UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

CORSO DI LAUREA TRIENNALE IN ECONOMIA

PROVA FINALE

"Rivoluzione Bitcoin: criticità e opportunità di un nuovo concetto di denaro"

"Bitcoin Revolution: critical issues and opportunities of a new concept of money"

RELATORE:

CH.MO PROF. Francesco Zen

LAUREANDO: Simone Tuggia

MATRICOLA N. 1090230

ANNO ACCADEMICO 2016 –2017

Sommario

INTRODUZIONE....3

CAPITOLO PRIMO: NASCITA ED EVOLUZIONE DEL BITCOIN....**4**

1.1 SATOSHI NAKAMOTO E STORIA DELLA MONETA VIRTUALE....4

1.1.1 Predecessori....4
1.1.2 Satoshi Nakamoto e i primi anni....5
1.1.3 Il caso WikiLeaks....5
1.1.4 Dark Web e Silk Road....6
1.1.5 La crescita e la diffusione del 2013....7
1.1.6 Gli attacchi hacker a Mt. Gox....7

1.2 FUNZIONAMENTO DEL SISTEMA BITCOIN....8

1.2.1 Attività di "mining"....8
1.2.2 Il "Peer-To-Peer Electronic Cash System"....9
1.2.3 La "blockchain"....10

1.3 BITCOIN E CARATTERISTICHE FONDAMENTALI DEL DENARO....11

1.3.1 Unità di conto....11
1.3.2 Riserva di valore....11
1.3.3 Mezzo di scambio....12

1.4 MONETA O COMMODITY?....12

1.4.1 Bitcoin e Gold Standard....12
1.4.2 Bitcoin come "commodity currency"....13

1.5 LE ALTRE CRIPTOVALUTE....15

CAPITOLO SECONDO: LE CRIPTOVALUTE E LE ISTITUZIONI....**17**

2.1 LIBERTA' ED INDIPENDENZA DA GOVERNI E BANCHE CENTRALI....17

2.2 BITCOIN E POLITICA MONETARIA....**18**

2.3 IL SISTEMA BTC E LE BANCHE CENTRALI....19

2.3.1 LA BCE....19
2.3.2 La Fed....20

2.4 BITCOIN E ATTIVITA' ILLEGALI....21

2.5 REGOLAMENTAZIONE INTERNAZIONALE....22

2.5.1 Gli Stati Uniti....23
2.5.2 L'Europa....23
2.5.3 La Cina....24
2.5.4 La Russia....25
2.5.5 Il Giappone....25

2.6 OGGI: IL BITCOIN COME INVESTIMENTO SPECULATIVO....26

CAPITOLO TERZO: OPPORTUNITÀ E CRITICITÀ....**28**

3.1 PROBLEMI STRUTTURALI....28

3.1.1 TEMPI DI TRASFERIMENTO....28
3.1.2 LIMITE DEI 21 MILIONI DI UNITÀ E DEFLAZIONE....28
3.1.3 IL "51% HASH POWER ATTACK"....29
3.1.4 COSTI DI GENERAZIONE....31
3.2 SICUREZZA....32
3.3 DIFFUSIONE ED ECONOMIE DI RETE....33
3.4 VOLATILITA'....35
3.5 CONCLUSIONI E POSSIBILI SVILUPPI FUTURI....35
Bibliografia (in ordine alfabetico)....37

INTRODUZIONE

Negli ultimi vent'anni si è verificata una rivoluzione senza precedenti: grazie ad internet e ai servizi ad esso connessi, siamo in grado di ottenere informazioni e trasferire dati dalla parte opposta del mondo pressochè istantaneamente; siamo arrivati a dare per scontato un insieme di tecnologie che solo trent'anni fa non solo non esistevano ma non apparivano neppure concepibili. Oggi per chi vive nei Paesi industrializzati, ma non solo, appare sempre più inimmaginabile la possibilità di lavorare, o addirittura vivere, senza utilizzare in alcun modo internet. Bitcoin e il sistema blockchain, secondo molti sostenitori, sono destinati a diventare protagonisti di questo nuovo mondo interconnesso, rivoluzionandone le transazioni commerciali e non solo.

