenti, ovvero i trasferimenti di bitcoin da un utente all'altro, avvengono in maniera diretta attraverso la rete, senza la necessità di intermediari.

- **Facilità d'implementazione**: il codice è *open source*[5], e ne esistono numerose implementazioni gratuite in rete. Un sito *e-commerce* che vuole adottare questo mezzo di pagamento può farlo senza grandi complicazioni tecniche, senza costi di licenza e senza contratti vincolanti con gli istituti di credito.

[5] Software non coperto da copyright e accessibile a chiunque.

- **Semplicità di custodia**: I bitcoin sono custoditi nel *wallet* cioè un portafoglio nel proprio computer (praticamente come fossero dei file in una cartella) e quindi è possibile tenerli in casa senza doversi avvalere dei servizi di una banca.

1.5 ALTERNATIVE COINS

Il fenomeno Bitcoin, a causa della sua innovazione e del suo anticonformismo, ha da subito destato molto scalpore soprattutto nel mondo dei programmatori informatici che ne capirono fino in fondo il funzionamento e le potenzialità.
Alcuni di questi sviluppatori seguendo le orme di Satoshi Nakamoto e copiando alcuni aspetti del suo lavoro crearono altre criptovalute; ciò è stato possibile per merito del carattere *open source* di Bitcoin grazie al quale chiunque poteva e può visionare e modificare il software Bitcoin.
Tutte le criptovalute nate dopo Bitcoin vengono definite *"alternative coins"* (o *altcoins*).
Secondo il sito coinmarketcap.com al momento (Agosto 2017) esistono 1032 *alternative coins* diverse e, visto il potenziale posseduto da questi sistemi di pagamento, tale numero è in aumento (basti pensare che solamente due anni fa, nel 2015, ne erano presenti circa 600).
Le *alternative coins* hanno tutte dei tratti comuni alla base del loro funzionamento e tali tratti consentono di definirle a tutti gli effetti criptovalute.
Tutte queste valute sono decentralizzate, non fanno affidamento cioè ad alcuna autorità centrale; inoltre sono fondate su una tecnologia di base simile (o addirittura identica) alla *blockchain* introdotta da Bitcoin. La quasi totalità delle *altcoins* infine, utilizza il *mining* (verrà analizzato in seguito) come risorsa per controllare la veridicità delle transazioni e per emettere "moneta". (Meggiato, 2014)
Alcune di queste criptovalute replicano fedelmente i principi base e le tecnologie di Bitcoin mentre altre aggiungono nuove caratteristiche e funzioni.
Di seguito viene proposta una tabella con le prime 10 criptovalute, dopo Bitcoin ovviamente, in ordine decrescente di capitalizzazione di mercato.

NOME	CAPITALIZZAZIONE DI MERCATO (USD)	PREZZO (USD)	UNITA' IN CIRCOLAZIONE	VOLUME (24H)
Bitcoin	$ 53.674.060.395	$ 3254,28	16.493.375 BTC	$1.050.210.000
Ethereum	$ 24.608.936.985	$ 262,26	93.834.838 ETH	$1.006.710.000
Ripple	$ 6.910.135.465	$ 0,180215	38.343.841.883 XRP	$ 54.235.400
Bitcoin Cash	$ 4.368.204.158	$ 264,99	16.484.163 BCH	$ 173.275.000
Litecoin	$ 2.380.090.953	$ 45,46	52.351.457 LTC	$ 102.636.000
NEM	$ 2.319.534.000	$ 0,257726	8.999.999.999 XEM	$ 10.969.800
Dash	$ 1.440.089.255	$ 192,60	7.477.177 DASH	$ 23.377.100
Ethereum Classic	$ 1.437.636.793	$15,25	94.296.617 ETC	$ 50.489.200
IOTA	$ 1.249.037.523	$ 0,449370	2.779.530.283 MIOTA	$ 8.382.510
NEO	$ 981.270.000	$ 19,63	50.000.000 NEO	$ 130.616.000
Monero	$ 708.474.748	$ 47,55	14.898.791 XMR	$ 8.380.070

Tabella 1: *Bitcoin e le prime dieci alternative coins per capitalizzazione di mercato (dati rilevati il giorno 06/08/2017). (CoinMarketCap, 2017)*

Va precisato che, data l'elevata volatilità delle criptovalute, i dati riportati in questa tabella possono subire considerevoli variazioni, quindi nel momento in cui verrà letta questa tesi potrebbero essere estremamente discostanti dai dati effettivi in quell'istante.

2 FUNZIONAMENTO

2.1 LA BLOCKCHAIN

La base su cui poggia l'intero sistema Bitcoin è una tecnologia innovativa chiamata *blockchain.*
La *blockchain* è un protocollo di comunicazione ovvero una base di dati fatta di blocchi che memorizzano al loro interno tutte le transazioni valide avvenute; in ogni blocco è contenuto l'*hash* (una funzione algoritmica informatica) del blocco precedente, questo consente di collegare insieme i blocchi consecutivi formando una catena in cui ogni anello aggiuntivo rinforza quello precedente.
Questa funzione di Bitcoin rappresenta il modo principale con cui il sistema sopperisce alla mancanza di un'autorità centrale: la *blockchain* infatti è la garanzia che ogni utente ha sulla buona riuscita delle transazioni. (Bellini, 2017)
Ogni scambio viene registrato in un blocco facente parte della catena e rappresenta la prova che quella transazione è avvenuta rispettando tutti i parametri imposti dal sistema. Questo meccanismo genera alti livelli di sicurezza infatti, quando una transazione viene registrata nella *blockchain* diventa impossibile modificarla o annullarla. Tale particolarità protegge gli utenti da eventuali frodi o truffe ai danni sia del compratore che del venditore.
Riassumento quindi da un punto di vista tecnico la blockchain è un insieme di blocchi contenenti transazioni, posti in ordine cronologico a partire dal *"genesis block"* in cui ciascun blocco è legato tramite l'*hash* al blocco precedente.
Da un punto di vista più concettuale invece la *blockchain* è un registro pubblico in cui viene minuziosamente registrata dal sistema ogni transazione effettuata e a cui chiunque può accedere.
La figura seguente spiega il ruolo che la *blockchain* assume nelle transazioni in bitcoin.

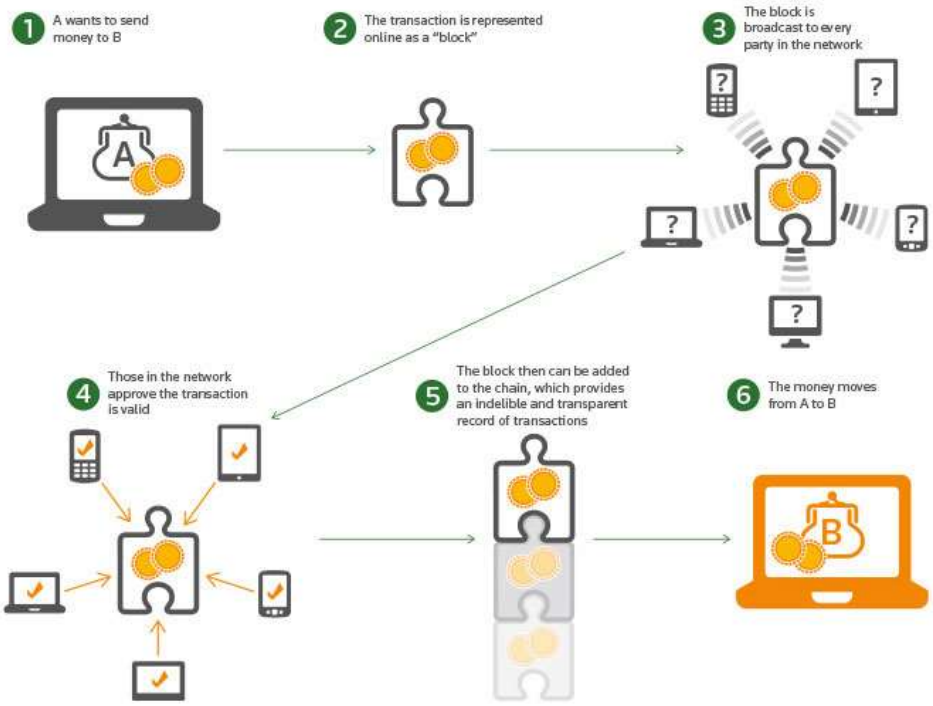

Figura 2: *Funzionamento della Blockchain (Bellini, 2017).*

2.2 COME OTTENERE BITCOIN

Esistono quattro modi per ottenere bitcoin:

- **Cambiare una valuta in bitcoin**: ovvero acquistare bitcoin presso gli *exchange* online in cambio di valuta legale o di altre criptovalute. Il tasso di cambio a cui comprare o vendere bitcoin è fissato dalla stessa piattaforma online che quindi svolge il ruolo di *market maker*. I migliori e più famosi Bitcoin *exchange* al momento (ovvero quelli più usati e più votati dagli utenti) sono *Coinbase*, *LocalBitcoins* e *Poloniex* (BestBitcoinExchange, 2017).

- **Bitcoin ATMs (o Bancomat Bitcoin)**: si tratta di dispositivi fisici in cui è possibile acquistare bitcoin con un enorme abbattimento dei tempi per l'autenticazione richiesti dagli *exchange* online, infatti se si è già in possesso di un *wallet* la transazione avviene in meno di 30 secondi. Il primo Bitcoin ATM è stato prodotto dall'azienda americana

Robocoin ed installato nell'ottobre 2013 presso la *Waves Coffee House* di Vancouver, Canada. Già nel suo primo giorno di funzionamento questo Bancomat Bitcoin ha registrato ben 81 transazioni per un valore totale di oltre 10.000 $. Visto l'aumento dell'offerta di bitcoin nel mondo, il numero di Bitcoin ATMs sta aumentando proporzionalmente (Schiaroli, 2012).

- **Vendere beni o servizi in cambio di bitcoin**: nel mondo sono sempre più numerosi i negozi fisici e i siti di compravendita online che accettano pagamenti in bitcoin.

- **Fare mining**;

I primi tre metodi sono tradizionali e possono essere applicati a qualsiasi valuta mentre il *mining* è una tecnica che viene utilizzata da Bitcoin (e da gran parte delle *alternative coins*) per ovviare alla mancanza di un intermediario finanziario che garantisca la sicurezza nelle transazioni.

2.3 IL MINING

Come già accennato, uno dei punti cardine su cui è stato creato il Bitcoin è la totale decentralizzazione quindi l'indipendenza dalle banche o da qualsiasi altra istituzione.
E' stato anche detto che la *blockchain* ha come scopo garantire la sicurezza delle transazioni; ma com'è possibile che le transazioni siano sicure in un sistema autonomo e lontano da tutte quelle che fino ad oggi erano considerate le certezze fisiche per quanto riguarda gli scambi di denaro? Come sopperire alla mancanza di un'autorità centrale? Come garantire la fiducia in un sistema così diverso da ciò a cui siamo abituati?
La risposta a questi quesiti viene fornita da un processo chiamato *mining*[6].
Il *mining* è un processo basato sulla risoluzione di un *proof-of-work* che consente ad ogni individuo (detto anche *miner*) di mettere a disposizione del sistema Bitcoin la potenza di calcolo di un calcolatore (tramite un software *open source* e gratuito) facendo in modo che questo lavori per decriptare e verificare le informazioni scambiate in ogni transazione, per poi creare un

[6] Il termine *mining* vuole rievocare un'esplicita analogia con le miniere in cui i minatori scavano per ottenere l'oro.

blocco che raggruppi tutte le transazioni effettuate e validate in un certo intervallo di tempo; tutto questo allo scopo di mantenere l'integrità della *blockchain*.

Ma come fa Bitcoin a verificare la correttezza di ogni transazione?

Il sistema impone la risoluzione di una funzione *hash* per ottenere un *hash value*, ovvero una stringa alfanumerica di lunghezza prefissata. Ai dati della transazione iniziale è associato un unico *hash value* ed è quindi l'unico elemento che, una volta trovato dai miners, può accertare la transazione e creare il blocco. Questo processo ha un elevato grado di sicurezza in quanto anche un minimo cambiamento nei dati iniziali modifica completamente l'*hash value*.

Un ulteriore elemento che aumenta la sicurezza di Bitcoin è che ogni nuovo *hash value* contiene informazioni su tutti i blocchi precedenti; ciò significa che nemmeno a posteriori è possibile modificare o falsificare i dati di uno scambio avvenuto in precedenza altrimenti il sistema se ne accorgerebbe. (Meggiato, 2014)

Tutti i nodi della rete competono per essere i primi a trovare una soluzione ad un problema crittografico che riguarda il blocco candidato, un problema che non può essere risolto in altri modi se non tramite un enorme numero di tentativi con cui si cerca di trovare la stringa che riesca a chiudere il blocco. Quando un nodo trova l'*hash value* corretto lo annuncia al resto della rete attribuendosi così i bitcoin in premio previsti dal protocollo; i nodi che ricevono il nuovo blocco lo verificano e lo aggiungono alla catena, ricominciando il lavoro di *mining* al di sopra del blocco appena ricevuto.

Per ogni blocco completato si ottiene come ricompensa sia una frazione in bitcoin, frazione che dipende da molte variabili tra cui la complessità di ogni transazione e la capacità computazionale messa a disposizione del sistema Bitcoin, sia delle commissioni di transazione.

Nel sistema Bitcoin le regole per il *mining* sono stabilite con estrema precisione. Infatti ogni due settimane si devono produrre mediamente 2.016 nuovi blocchi, circa 1 ogni 10 minuti, indipendentemente dal numero di transazioni presenti nel sistema.

Alla fine del periodo di due settimane se i nuovi blocchi prodotti si discostano dal numero obiettivo di 2.016, la difficoltà di produzione di un nuovo blocco viene diminuita o aumentata, a seconda che l'output di nuovi blocchi sia stato inferiore o superiore alla soglia.

Anche la quantità di nuovi bitcoin emessi ad ogni produzione di un nuovo blocco è fissata (ovvero la ricompensa per i minatori). Tale importo si attestava originariamente in 50 BTC per blocco, e viene dimezzata progressivamente ogni 210.000 nuovi blocchi ovvero circa ogni 4 anni (bitcoinmining.com, 2017).

Questa ricompensa attribuita ai *miners* che risolvono un blocco è l'unico modo che il sistema Bitcoin ha per emettere "moneta" e visto che tali ricompense sono rigorosamente prestabilite è possibile concludere che si tratta di un sistema con un'offerta anelastica.

Alla luce di quanto detto e appurato che non solo la quantità e delle transazioni ma anche il numero di miners aumenta sempre di più nel tempo, la difficoltà di creare ogni singolo blocco cresce ad un tasso elevato. Infatti più *miners* sono presenti nel sistema e più potenza di calcolo viene erogata per risolvere il blocco, ma quando quest'ultima aumenta il sistema fa in modo di rendere più complessi gli algoritmi da decriptare, aumentando di conseguenza il numero di calcoli mediamente necessari a creare un nuovo blocco (in modo da raggiungere sempre il numero limite di 2.016 nuovi blocchi ogni due settimane) e aumentando quindi il costo di creazione dello stesso.

A tale proposito si noti la Figura 3.

In parole povere il *mining* è stato ideato da Satoshi Nakamoto per rendere sicura la *blockchain* e tale sicurezza è "comprata" dallo stesso protocollo attraverso un particolare sistema di attribuzione di ricompense.

C'è da dire però che il *mining* è un processo molto costoso per i *miners* in quanto i calcolatori appositi hanno prezzi elevati, vengono sfruttati al massimo della loro CPU (e quindi si usurano in poco tempo) e il processo in sé consuma molta energia elettrica.

Ad oggi per fare *mining* è necessario iscriversi ad una *pool* cioè un gruppo di *miners* che riunisce la capacità computazionale di ogni individuo in modo da impiegare meno tempo a risolvere un blocco e quindi avere più probabilità di essere ricompensati; in cambio dell'adesione a queste *pool* è necessario pagare una tassa pari ad una percentuale variabile per ogni ricompensa ricevuta.

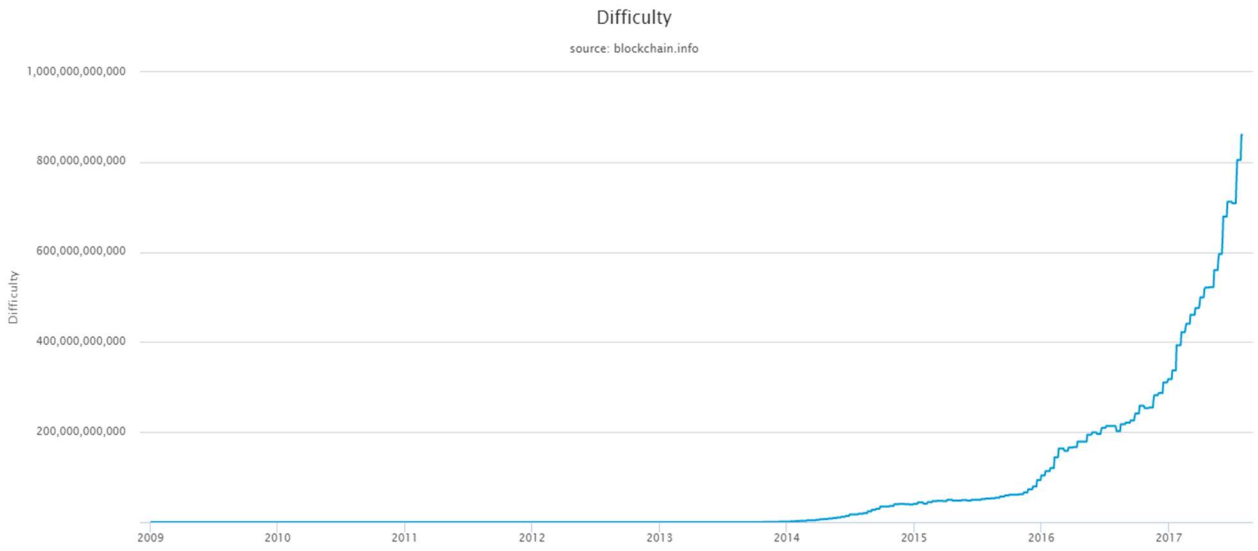

Figura 3: *Difficoltà del mining dal 2009 ad oggi (Luglio 2017) (Blockchain.info, 2017).*

2.4 TRANSAZIONI IN BITCOIN

Mettendo assieme tutti i concetti espressi finora si ottiene un quadro generale di come funzionano le transazioni con i bitcoin.

Partendo dall'inizio: una transazione (cioè l'invio di bitcoin da un wallet A a un wallet B) avviene utilizzando un codice segreto detto *private key* (chiave privata) o *seed*, che identifica in modo univoco un wallet e che serve per porre la firma digitale sulle uscite di bitcoin.

Solo possedendo la chiave privata è possibile spendere dei bitcoin a questa associati. Le chiavi private sono memorizzate nel nostro computer o presso server a seconda del tipo di wallet che si possiede.

La chiave pubblica si origina a partire dalla chiave privata e viene utilizzata per verificare le firme digitali sulle transazioni, senza dover divulgare la chiave privata, e non viene rivelata finché la transazione non viene firmata.

Per ogni chiave privata esiste solamente una chiave pubblica in grado di decriptare il codice correttamente e ciò rende lo scambio unico.

Infine dalla chiave pubblica è generato l'indirizzo Bitcoin, ovvero l'indirizzo effettivo di ciascuno dei wallet coinvolti nello scambio (Peck, 2012).

Quando si conoscono le chiavi private di entrambi i *wallet* la transazione può avere luogo.

Una volta che la transazione è compiuta tra gli utenti, va confermata dal sistema Bitcoin.

Per verificare e confermare la transazione viene avviato il processo di *mining* in cui i *miners* racchiudono le transazioni avvenute negli ultimi 10 minuti in un nuovo blocco che sarà quindi l'ultimo della *blockchain*. Grazie a questo processo viene implementata la sicurezza nel registro delle transazioni e viene verificato e approvato lo scambio in questione.