Nel seguente elaborato ripercorrerò brevemente la storia del sistema Bitcoin, nato come semplice esperimento, divenuto oggetto di dibattito e speculazione e adesso descritto come una potenziale rivoluzione radicale dei concetti di denaro e di libero mercato; tutto nel giro di meno di un decennio. Vero protagonista di scandali e rivoluzioni degli ultimi anni (da WikiLeaks a Silk Road), considerato una delle più grandi innovazioni della storia dai sostenitori e bollato come banale schema truffaldino dai critici. Negli ultimi anni, in particolare, è divenuto anche oggetto di preoccupazioni e tentativi di regolazione da parte di

governi e banche centrali di tutto il mondo.
Confronterò le caratteristiche fondamentali del Bitcoin con quelle del denaro come lo conosciamo (o almeno come è stato concepito finora), evidenziandone gli aspetti realmente rivoluzionari anche agli occhi degli utenti meno esperti. Sottolinerò poi le problematiche che potrebbero rallentarne o impedirne la diffusione nel mondo reale, evidenziandone i maggiori vantaggi e i più gravi difetti, cercando di fornire un analisi di questo fenomeno e riflessioni sui suoi possibili sviluppi futuri nel breve e nel lungo periodo.

CAPITOLO PRIMO: Nascita ed evoluzione del Bitcoin

1.1 SATOSHI NAKAMOTO E STORIA DELLA MONETA VIRTUALE

1.1.1 Predecessori

Prima dell'introduzione del sistema Bitcoin (BTC), c'erano già stati diversi tentativi di creare una valuta digitale sicura e che, allo stesso tempo, permettesse di tutelare l'anonimato degli utenti e fosse in grado di operare senza un'autorità centrale.
Già nel 1998, Wei Dai aveva concepito "b-money", una moneta virtuale che aveva già previsto un sistema di pagamenti legato a un libro mastro virtuale paragonabile alla *blockchain* del sistema BTC, ma meno complesso e, quindi, meno sicuro nel confermare le transazioni.
Nel 2005, Nick Szabo ha presentato "bit-gold", dal punto di vista tecnico molto simile ai bitcoin, ma con gravi difetti fondamentali dal punto di vista economico: non era stata prevista una quantità ben precisa di moneta virtuale da distribuire e, soprattutto, la velocità a cui distribuirla; chiunque si fosse procurato un computer abbastanza potente avrebbe potuto produrne una quantità pressochè illimitata, azzerandone il valore.
Indubbiamente, Bitcoin è in parte basato sulle caratteristiche fondamentali di questi

predecessori, ma ha saputo distinguersi per una maggiore efficienza nella combinazione degli elementi strutturali dell'intero sistema attraverso il legame tra blockchain e attività di *mining*, come verrà illustrato in seguito. Anche le centinaia di criptovalute nate dopo il successo di Bitcoin negli ultimi anni, non si sono mai distaccate troppo dagli aspetti fondamentali del sistema BTC (si veda sotto-capitolo 1.5).

1.1.2 Satoshi Nakamoto e i primi anni

Satoshi Nakamoto è considerato l'ideatore del sistema BTC e l'autore del paper "Bitcoin: A Peer-to-peer Electronic Cash System." (disponibile su www.bitcoin.org). Pubblicato nel 2008, il paper illustra il funzionamento e le caratteristiche fondamentali della criptovaluta, mentre il software per la creazione dei bitcoin venne introdotto l'anno successivo. "Satoshi Nakamoto" probabilmente è in realtà uno pseudonimo, mentre la vera identità del creatore (o dei creatori) del Bitcoin non è stata ancora svelata. Si sono diffusi vari rumors, negli ultimi anni, riguardo a chi possa essere davvero la mente dietro la nascita della criptovaluta. Nel dicembre 2015, Wired e Gizmodo ipotizzarono che l'inventore della criptovaluta fosse l'imprenditore australiano Craig Wright che però, dopo essere stato indagato sotto pressioni da parte della Fed americana, ha dichiarato di non essere coinvolto e di voler prendere le distanze dal fenomeno (si veda Plateroti 2017b).