Una volta registrata la transazione nella *blockchain*, il trasferimento di bitcoin tra i due soggetti è ufficialmente avvenuto.

Quanto tutto questo processo appena descritto è svolto in maniera corretta, cioè le transazioni sono state controllate e registrate con successo nella *blockchain*, allora tali transazioni risultano irreversibili e non potranno più essere modificate.

La Figura 4 spiega i passaggi che avvengono durante una transazione con i bitcoin.

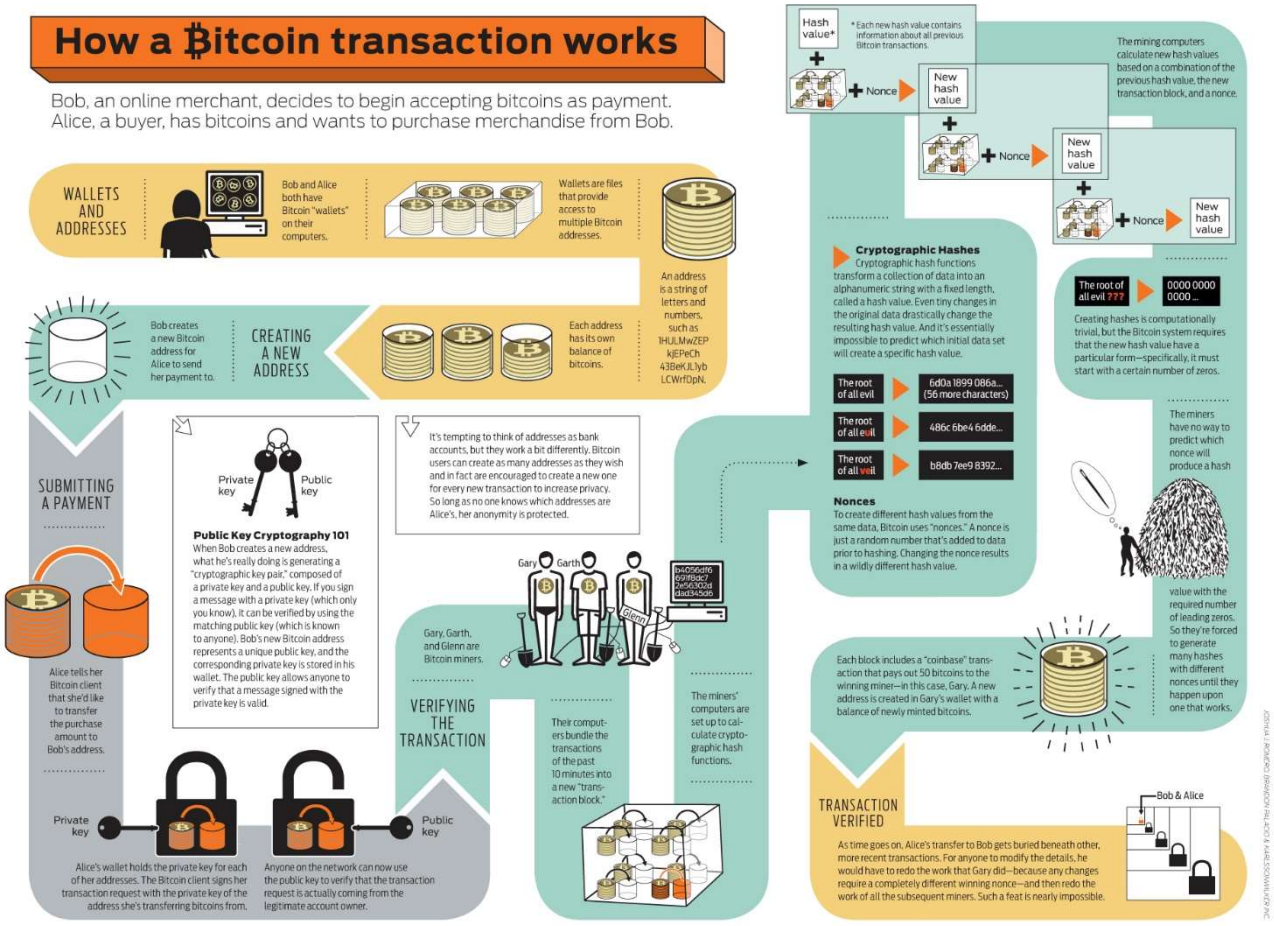

Figura 4: *Funzionamento delle transazioni nel sistema Bitcoin (Peck, 2012).*

2.5 IL PROBLEMA DEL DOUBLE SPENDING

Dal processo appena descritto per le transazioni si evince un grande rigore e una assoluta precisione nei meccanismi per la verifica degli scambi e successivamente per la creazione dei relativi blocchi.

Tutto ciò per evitare quella che è una delle più grandi minacce al Bitcoin: il *double spending*. Questo problema consiste nella possibilità di spendere una stessa unità di valuta digitale più di una volta.

Essendo una moneta completamente virtuale è lecito pensare che qualche abile hacker possa copiare bitcoin da qualche *wallet* o rubarli dalle transazioni avvenute in passato.

Bitcoin ha adottato una soluzione efficace contro questo tipo di frode. Quando i *miners* creano un blocco, l'*hash value* ricavato contiene delle cifre che confermano ogni volta la veridicità di tutte le transazioni presenti nella *blockchain* fino a quel momento. Il che significa che per ogni blocco che viene aggiunto tutte le transazioni presenti vengono "ricontrollate" e visto che abbiamo detto che un nuovo blocco viene aggiunto circa ogni 10 minuti significa che ogni volta che questo intervallo di tempo trascorre, verrà effettuato un ulteriore controllo.
Nel momento in cui qualcuno dovesse effettuare una transazione con un ammontare di bitcoin già usato in passato, il sistema se ne accorgerebbe subito e non confermerebbe tale scambio rendendo quindi vano il tentativo di un *double spending attack*.
Nonostante questo, è convenzione del sistema ritenere che una transazione è sicuramente non soggetta a *double spending* solo dopo un certo numero di conferme (e quindi dopo un certo numero di blocchi). Questo perché un truffatore particolarmente abile potrebbe modificare l'*hash value* del blocco contenente la transazione fasulla in modo da generare una biforcazione nella *blockchain*.
Affinché l'attacco abbia successo è necessario che la biforcazione originata dal blocco contenente la transazione fraudolenta sia più lunga dell'altra e che quindi sia erroneamente ritenuta da Bitcoin più sicura (questo perché più blocchi significano più controllo e più certezze). La conseguenza di questo processo è che la biforcazione più corta viene trascurata e i nuovi blocchi andranno aggiunti nella parte più lunga, quella cioè contenente un *double spending problem*.
Il *double-spending* quindi è una "gara" tra il nodo/cliente disonesto (l'eventuale hacker) e tutti gli altri nodi onesti del network a chi produce più blocchi a partire da quello corrente in modo da rendere una biforcazione della *blockchain* più lunga dell'altra (Hanna Halaburda, 2016).
Ma che probabilità ha il *double spending attack* di andare a buon fine?
La risposta a questo quesito è spiegata in termini statistici dallo stesso Satoshi Nakamoto nel suo *paper*. Il creatore di Bitcoin sostiene che la probabilità che l'attacco abbia successo dipende dalla capacità di calcolo del nodo disonesto (*h*, percentuale della potenza di calcolo totale del network detta *hashrate*) e dal numero di conferme (*n*) che la controparte attende prima di cadere nella trappola.
A tale proposito Nakamoto specifica che se la potenza di calcolo del nodo disonesto *h* è superiore a quella complessiva dei nodi onesti, ovvero se *h* è maggiore del 50%, l'attacco avrà successo nel 100% dei casi indipendentemente da *n*.
Quindi fissato un numero di conferme *n*, maggiore è la capacità computazionale *h* del nodo disonesto e maggiore è la probabilità che l'attacco vada a buon fine.

Fissato invece *h*, maggiore è *n* e minore sarà la probabilità di successo dell'attacco (Nakamoto, 2008).

A questo punto ha senso chiedersi quante conferme sono necessarie per essere sicuri di non incorrere in questa minaccia.

Nella guida sull'utilizzo di Bitcoin, pubblicata nel forum ufficiale bitcoin.org è scritto che sarebbe necessario attendere quanto meno sei conferme per pensare che un pagamento sia protetto da questo tipo di attacchi. Questo numero deriva dal fatto che il nodo disonesto dovrebbe essere in possesso di un hardware incredibilmente potente per riuscire a sostituire sei blocchi.

In ogni caso è assodato che più conferme si attendono e più la sicurezza aumenta.

3 PROFILI ECONOMICI

3.1 BITCOIN PUO' ESSERE DEFINITO "MONETA"?

Il primo punto prettamente economico da discutere è se bitcoin possa essere effettivamente considerato "moneta" o meno.
Anzitutto è necessario specificare che per moneta si intende tutto ciò che viene utilizzato come mezzo di pagamento e che assolve alle tipiche funzioni di:

- *Unit of account* (unità di conto);
- *Medium of exchange* (mezzo di scambio);
- *Store of value* (riserva di valore).

Un'altra definizione è data dal report della Banca Centrale Europea "*Virtual Currency Scheme*" nel quale si stabilisce che come moneta legale (moneta fiat) si intende "*ogni valuta legale istituita e rilasciata da un'autorità centrale, accettata dalle persone in cambio di beni e servizi grazie alla fiducia che questi ripongono in quell'autorità*", sottolineando come la fiducia sia l'elemento cruciale nei sistemi di moneta fiat. (Virtual currency schemes - a further analysis, 2015)
Sempre nello stesso report della BCE, il bitcoin viene collocato nella categoria delle valute virtuali, definite come *"monete digitali non regolate, istituite e controllate generalmente dai suoi sviluppatori ed accettate ed utilizzate tra i membri di specifiche comunità virtuali".*
Queste due definizioni di moneta sopra esposte non solo sono diverse tra loro, ma concentrano l'attenzione del lettore in punti completamente diversi: la prima si focalizza sulle funzioni che una moneta deve possedere per essere definita tale, mentre la seconda parla di chi deve emettere moneta e di chi deve accettarla. In questo capitolo verranno analizzati entrambi gli aspetti.
Per quanto riguarda la prima definizione data di moneta è importante citare Hayek, che nel 1976 scrisse che *"tali usi della moneta* [riferito alle funzioni unità di conto e riserva di valore] *sono, semplicemente, conseguenze della funzione fondamentale della moneta quale mezzo di scambio e solo in condizioni eccezionali, come in caso di rapido apprezzamento, se ne separano".* (Hayek, 1976)

Senza alcun dubbio si può dire che Bitcoin assolve alla funzione di *medium of exchange* in quanto non solo funge da mezzo di scambio, ma mira a rendere gli scambi più rapidi ed efficienti rispetto a quelli effettuati con qualsiasi altra moneta.

Tuttavia è importante sottolineare che Bitcoin non è universalmente accettato come strumento di pagamento perciò, nonostante gli esercizi commerciali che lo adottano siano in costante aumento, al momento può risultare ancora difficile spenderli; questo può limitare notevolmente l'applicabilità del concetto di mezzo di scambio a tale criptovaluta.

Riguardo le altre due funzioni fondamentali della moneta, la volatilità presente all'interno della moneta stessa, dovuta al fatto che il sistema non può regolare la liquidità monetaria in funzione della domanda, rende il Bitcoin inadeguato come riserva di valore, impedendo che esso diventi un'unità di conto e che, a sua volta, possa sostituire le valute tradizionali.

Infatti come unità di conto, una moneta instabile non permetterebbe calcoli realistici; come riserva di valore, chi detiene liquidità preferirebbe una valuta che si apprezza, ma, in questo caso prendere denaro in prestito non sarebbe vantaggioso (R.A., 2014).

Sempre nel suo testo *"la denazionalizzazione della moneta"* Hayek aggiunge: "*un livello di prezzi stabile e un livello di occupazione stabile ed elevato non richiedono né permettono che la quantità totale di moneta sia mantenuta costante o muti a un tasso costante. [...] Mantenere costante la quantità di moneta non assicura che il flusso della moneta rimarrà costante e, per far sì che il flusso della moneta si comporti nella maniera desiderata, l'offerta di denaro deve possedere una considerevole elasticità."* (Hayek, 1976)

In Bitcoin l'offerta è quasi completamene anelastica in quanto è fissata a priori dal protocollo e muta a tasso costante nel tempo. Questo fatto avvalora notevolmente la tesi della scuola austriaca secondo cui le criptovalute non possono essere considerate moneta.

Passando alla seconda definizione, è immediato constatare che tra questa e la definizione di "valute virtuali" ci sono enormi differenze; viene posta molta attenzione sul soggetto che regola e controlla le rispettive valute ("autorità centrale" e "sviluppatori", rispettivamente) e sui soggetti che utilizzano la valuta in questione ("persone" e "membri di specifiche comunità virtuali", rispettivamente).

Ma queste definizioni sono così realistiche?

A dire il vero ci sono alcune discrepanze dovute al fatto che l'ambiente delle criptovalute è altamente instabile nonostante per alcune di queste (come Bitcoin) sia in continua espansione.

Vista l'ampiezza e la portata che il fenomeno Bitcoin ha assunto, è impossibile poter dire che è regolato e controllato dai suoi sviluppatori, infatti come già detto il sistema è regolato da individui o gruppi di individui indipendenti (i minatori).

Inoltre Bitcoin ad oggi ha raggiunto una diffusione tale da non essere più accettato ed utilizzato solo "tra i membri di specifiche comunità virtuali" ma chiunque può acquistare e spendere bitcoin quindi anche in questo caso ormai si può tranquillamente parlare di "persone".
In conclusione secondo il report della BCE le criptovalute non possono essere considerate monete legali data la mancanza di un'autorità centrale che ne regoli i movimenti.

3.2 DIFFERENZA CON LE VALUTE LEGALI

Fatte queste considerazioni è fondamentale capire nel dettaglio che differenze ci sono tra i bitcoin e le valute legali.
Un'importante conseguenza della decentralizzazione di Bitcoin è che questo, a differenza delle valute legali, non è soggetto a politiche monetarie: infatti non essendo presente un'autorità centrale nessuno può esercitare azioni coercitive sulla valuta. L'offerta di moneta, che per le valute legali può essere modificata dalla banca centrale, nel caso di Bitcoin è stata stabilita a priori dal protocollo ed è stata programmata in modo che aumenti costantemente fino a raggiungere il limite di 21 milioni (soglia che verrà raggiunta nel 2140 circa). Infatti, l'andamento della produzione di bitcoin è stabilito da un algoritmo con un andamento a rendimenti marginali decrescenti nel tempo.
Inoltre è necessario specificare che Bitcoin non ha corso legale, ciò significa che i bitcoin sono accettati come mezzo di pagamento solo su base volontaria. Ad esempio non possono essere utilizzati per estinguere delle obbligazioni se il creditore si rifiuta di accettarli.
Non solo Bitcoin è un sistema decentralizzato in cui non esiste alcuna autorità che ne regoli il funzionamento e ne controlli i movimenti, ma non esiste nemmeno un'autorità che "eroghi moneta". Non esiste una specie di Zecca dello Stato che si occupa di coniare i bitcoin ma questa funzione è svolta dal processo di *mining* precedentemente descritto, che permette a chiunque di "creare" questa criptovaluta.
Passando alle differenze più pratiche e meno concettuali è importante sottolineare che le transazioni effettuate con i bitcoin sono meno costose e più veloci rispetto a quelle effettuate tramite valuta legale. Il costo di ogni transazione si abbassa notevolmente data la completa assenza di intermediari finanziari, infatti mediamente per ogni transazione viene addebitata al

mittente una commissione di 457 satoshis[7] per ogni byte trasferito (dati aggiornati al 23 Agosto 2017) ma tale somma varia notevolmente sia in base al numero di informazioni scambiate in una transazione (i byte appunto) sia al tempo necessario per la verifica di ogni scambio, ossia alla difficoltà di creazione dei blocchi. (BitcoinFees, 2017)

Per dare un'idea concreta dei dati appena citati è utile ritenere che mediamente una transazione in Bitcoin è di circa 250 byte (Andersen, 2014), perciò si avrà una commissione pari a 0,00114 BTC che al momento equivalgono a circa 4,80 $.

Le transazioni sono anche molto più veloci in quanto le procedure sono completamente automatizzate; in media ogni transazione impiega 10 minuti per essere ultimata (che è esattamente il tempo necessario per la creazione di un blocco).

3.3 LEGALE O ILLEGALE?

C'è una domanda che tutti coloro che hanno approcciato questa nuova criptovaluta si sono posti: il Bitcoin è legale?

La risposta più immediata da dare è "assolutamente sì, Bitcoin è legale". Questa risposta è frutto di un sistema estremamente sicuro e trasparente che mira a proteggere la privacy degli utenti e non esiste alcuna traccia di eventuali frodi provenienti dal protocollo (gli hacker sono un argomento a parte che non ha nulla a che vedere con il sistema in sé).

La situazione è un po' più complessa se ci si chiede se il suo utilizzo sia legale o meno.

Per rispondere a questo quesito è necessario capire se le banche centrali e le istituzioni competenti approvano o quantomeno consentono l'uso di Bitcoin.

Inizialmente governi e istituti bancari hanno provato ad osteggiare in tutti i modi Bitcoin, ma con il passare del tempo si sono resi conto della potenzialità delle criptovalute e ad oggi alcuni istituti stanno studiando il modo di supportarle.

Ovviamente è difficile se non impossibile delineare un quadro completo ed esaustivo sulla legalità delle criptovalute poiché la situazione varia da paese a paese, e da banca a banca (Meggiato, 2014).

A proposito dell'illegalità ci sono da chiarire alcuni concetti.

[7] Un satoshi è l'unità più piccola in cui si può dividere un bitcoin ed è pari a 0,00000001 BTC.

Anzitutto definiamo il concetto di *deep web*: con tale termine si intendono tutti quei contenuti non segnalati dai normali motori di ricerca. I siti che ci appaiono digitando un termine su *Google* o su qualsiasi altro *browser* sono solo una piccola parte di tutto il vero web.

E' ormai assodato che la parte del web che tutti conoscono ed utilizzano quotidianamente compone circa il 4% dell'intero web; la restante parte (il 96%) viene chiamata *deep web* (o web sommerso). (Deriu, 2016)

Su tutto ciò che viene considerato *deep web* le uniche valute utilizzate come pagamento sono le criptovalute e, prima tra tutte, Bitcoin; questo perché lì è possibile comprare e vendere qualsiasi oggetto senza nessun limite o regolamento e quindi l'anonimato e la non tracciabilità sono due caratteri fondamentali che ogni utente ricerca.

In questo spazio vengono svolte attività considerate illegali in molti paesi del mondo come la vendita di droghe, armi, persone e qualsiasi bene per cui esista una domanda.

Il punto è che anche se con i bitcoin si svolgono tali attività, questo non fa del sistema di pagamento un protocollo illegale in quanto non è nato con questo scopo e il suo fine non è quello di favorire il mercato degli oggetti sopra citati (anche se in realtà, indirettamente, lo fa). L'illegalità per Bitcoin può rappresentare non solo un motore trainante per la sua crescita e diffusione, ma anche una forte leva che può modificarne il prezzo. Esempi a sostegno di questa affermazione sono i casi di *Mtgox* e *Silk Road* descritti in precedenza.

Alla luce di quanto detto finora, l'ambiente generato con la nascita Bitcoin e delle *alternative coins* sembra perfetto per svolgere attività illecite quali il riciclaggio di denaro, l'esportazione illecita di capitali e l'evasione fiscale.

Il riciclaggio di denaro[8] è una pratica resa più semplice dalle criptovalute in quanto per natura anonime e non tracciabili, quindi la loro origine non è verificabile. Se un soggetto ottiene bitcoin dalla vendita di un bene considerato illegale dall'ordinamento, nessuno potrà mai risalire alla sua identità e quindi nessuno potrà associare a tale soggetto la vendita del bene in questione. Per lui sarà molto facile giustificare il guadagno in qualsiasi modo voglia, visto che nessuno ha la facoltà di confermarlo o smentirlo.