Per circa due anni, i bitcoin rimangono poco più di una curiosità tecnologica. Il primo, storico pagamento viene effettuato il 22 maggio 2010: il programmatore Laszlo Hanyecz, offre 10.000 bitcoin in cambio di due pizze della catena Papa John's; all'epoca il valore stimato di un singolo bitcoin era inferiore al centesimo di dollaro ma, sette anni dopo, il prezzo avrebbe superato i 2000 dollari. La transazione viene festeggiata con ironia sul web ogni anno con il "Bitcoin Pizza Day". In un'intervista del New York Times, Hanyecz ha dichiarato di non avere rimpianti per il proprio acquisto, affermando di essere stato soddisfatto di aver ottenuto un bene tangibile in cambio di qualcosa che, all'epoca, era considerato senza nessun valore (si veda Bilton 2013).

1.1.3 Il caso WikiLeaks

La criptovaluta attira prepotentemente l'attenzione dei media durante il giugno del 2011. Julian Assange attraverso WikiLeaks aveva rilasciato pubblicamente informazioni riservate e scottanti riguardo alla guerra in Afghanistan, portando i maggiori fornitori di servizi per i

pagamenti online (tra i quali PayPal, Bank of America ecc) a impedire ai sostenitori di WikiLeaks di effettuare donazioni ricorrendo ai propri servizi. Allora Assange cominciò ad accettare donazioni in bitcoin, fornendo alla criptovaluta una inaspettata pubblicità che ne sottolineava la flessibilità e, in particolare, la totale indipendenza dai servizi bancari e dalla volontà dei governi, che erano praticamente tutti schierati contro Assange e WikiLeaks.
Dopo questi avvenimenti, Satoshi Nakamoto si è definitivamente ritirato dalla community online del sistema BTC.

1.1.4 Dark Web e Silk Road

Il Bitcoin nel corso degli anni non si è solo affermato agli occhi dell'opinione pubblica come la valuta ideale dei libertari più estremi, ma anche come il mezzo di pagamento ideale per criminali interessati a vendere beni illegali o a riciclare denaro sporco grazie all'anonimato promesso dal sistema BTC.
Ricorrendo a browser speciali come Tor, è possibile accedere al Dark Web, una parte della rete internet non accessibile attraverso i browser tradizionali, rimanendo nell'anonimato. Sul Dark Web è possibile trovare siti specializzati nella vendita di beni illegali come droghe, armi e documenti falsi, che possono essere acquistati con pagamenti in bitcoin. Il sito di maggior successo è stato probabilmente il famigerato Silk Road, che in pochi anni si era affermato come la più celebre piattaforma di incontro tra venditori e compratori di prodotti illegali, in particolare sostanze stupefacenti, prima di essere chiuso dall'FBI nel 2013. Il fondatore del sito, Ross William Ulbricht, sarebbe stato arrestato due anni dopo e condannato all'ergastolo. Secondo una stima del'FBI, il sito avrebbe conseguito ricavi per 1,2 miliardi di dollari nei suoi due anni e mezzo di attività e lo stesso Ulbricht, al momento dell'arresto, è stato trovato in possesso di circa 26000 bitcoin, per un valore complessivo, all'epoca, di circa 3,5 milioni di dollari.
Inevitabilmente, la scoperta e lo smantellamento di attività illegali contribuirono ad attirare l'attenzione delle istituzioni in tutto il mondo, sollevando dubbi sulla legalità del sistema BTC (vedi sotto-capitolo 2.4).

1.1.5 La crescita e la diffusione del 2013

Nel corso del 2013, la criptovaluta attirò l'attenzione dei media anche per la crescita vertiginosa del prezzo a cui veniva scambiata. Il valore del Bitcoin era pari a 15 dollari all'inizio dell'anno, ma a novembre aveva superato i 1200, attirando un numero sempre maggiore di speculatori interessati ai bitcoin non come mezzo di scambio, ma come inusuale opportunità di investimento.

Mentre il sistema BTC continuava ad essere al centro di scandali per essere impiegato in attività illegali e controverse, cresceva anche il numero di business regolari online (e non solo) che cominciavano ad accettare pagamenti in criptovaluta, in molti casi anche soltanto come manovra pubblicitaria, dato che nonostante un progressivo aumento delle transazioni, il numero di utenti che effettuava pagamenti in bitcoin era ancora piuttosto limitato. Uno degli esempi più significativi è stato Jiasule, provider di servizi di sicurezza informatica di Baidu, il motore di ricerca più utilizzato in Cina; il servizio di pagamento sarebbe stato però ritirato alla fine dello stesso anno, nel tentativo da parte del governo cinese di contenere e regolare la criptovaluta, impedendo alle istituzioni finanziarie di trattarle (si veda Halaburda 2016, p. 98). La crescita incredibile del Bitcoin avrebbe raggiunto livelli ancora più impressionanti (e maggiore attenzione da parte dei media) nella prima metà del 2017 (si veda sotto-capitolo 2.6).

1.1.6 Gli attacchi hacker a Mt. Gox

La *mission* di Mt. Gox (uno dei principali provider di servizi legati alla sistema BTC, in particolare come "cambiavaluta"), era di fornire servizi affini a quelli di una banca a chiunque avesse un telefono cellulare con connessione ad internet, senza neppure richiedere dati identificativi fondamentali, custodendo i bitcoin dei clienti e cambiandoli su richiesta in moneta avente corso legale: potenzialmente un'innovazione radicale, in linea con lo spirito *open-source* della criptovaluta. Dopo una crescita continua, Mt. Gox era arrivato a gestire oltre il 21% delle transazioni complessive del sistema BTC, ma nel febbraio 2014, in seguito ad attacchi da parte di hacker, rimase vittima di un furto di 744.408 bitcoin depositati dai propri clienti, per un buco complessivo di circa 400 milioni di dollari. La notizia gettò i proprietari di bitcoin nel panico: si diffuse il timore che un simile attacco potesse ripetersi anche presso altri provider di servizi e il prezzo della criptovaluta crollò dopo un anno di crescite senza precedenti. I clienti che persero i propri bitcoin non hanno speranze di rivedere

i propri soldi: anche oggi, infatti, non è prevista una tutela da parte degli Stati, come invece è presente in caso di fallimento delle banche, per questo tipo di "correntisti".
La comunità Bitcoin ha reagito all'episodio sostenendo che le ingenti perdite subite da Mt. Gox erano legate a gravi errori e negligenze da parte del management e non a debolezze del sistema BTC; in effetti, negli ultimi quattro anni, non si sono più verificati episodi di simile entità.