L'esportazione illecita di capitali è più semplice da spiegare con un esempio: supponiamo che un individuo decida di iniziare a possedere bitcoin. Il primo passo da compiere è scaricare sul computer il software gratuito di Bitcoin per poi aprire un "conto" su uno dei tanti *exchange*. Il passo successivo è trasferire i fondi dal proprio conto bancario a quello appena aperto in bitcoin. A questo punto non esiste più alcun intermediario in grado di controllare e di tracciare il flusso di moneta appena originato, perciò il soggetto in questione potrebbe tranquillamente trasferire

[8] Con il termine "riciclaggio di denaro" si intendono quell'insieme di operazioni mirate a dare una parvenza lecita a capitali la cui provenienza è in realtà illecita.

il patrimonio di bitcoin su un altro conto (aperto in qualsiasi parte del mondo) intestato magari a soggetti terzi. Una volta ultimato questo ipotetico processo il risultato è che i bitcoin hanno cambiato paese e anche giurisdizione. In questo modo i capitali sono stati trasferiti verso una destinazione completamente ignota e l'operazione effettuata non lascia alcuna traccia agli occhi di autorità finanziarie tra cui quelle dell'antiriciclaggio e del controllo sull'esportazione di capitali. (Schiaroli, 2012)

Diverso invece è il problema fiscale: se si guadagnano bitcoin, come ci si deve rapportare con il Fisco?

Al momento la legge non supporta ancora del tutto il caso delle cripto-monete quindi ci si deve per forza rivolgere ad un commercialista per valutare ogni situazione nello specifico.

Bitcoin è a tutti gli effetti un fenomeno mondiale che si sta espandendo costantemente e i dati ci danno prova che vengono registrate moltissime transazioni ogni giorno.

Una situazione del genere non può essere ignorata dal Fisco perché questo significherebbe favorire l'illegalità e la circolazione di denaro "in nero".

Le uniche tasse si pagano nel momento in cui si fa la conversione da bitcoin a valuta legale, ma questo non è assolutamente detto che avvenga; è possibile ottenere bitcoin e utilizzarli per acquistare qualsiasi cosa senza mai convertirli.

Concettualmente se vengono generati profitti con le cripto-monete si tratta a tutti gli effetti di guadagni, e in quanto tali andrebbero dichiarati e tassati. (Gomiero, 2017)

Detto ciò Bitcoin risulta uno strumento incredibilmente potente per eludere i controlli sulla circolazione di denaro "sporco" e per gli acquisti online di prodotti illegali.

L'introduzione di tecnologie innovative causa sempre l'accesso a nuove opportunità, anche illecite, ed è un compito del governo emanare norme altrettanto innovative atte a contrastarle.

La Banca d'Italia nel 2015 scrisse l'*"Avvertenza sull'utilizzo delle cosiddette valute virtuali"* in cui afferma che *"In Italia, l'acquisto, l'utilizzo e l'accettazione in pagamento delle valute virtuali debbono allo stato ritenersi attività lecite; le parti sono libere di obbligarsi a corrispondere somme anche non espresse in valute aventi corso legale"*. (Banca D'Italia, 2015)

Inoltre lo stesso documento fa un monito ai cittadini per renderli consapevoli dei rischi che derivano dall'utilizzo delle criptovalute.

In Italia quindi così come nell'Unione Europea non esiste ancora un regolamento chiaro ed efficace per Bitcoin.

3.4 BITCOIN E LE BANCHE

In tutto ciò detto finora non è chiaro che rapporto ci sia tra Bitcoin e le banche.
Di certo tutte le banche centrali del mondo, da quando sono venute a conoscenza di tale sistema di pagamento si sono da subito allarmate date le grandi potenzialità di cui è dotato.
Il rischio più grosso che tutte le banche centrali temono è la perdita di controllo. Non si parla di controllo su Bitcoin che, essendo un sistema decentralizzato, è pari a zero, quanto piuttosto la paura che questo sistema di pagamento inglobi talmente tante risorse da rendere inefficace il controllo che le istituzioni monetarie esercitano su emissione, circolazione e valore della moneta. (Plateroti, 2017)
La prima istituzione monetaria a capire i rischi nascosti di Bitcoin, è stata la Banca Centrale Europea: nel 2012 una task force di esperti è stata incaricata da Mario Draghi di tenere sotto controllo la penetrazione dei bitcoin nei confini dell'Eurozona. Nell'ultimo rapporto del 2015 consegnato al direttorato di Francoforte *("Virtual currency schemes – a further analysis"),* Bitcoin figura a sorpresa come *«la più grande minaccia potenziale per la politica monetaria e la stabilità dei prezzi, per la stabilità finanziaria e la vigilanza prudenziale»* (Plateroti, 2017).
Inoltre Banca d'Italia e Consob hanno sorvegliato l'intero mercato di Bitcoin monitorando soprattutto il suo uso negli acquisti di beni e servizi. La Banca d'Italia ha emanato già dal 2015 un allarme della vigilanza sull'uso e la diffusione delle valute virtuali.
La *European Banking Authority*, l'autorità di controllo sulle banche, senza usare mezzi termini scrisse: *«Si deve scoraggiare in ogni modo l'acquisto, il possesso o la vendita di Bitcoin tra banche commerciali e tra intermediari finanziari residenti in Italia».* (Plateroti, 2017)
Da ciò si evince che il comportamento non solo della BCE, ma anche delle altre banche centrali è (o almeno era) quello di ostacolare in ogni modo l'ascesa di Bitcoin che viene visto come una minaccia in grado di sottrarre potere e autorità alle istituzioni monetarie.
Addirittura si parla di guerra tra banche centrali e Bitcoin in cui le prime tentano di arrestare l'ascesa della criptovaluta tramite varie armi tra cui la sensibilizzazione degli utenti ai rischi che questo sistema di pagamenti può comportare e l'esercizio del cosiddetto monopolio bancario tramite il rigido controllo sulla moneta legale che, per il momento, costituisce la maggior parte degli scambi.
Appena scoppiato il fenomeno Bitcoin, tutte le banche mondiali lo avevano inquadrato come un pericolo e quindi tentarono di frenarlo, ma da due anni a questa parte alcune banche si sono rese conto delle opportunità generate dalle criptovalute.
Infatti R3, una startup americana operante nel campo della finanza, si è posta l'obiettivo di applicare al mondo bancario la tecnologia sottostante a Bitcoin, la *blockchain.*

Questo fatto potrebbe causare una rivoluzione nel sistema bancario ed R3 è stata supportata e finanziata da quarantadue tra le più grandi banche al mondo tra cui Intesa SanPaolo, Unicredit, Bank of America, Deutsche Bank, J.P. Morgan, Goldman Sachs e molte altre.
L'applicazione della tecnologia *blockchain* al mondo bancario potrebbe ridurre drasticamente i tempi attualmente necessari alle transazioni di moneta, tagliando fuori dal processo tutti quegli enti al momento necessari per regolarle.
Questa nuova tecnologia procurerebbe un enorme risparmio all'industria bancaria: si tratta di circa 15-20 miliardi di dollari risparmiati all'anno. (HDblog.it, 2015)

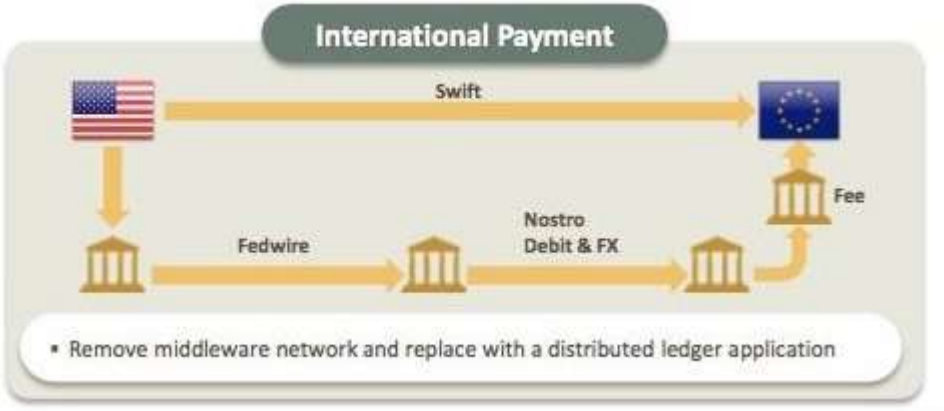

Figura 5: *Schema dei pagamenti tra USA ed Unione Europea se la tecnologia blockchain venisse applicata al mondo bancario (HDblog.it, 2015).*

In un articolo pubblicato dal sito Linkiesta nel Febbraio 2016 viene fatto un paragone molto forte ma che rende bene l'idea delle potenzialità di Bitcoin.
Vengono paragonate le banche alla grande società *Blockbuster* e Bitcoin ad una piattaforma di *BitTorrent.* Da un lato abbiamo una società che vende prodotti tangibili, i dvd, tramite negozi fisici e dall'altra un sistema *peer-to-peer* con cui gli utenti possono scaricarsi gratuitamente e in poco tempo i film che vogliono vedere.
"Da una parte gli accordi con le case cinematografiche, dall'altra l'indifferenza per il diritto d'autore. Da una parte una realtà fallita, con innumerevoli negozi chiusi e personale mandato a casa, e dall'altra una delle realtà che hanno cambiato il modo di fruire di film, serie tv e musica". (Patti, 2016)
Questo caso presenta evidenti analogie con il rapporto tra banche e Bitcoin, anche se ovviamente la questione è molto più delicata in quanto si tratta di denaro, non di film ed esistono istituzioni che agiscono per mantenere l'integrità di un sistema monetario che difficilmente potrà essere spodestato completamente da una valuta digitale.

4 IL FUTURO DI BITCOIN

Per poter anche solo pensare di fare una minima previsione sul futuro di Bitcoin è necessario, alla luce di quanto detto finora, stabilire quali siano i vantaggi e gli svantaggi di tale rete di pagamento.

4.1 VANTAGGI

1. **Riduzione dei costi delle transazioni**

   Le transazioni in bitcoin prevedono una commissione a carico del mittente che al momento è in media di 0,00114 BTC (pari a circa 4,80 $ al tasso di cambio attuale (23 Agosto 2017)) ma varia in base all'entità della transazione stessa. (BitcoinFees, 2017)

   Un'importante differenza in questo caso è che con i tradizionali sistemi di pagamento elettronici, quando si acquistano beni o servizi, la commissione è a carico del venditore e consiste in una percentuale sul totale scambiato nella compravendita. Con Bitcoin invece la commissione è totalmente a carico di colui che acquista e, non dipende tanto dal totale transato quanto dalle dimensioni in byte della transazione.

   Inoltre a tali commissioni va aggiunto che gli esercenti, per poter usufruire di sistemi di pagamento elettronici diversi dalle criptovalute, devono sostenere dei costi di installazione dei terminali POS nei negozi fisici. I costi dovuti all'accettazione di questi strumenti riducono la marginalità sulle vendite degli esercenti e questo fatto ha come plausibile conseguenza un aumento della soglia dei prezzi che quindi si traduce in un costo indiretto per il consumatore.

   Perciò è presumibile pensare che un ulteriore aumento nella diffusione di Bitcoin come sistema di pagamento potrebbe portare ad un generale abbassamento del livello dei prezzi.

2. **Riduzione dei tempi delle transazioni**

   Come detto in precedenza una transazione in Bitcoin impiega 10 minuti per essere verificata, confermata e registrata nella *blockchain*. In base all'importo della transazione, è poi utile attendere più di una conferma in modo da prevenire eventuali problemi di *double spending*. Per prevenire quasi completamente questo problema il

sistema consiglia di aspettare almeno sei conferme, perciò in massimo 60 minuti si ha la certezza non solo che la transazione sia andata a buon fine, ma anche che non ci siano stati attacchi di alcun genere.

Va comunque detto che per due persone lontane che compiono uno scambio online un'ora di tempo è un intervallo breve rispetto alle tempistiche necessarie dal sistema bancario per approvare altri tipi di pagamenti elettronici.

Per fare un confronto si osservi la Tabella 2.

STRUMENTI DI PAGAMENTO	**COSTI A CARICO DEL MITTENTE**	**COSTI A CARICO DEL DESTINATARIO**	**TEMPI**
Bitcoin	4,06 € (23 Agosto 2017)	nessuno	Da pochi secondi a 60 minuti
Carte di credito / prepagate	nessuno	Dal 3,5% al 4% sul transato	Pochi secondi
Carte di debito	nessuno	dal 2% al 2,25% sul transato	Pochi secondi
Paypal	nessuno	dal 1,8% al 3.4% + 0,35€ sul transato	Pochi secondi
Bonifici SEPA 2017	Fino a 50 €	nessuno	Massimo 3 giorni
Bonifici Extra SEPA	Fino a 50 €	Fino a 15 €	3-4 giorni
Vaglia postale	6,00 €	nessuno	3-4 giorni

Tabella 2: *Confronto di costi e tempi tra i sistemi di pagamento più diffusi.*

E' facile constatare come Bitcoin sia uno tra i sistemi di pagamento più economici e più rapidi. Si nota anche che le carte di credito hanno tempi ancora inferiori a Bitcoin ma questo solo perché il sistema deve confermare le transazioni; in linea di massima è possibile accettare anche transazioni non confermate (che quindi in tal caso impiegherebbero pochi secondi per avvenire) con tutti i rischi che ciò comporta.

3. **Accessibilità**

Qualsiasi individuo dotato di un computer e di una connessione Internet può facilmente creare un *wallet*, un indirizzo e effettuare/ricevere pagamenti da qualsiasi parte del mondo.

Per avere un portafoglio Bitcoin non è assolutamente necessario possedere un conto corrente e questo comporta che, non essendoci di mezzo alcuna banca, ognuno ha il completo controllo sui propri bitcoin.

4. **Trasparenza**

Le transazioni in Bitcoin sono tutte registrate nella *blockchain* e in tal modo sono consultabili da chiunque in ogni momento. Tuttavia in questo registro non sono presenti nomi (per via dell'anonimato) ma solamente indirizzi e username, quindi risulta alquanto difficile da interpretare.

In ogni caso conoscendo gli indirizzi delle due parti coinvolte in una transazione è possibile verificarla e questa qualità rende Bitcoin un sistema trasparente.

5. **Ruolo degli esperti**

Nessuna istituzione in Bitcoin ha il potere di apportare modifiche al protocollo; ma se in futuro dovesse sorgere qualche punto debole come potrebbe venire risolto?

A questo scopo assume un ruolo fondamentale la comunità di programmatori e di esperti che si adopera per risolvere eventuali imperfezioni.

Le ipotetiche nuove modifiche vengono apportate tramite l'emissione di nuove versioni del protocollo Bitcoin, ma queste vengono considerate ufficialmente accettate solo se la maggior parte di *miners* e di utilizzatori si converte a tale versione. Se ciò non accade allora la nuova versione viene rifiutata e nulla è cambiato. Se invece la maggioranza accetta questa versione ma alcuni *miners* continuano a lavorare con la vecchia, i blocchi da loro risolti vengono rifiutati dal sistema. (Schiaroli, 2012)

Questa particolarità del network Bitcoin assicura un elevato livello di democrazia al suo interno, in modo che solo le modifiche ritenute vantaggiose dalla maggioranza vengano effettuate e le altre scartate.

6. **Sicurezza**

Quando si effettuano acquisti online con le carte prepagate, vengono comunemente richiesti i dati presenti sulla carta. Questo può generare problemi nel momento in cui il

sito da cui stiamo acquistando abbia metodi di archiviazione dei dati poco sicuri e/o facilmente penetrabili.

Con Bitcoin funziona diversamente: le transazioni richiedono sia la chiave pubblica (visibile a chiunque) che quella privata; quando vengono unite le due chiavi si genera una funzione matematica che non ha alcuna traccia della chiave privata usata in precedenza. In poche parole finché la chiave privata resta segreta, nessuno può rubare bitcoin.

7. **Irreversibilità**

Le transazioni in Bitcoin sono totalmente irreversibili in quanto una volta registrate nella *blockchain* non è più possibile annullarle. Un individuo che ha inviato bitcoin non può in alcun modo recuperarli senza il consenso del destinatario. Questo rende vano il classico tentativo di frode diffuso con le carte di credito, in cui viene effettuato un acquisto e poi si contatta la società che fornisce le carte per annullare la transazione e ottenere un rimborso senza però restituire la merce.

8. **Non genera inflazione**

L'inflazione dipende fortemente dalla quantità di moneta in circolazione, o meglio, dal tasso di crescita dello stock nominale di moneta. A parità di altre condizioni *("ceteris paribus")* se tale tasso di crescita aumenta, anche l'inflazione aumenta mentre se il tasso di crescita diminuisce, anche l'inflazione a sua volta diminuisce. Questo rapporto è espresso dalla formula seguente:

$$\pi = g_m - g_y$$

Equazione 1: *Equazione per l'inflazione nel medio periodo. (Blanchard, 2013)*

Dove π rappresenta l'inflazione, g_m è il tasso di crescita dello stock nominale di moneta e g_y è il tasso di crescita della produzione (che in questo caso viene considerato costante in quanto non rilevante per la questione in esame). (Blanchard, 2013)

Per quanto riguarda le valute legali, se le banche centrali lo ritengono opportuno possono modificare l'offerta di moneta, aumentando o diminuendo la variabile g_m.

Se l'offerta di moneta aumenta, il valore unitario che la moneta aveva in precedenza diminuisce e questo costringe i commercianti ad aumentare i prezzi per guadagnare come prima. Questo processo quindi genera inflazione.

Parlando di Bitcoin invece, non essendo controllato da alcuna autorità, e non essendo di conseguenza soggetto alla politica monetaria, non esiste un ente che possa "stampare più moneta" e non esiste quindi un ente che possa modificare il parametro g_m.
L'andamento di g_m è già stabilito a priori dal protocollo ed è destinato a diminuire fino a raggiungere lo zero; infatti questa variabile nel caso di Bitcoin rappresenta la ricompensa in criptovaluta data ai *miners* in cambio del loro lavoro (che è l'unico modo in cui il sistema può emettere BTC) e, come detto, è destinata a dimezzarsi ogni 4 anni fino a che l'offerta di bitcoin in circolazione raggiungerà il limite massimo prefissato dal sistema in 21 milioni di unità, e quindi il "problema" dell'inflazione non sussiste (Bitcoin Veneto Team, 2017).
Per capire meglio questo concetto è utile osservare il grafico seguente.

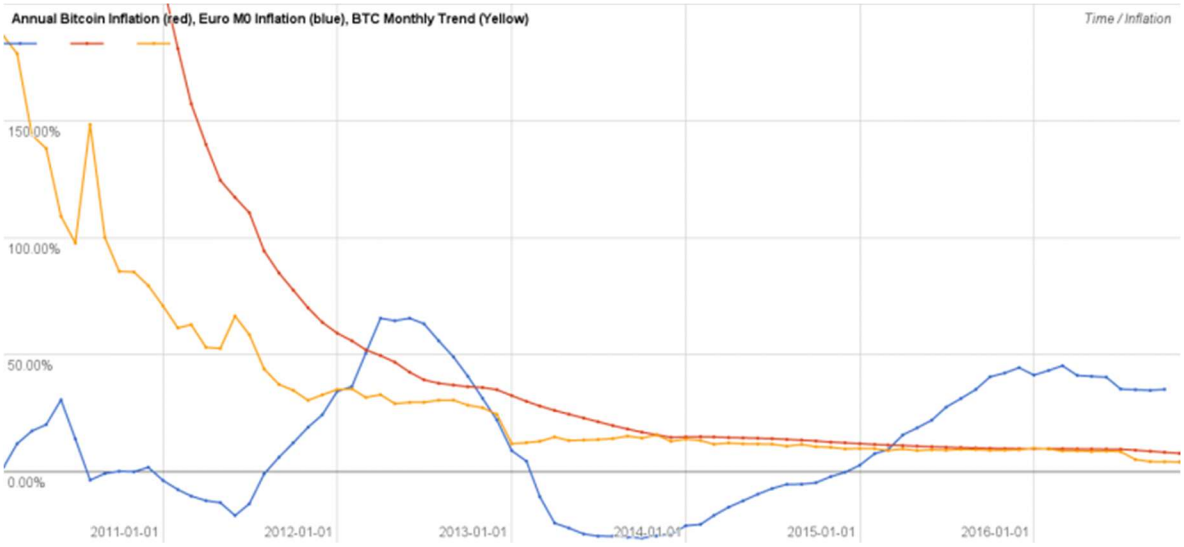

Figura 6: *Grafico avente in ascissa il tempo e in ordinata il tasso di inflazione.*

Dalla Figura 6 è possibile notare l'andamento dell'inflazione reale del BTC in rosso (dati di Blockchain.info) e dell'EURO in blu (dati ufficiali della BCE). L'inflazione in Bitcoin decresce ad un tasso pressoché costante mentre per quanto riguarda l'EURO ha un andamento variabile a seconda delle vicende politiche europee e non solo. (BlockchainTop, 2016)

4.2 SVANTAGGI

1. **Necessaria conoscenza tecnologica**

   Lo svantaggio che sicuramente si nota per primo è che, a differenza del contante, i bitcoin sono più difficili da gestire, o meglio, necessitano di una conoscenza tecnologica. Tale conoscenza può essere anche minima in quanto la gran parte dei processi descritti in questo testo sono superflui per l'individuo che vuole tenere bitcoin solo per acquistare determinati beni in determinati siti. In ogni caso è necessario quanto meno sapere come aprire un *wallet* e come spendere tale criptovaluta. Per arginare questa problematica esistono molti siti online che spiegano dettagliatamente come comportarsi in questi casi ed esistono anche iniziative che offrono corsi o consulenze in materia. Di sicuro utilizzare questa valuta è più complesso e meno intuitivo rispetto al semplice contante a cui si è abituati, ma sono disponibili tutti i mezzi necessari per imparare a gestirla.

2. **Volatilità**

   Lo svantaggio più importante in assoluto è l'estrema volatilità insita in Bitcoin e in tutte le criptovalute in generale. Questa forte instabilità nel prezzo di Bitcoin è una grande attrazione per chi li detiene a scopi puramente speculativi, mentre è un problema per tutte le altre categorie di utenti. Le grandi fluttuazioni che si notano in qualsiasi grafico sull'andamento del valore di Bitcoin, sono la principale causa che frena e rallenta la sua diffusione in quanto, mediamente, gli individui sono avversi al rischio per quanto riguarda sistemi di pagamento così innovativi e preferiscono quindi rimanere ancorati ai sistemi tradizionali.

   Una più elevata stabilità dei prezzi sicuramente gioverebbe a Bitcoin, aumentandone la diffusione e facilitando le scelte degli individui in merito a investimenti o risparmi.

3. **Irreversibilità**

   Questa qualità di Bitcoin può essere sia un vantaggio che uno svantaggio.

   E' stata introdotta dal sistema per evitare frodi ma ha anche degli aspetti negativi. Se ad esempio durante una transazione si sbaglia ad inserire l'indirizzo del destinatario l'importo della transazione può considerarsi perso in quanto sarebbe molto difficile risalire all'identità di quest'ultimo e, anche se si riuscisse, questo non sarebbe comunque costretto a restituirlo.

Tale configurazione è completamente diversa dai sistemi di pagamento elettronici tradizionali in cui esiste un processo chiamato *chargeback* con cui è possibile per un utente chiedere l'annullamento dello scambio e il rimborso dell'importo.

4. **Mancanza di diffusione**

Questo più che uno svantaggio è un limite temporaneo. Al momento Bitcoin non è ancora molto diffuso e gli esercizi commerciali (sia fisici che online) che accettano questo tipo di pagamento sono ancora pochi. E' necessario fare una distinzione: i siti di *e-commerce* che adottano questa criptovaluta sono in rapida espansione, soprattutto se consideriamo il *deep web* ma non solo. Per quanto concerne i negozi fisici invece in pochi sono a conoscenza dell'esistenza di Bitcoin e tra questi c'è ancora molta incertezza a riguardo, soprattutto in Italia; se si considerano invece di Giappone o Stati Uniti le criptovalute sono sicuramente più diffuse.

5. **Rischio di smarrimento**

Abbiamo constatato che la sicurezza è sicuramente un pregio di Bitcoin, ma è importante fare estrema attenzione in quanto, essendo detenuti in portafogli virtuali all'interno del computer, se questo dovesse rompersi o se venisse smarrito, i bitcoin al suo interno verrebbero irrimediabilmente persi. Inoltre se si dovesse smarrire la chiave privata associata ad un certo *wallet*, i bitcoin al suo interno non potrebbero più essere inviati e quindi con essi non sarà possibile effettuare transazioni.

4.3 IPOTESI FUTURE

Il fatto più importante da sottolineare è che il futuro di Bitcoin è estremamente incerto.
Questa grande incertezza è causata da molti elementi tra cui:

- l'elevata volatilità insita nel sistema stesso che può essere causa di sbalzi nel valore di un bitcoin sia nel breve che nel lungo periodo.
- le preferenze future degli utenti e il loro atteggiamento verso Bitcoin, che potrebbe venire alterato da innumerevoli fattori.
- le *alternative coins:* magari in futuro qualcuna di queste surclasserà Bitcoin facendone precipitare il valore.

Il punto è che il futuro di questa criptovaluta non può essere predetto perché addirittura il presente è in continuo mutamento.
Per dare un'idea dell'instabilità di questo fenomeno basti pensare che il 2 Agosto 2017 è uscito un articolo sul *"The Economist"* intitolato *"Bitcoin divides to rule"*. Esattamente il giorno prima, l'1 Agosto 2017, senza alcun tipo di preavviso, un gruppo di attivisti Bitcoin e imprenditori crearono una seconda versione della criptovaluta.
In meno di un giorno di vita il valore di un'unità di *"Bitcoin Cash"* (così è stata chiamata questa nuova versione di Bitcoin) ha raggiunto quota 600$ e il valore complessivo immesso nel mercato nello stesso giorno è stato di circa 10 miliardi di dollari. Questi sono valori relativamente "piccoli" rispetto a quelli assunti da Bitcoin che ad oggi (2 Agosto 2017) vale circa 2.700$ con un valore complessivo di circa 45 miliardi di dollari.
Questi appena citati sono dei dati che fanno capire in modo pratico non solo il grado di volatilità del sistema Bitcoin in sé ma anche l'imprevedibilità delle conseguenze che una qualsiasi azione esterna al protocollo può causare; ciò è dovuto ovviamente alla decentralizzazione e al fatto che in questi casi non esiste un'autorità che possa intervenire per attenuare la situazione e limitare i danni.
La causa di questa "biforcazione" si rileva nel problema di come aumentare la capacità del sistema, il quale può supportare fino ad un massimo di 7 transazioni al secondo. Questa nuova versione è in grado di processare 56 transazioni al secondo, ma per il resto opera esattamente come la versione originale.
La domanda da porsi adesso è se *Bitcoin Cash* sarà come tutte le altre *altcoins* o se invece riuscirà a farsi spazio.
L'unico fatto certo, al momento, è che questa biforcazione ha reso i possessori di bitcoin più ricchi: essi hanno ottenuto un ammontare della nuova versione della criptovaluta pari a quello

che già possedevano della versione originale e, sempre al momento, queste due messe insieme sono valutate di più rispetto che l'originale da sola. (The Economist, 2017)

Il futuro di Bitcoin è inoltre strettamente connesso al futuro del *mining*.

La ricompensa per ogni blocco creato dai *miners* era inizialmente di 50 BTC ma abbiamo detto essere destinata a dimezzarsi circa ogni 4 anni. Al momento (Agosto 2017) la ricompensa è di 12,5 BTC per blocco ma in futuro, quando la ricompensa sarà vicina allo zero, la sola remunerazione per i minatori sarà data dalle commissioni di transazione.

Nel 2140, periodo in cui si stima raggiungere la soglia limite di 21 milioni di bitcoin, la ricompensa in BTC per blocco sarà pari a zero poiché non saranno più emessi bitcoin perciò il futuro di tale criptovaluta dipenderà esclusivamente dalla sua diffusione.

Solo se questo sistema di pagamento sarà sufficientemente diffuso, e quindi il numero di transazioni aumenterà, i minatori potranno continuare il loro lavoro vedendo aumentati i ricavi delle commissioni che compenseranno, almeno in parte, le mancate ricompense per ogni blocco creato.

Se invece il numero delle transazioni non sarà tale da rendere il *mining* sostenibile, molti minatori abbandoneranno questa attività. La conseguenza più plausibile è che il *mining* quindi verrà svolto da pochi individui o società e questo potrebbe portare tali soggetti ad avere il controllo sulle transazioni e sulla *blockchain*, facendo diventare Bitcoin un sistema non più decentralizzato.

Ma da cosa dipende la diffusione di Bitcoin?

In parte dipende sicuramente dal mondo dell'illegalità; molti possessori di bitcoin sfruttano l'anonimato e la non regolamentazione per effettuare transazioni riguardanti beni o servizi illeciti. Sicuramente queste transazioni hanno aiutato molto la crescita della criptovaluta in questione ed è ragionevole pensare che potranno contribuire anche alla sua diffusione futura.

In merito al futuro di Bitcoin esistono molte opinioni contrastanti; nel forum ufficiale bitcointalk.org è possibile leggere discussioni in cui si ritiene che Bitcoin possa rivoluzionare l'intera economia globale oppure commenti in cui si dice che Bitcoin è un sistema che non sarà mai sufficientemente diffuso e che quindi sarà destinato a scomparire.

Certo è che le opinioni sul futuro di tale criptovaluta sono a dir poco eterogenee.

E' vero che Bitcoin ha il potenziale per cambiare l'economia globale ma, come visto in precedenza, a causa della sua volatilità non può essere definito moneta e quindi non potrà mai prendere il posto della valuta legale.

Questo perché l'offerta di Bitcoin pianificata dal sistema non garantisce la stabilità della criptovaluta che quindi non potrà essere caratterizzata dalle funzioni "unità di conto" e "riserva di valore".

Di certo potrebbe esserci una qualche forma di "collaborazione" tra Bitcoin e valute legali magari per rendere le transazioni più veloci o meno costose (come ipotizzato dalla startup R3) oppure in futuro potranno venire affiancate per usi differenti; questo lo si potrà sapere solo con il tempo.

CONCLUSIONI

In definitiva è opportuno svolgere un'analisi SWOT che racchiuda in un unico quadro quanto detto fino ad ora in modo da ottenere una visione d'insieme su Bitcoin da cui poi trarre le dovute conclusioni.

- **Strengths:** I punti di forza di Bitcoin sono sicuramente la tecnologia *blockchain* in grado di rendere il sistema sicuro, affidabile e veloce; il processo di *mining* che riesce a sopperire in modo efficace alla mancanza di istituzioni monetarie; la rapidità delle transazioni e la loro economicità.

- **Weaknesses:** La più grande debolezza di Bitcoin è la sua volatilità; questo carattere è la fonte della diffidenza che molti individui hanno verso la criptovaluta, è uno dei motivi che rallentano la sua diffusione e inoltre è la causa principale per cui non può essere paragonato alle valute legali.

- **Opportunities:** Le opportunità che il sistema Bitcoin porta con sé sono molteplici: a partire dalla *blockchain* che viene studiata per poter essere applicata anche al sistema bancario in modo da velocizzare le transazioni. Sicuramente Bitcoin è visto come un'opportunità dagli speculatori che sono estremamente attratti dai suoi rendimenti così alti.

- **Threats:** La principale minaccia per il sistema è causata dal *double spending attack* mentre per gli utenti è la paura che qualcuno rubi i loro bitcoin, vista la comune diffidenza che si ha verso un qualcosa di così intangibile e di quasi "irreale".

E' chiaro che Bitcoin è un sistema di pagamento sostanzialmente diverso da tutto ciò a cui si era abituati prima del suo avvento ma l'innovazione ancora più grande è stata portata dalla *blockchain* e da tutte le opportunità di applicazione e di sviluppo ad essa connesse.
La tecnologia quindi assume un ruolo centrale in questa nuova criptovaluta e prende il posto di banche e autorità governative.

Il progresso tecnologico da solo però non è sufficiente; ad impostare e a stabilire il futuro di tale tecnologia sono comunque gli utenti che con la loro adesione a questo sistema contribuiscono alla sua diffusione.

Riguardo alla diffusione di Bitcoin, i governi e le istituzioni monetarie assumono un ruolo indiretto, ma molto importante; è vero che la criptovaluta ideata da Nakamoto è per natura priva di legami con qualsiasi ente ma è un "dovere" delle istituzioni cercare di avvicinarsi a questo sistema in modo da comprenderne i funzionamenti.

Se banche e governi continuano ad ignorare il fenomeno Bitcoin, questa assenza di posizione potrebbe comportare conseguenze spiacevoli.

Date le dimensioni che questo fenomeno ha assunto è necessario imporre delle regole per evitare una smisurata crescita dei traffici illeciti e di quei reati in precedenza descritti (riciclaggio di denaro ed esportazione illecita di capitali).

Un'altra questione che dovrebbe essere regolamentata è il problema fiscale; un sistema di pagamento così utilizzato come Bitcoin e che costituisce transazioni per un ammontare di più di un miliardo di dollari ogni 24h (CryptoCurrency Market Capitalizations, 2017) non può assolutamente essere ignorato dal sistema fiscale.

Bitcoin e valute legali non costituiscono due sistemi di pagamento alternativi, non è detto che l'uno debba scavalcare l'altro, anzi possono comportarsi come sistemi complementari. Il primo potrebbe essere utilizzato per un certo tipo di transazioni, come quelle in internet oppure quelle che richiedono tempi brevi, mentre il secondo per transazioni ancorate ad un sistema bancario stabile.

Perché ciò possa avvenire, è necessario che le istituzioni comprendano le opportunità derivanti da Bitcoin e cerchino di sfruttarle al meglio.

Numero di parole: 13.896

BIBLIOGRAFIA

ANDERSEN G. (2014). Tratto da bitcointalk.org:
https://bitcointalk.org/index.php?topic=813324.0
Ottobre, 6.

BANCA CENTRALE EUROPEA. (2015). *Virtual currency schemes - a further analysis.*
Tratto da ecb.europa:
https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
Febbraio.

BANCA D'ITALIA. (2015). *Avvertenza sull'utilizzo delle cosiddette valute virtuali.* Tratto da bancaditalia: https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf
Gennaio, 30.

BELLINI M. (2017). *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*.
Tratto da Blockchain4innovation:
http://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/
Marzo, 14.

BESTBITCOINEXCHANGE. (2017). *The best bitcoin exchanges*. Tratto da BestBitcoinExchange: https://www.bestbitcoinexchange.io/
Luglio, 26.

BITCOIN VENETO TEAM. (2017). *Bitcoin Veneto*. Tratto da bitcoinveneto.it:
https://bitcoinveneto.it/perche-bitcoin/

BITCOINFEES. (2017). *Predicting Bitcoin fees for transactions*. Tratto da bitcoinfees:
http://bitcoinfees.21.co/
Agosto, 6.

BITCOINMINING.COM (2017). *Bitcoin Mining*. Tratto da bitcoinmining:
https://www.bitcoinmining.com/

BLANCHARD, AMIGHINI, GIAVAZZI. (2013). *Macroeconomia, una prospettiva europea*. Il Mulino

BlockchainTop. (2016). Tratto da blockchaintop: https://www.blockchaintop.com/bitcoin-vs-valute-corso-forzoso-parte-2-inflazione- bozza/ Novembre, 23.

Blockchain.info. (2017). Tratto da blockchain.info: https://blockchain.info/it/charts/difficulty?timespan=all Luglio.

BUTERIN V. (2012). *Anniversary of the Great Bubble of 2011*. Tratto da bitcoinmagazine.com: https://bitcoinmagazine.com/articles/anniversary-of-the-great-bubble-of-2011-1339139269/ Giugno, 8.

CHAUM D. (1983). *Blind signatures for untraceable payments.* Tratto da http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF

COINMARKETCAP. (2017). *CryptoCurrency Market Capitalizations*. Tratto da Coin Market Cap: https://coinmarketcap.com/ Agosto, 7.

CRYPTOCURRENCY MARKET CAPITALIZATIONS. (2017). Tratto da CryptoCurrency Market Capitalizations: https://coinmarketcap.com/ Agosto, 7.

DAI W. (1998). *b-money, an anonymous, distributed electronic cash system.* Tratto da http://www.weidai.com/bmoney.txt

DERIU G. (2016). *Le profondità di Internet*. Tratto da insidevcode: http://www.insidevcode.eu/2015/01/29/le-profondita-di-internet/

DOTSON K. (2015). *Bitcoin Weekly 2015 August 19: Bitcoin flash crash and Bitfinex margin trades, Bitcoin XT fork splits community*. Tratto da Silicon angle: https://siliconangle.com/blog/2015/08/19/bitcoin-weekly-2015-august-19-bitcoin-flash-crash-and-bitfinex-margin-trades-bitcoin-xt-fork-splits-community/ Agosto, 19.

DT D. (2013). *BITCOIN a +1200% nel 2013: ma è tutto oro quello che luccica?* Tratto da intermarket and more: http://intermarketandmore.finanza.com/bitcoin-a-1200-nel-2013-ma-e-tutto-oro-quello-che-luccica-59396.html Novembre, 7.

ERIC HUGHES. (1993). *A Chyperpunk's Manifesto.* Tratto da https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto Marzo, 9.

FREDIANI C. (2014). *Cosa è successo a Mt. Gox e perché non è la fine dei bitcoin*. Tratto da Wired: https://www.wired.it/attualita/tech/2014/02/26/mt-gox-fine-bitcoin/ Febbraio, 26.

FREDIANI C. (2014). *Sequestrato Silk Road 2.0 e molti altri siti del Deep Web*. Tratto da Wired: https://www.wired.it/internet/web/2014/11/07/sequestrato-silk-road-2-0/ Novembre, 7.

GOLD & SILVER RESERVE INC. (1996). *Synopsis of e-gold transactions.* Tratto da https://web.archive.org/web/19980627133928/http://www.e-gold.com/unsecure/synopsis.htm#redeem

GOMIERO M. (2017). (BRAGATO A. Intervistatore) Giugno, 26.

HANNA HALABURDA, M. S. (2016). *Beyond Bitcoin, the economics of digital currencies.* Palgrave Macmillan.

HANYECZ L. (2010). Tratto da bitcointalk.org: https://bitcointalk.org/index.php?topic=137.0 Maggio, 18

HAYEK F. A. (1976). *La denazionalizzazione della moneta, analisi teorica e pratica della competizione tra valute.* Etas Editore.

MATONIS J. (2011). *Why are libertarians against Bitcoin?* Tratto da The Monetary Future: http://themonetaryfuture.blogspot.it/2011/06/why-are-libertarians-against-bitcoin.html Giugno, 26.

MEGGIATO R. (2014). *Il lato oscuro della Rete.* Feltrinelli.

NAKAMOTO S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Tratto da bitcoin.org: https://bitcoin.org/bitcoin.pdf

PECK M. (2012). *Bitcoin: The Cryptoanarchists' Answer to Cash*. Tratto da ieee spectrum: http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash Maggio, 30.

PLATEROTI A. (2017). Banche centrali, guerra ai Bitcoin. *Il Sole 24 ore*. Febbraio, 24.

R.A. (2014). Bitcoin's deflation problem. *The economist*.

SCHIAROLI I. W. (2012). *Dark web & bitcoin. La nuova era della rete.* Lantana.

SZABO N. (2005). *Bit Gold.* Tratto da Satoshi Nakamoto Institute: http://nakamotoinstitute.org/bit-gold/ Dicembre, 29.

TARAS. (2016). *Value overflow incident*. Tratto da bitcoinwiki: https://en.bitcoin.it/wiki/Value_overflow_incident Luglio, 22.

THE ECONOMIST. (2017). Bitcoin divides to rule. *The Economist*.

WAYNER P. (2008). *Disappearing Cryptography.* Morgan Kaufmann.