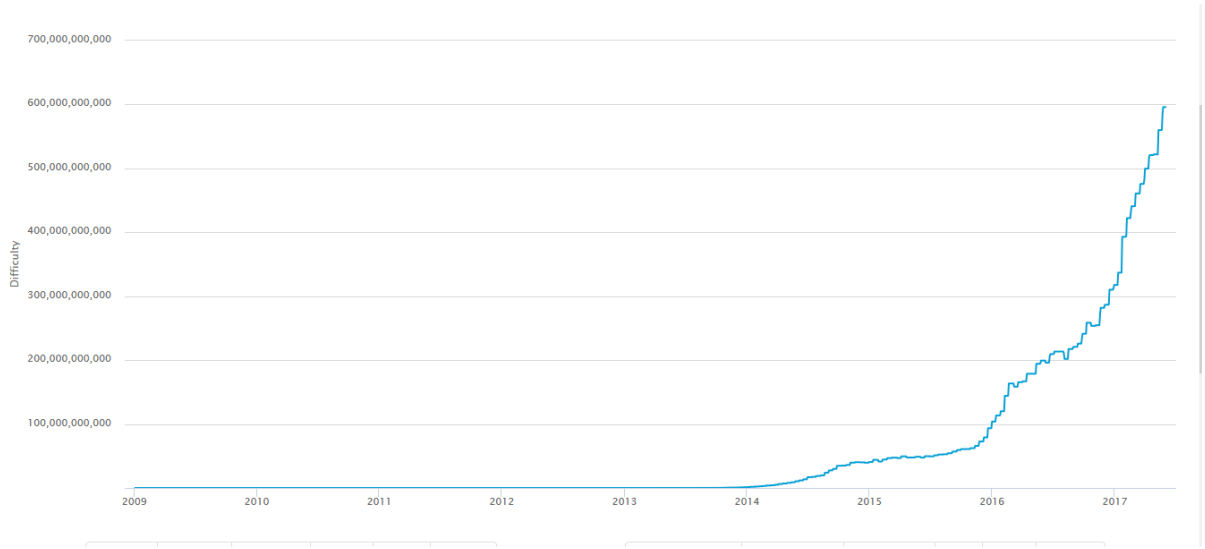
1.2 FUNZIONAMENTO DEL SISTEMA BITCOIN

1.2.1 Attività di "mining"

La creazione di nuovi bitcoin avviene attraverso la procedura di *mining*: tutti gli utenti interessati possono mettere a disposizione la potenza computazionale dei propri dispositivi per regolare le transazioni in bitcoin, svolgendo la funzione di *nodi* del sistema BTC. Attraverso questa procedura, i computer impiegati risolvono i *proof-of-work*, complicatissimi "puzzle crittografici" che garantiscono la sicurezza di ogni transazione e allo stesso tempo permettono la creazione di nuovi bitcoin, che vanno a ricompensare chi ha impiegato i propri mezzi per garantire il funzionamento del sistema BTC. I bitcoin ottenuti possono poi essere spesi, trasferiti o convertiti attraverso appositi portafogli elettronici.
Il numero complessivo di bitcoin creabili è pari a circa 21 milioni di unità e con un maggior numero di utenti coinvolti nel mining, aumenta anche la complessità dei puzzle crittografici da risolvere, garantendo in questo modo un'offerta stabile. Originariamente, infatti, il mining era praticabile da chiunque con relativa facilità (e teoricamente è tuttora eseguibile da chiunque scaricando gratuitamente un software open-source dedicato), ma negli ultimi anni, con il vertiginoso aumento del numero di *miners*, il mining è diventato di fatto possibile solo per chi utilizza hardware dedicato molto performante e costoso. Maggiore è la potenza computazionale complessiva dedicata al mining, minore è la quantità di bitcoin che il singolo utente potrà ottenere impiegando il suo dispositivo.
Con l'aumento dei prezzi della criptovaluta, un numero sempre maggiore di utenti ha cominciato interessarsi a questa attività aumentando vertiginosamente la potenza computazionale utilizzata complessivamente, tale sistema è quindi divenuto molto dispendioso anche in termini di energia impiegata ed è stato per questo oggetto di critiche (si veda sotto-capitolo 3.2.4) e di tentativi di miglioramento (si veda sotto-capitolo 1.5). Molti

utenti, infatti, preferiscono iscriversi a una "mining pool", un network dove tutti mettono a disposizione la loro potenza computazionale e vengono proporzionalmente ricompensati. Per la stragrande maggioranza degli utenti, attualmente, è più conveniente acquistare i bitcoin dai produttori, pagandoli con moneta avente corso legale.

Figura 1.1: la crescente difficoltà stimata delle operazioni di mining.
Fonte: blockchain.info



1.2.2 Il "Peer-To-Peer Electronic Cash System"

Nel paper "Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto descrive la sua visione del rivoluzionario sistema.
Nel sistema BTC non è prevista un'autorità centrale, ma tutto è regolato da un sistema *peer-to-peer* (P2P), tipologia di sistema adottato da vari network informatici come BitTorrent, che si occupa della condivisione di file in rete. Gli utenti della criptovaluta sono allo stesso tempo produttori ed utilizzatori del mezzo di scambio: i bitcoin, diversamente dalle monete aventi corso legale, non possono in alcun modo essere controllati da governi e banche centrali attraverso politiche monetarie espansive o restrittive.
Proprio per questo, i bitcoin sono stati immediatamente percepiti come un ottimo strumento per aggirare i servizi di intermediazione forniti dal sistema bancario, la cui reputazione, dopo la crisi finanziaria del 2007 era scesa ai minimi storici. Con Bitcoin viene eliminata la

necessità di un garante del valore della moneta scambiata: le parti coinvolte nella transazione possono essere sicure al 100% che la transazione pattuita sarà effettuata, grazie all'affidabilità del sistema Blockchain: anche facendo acquisti con criminali e aventi come oggetto beni o servizi illegali, venditore e acquirente possono essere sicuri che il trasferimento di denaro sarà effettuato. Con le monete aventi corso legale, invece, dobbiamo inevitabilmente fare affidamento su strutture governative come sistema giudiziario e forze dell'ordine.

1.2.3 La "blockchain"

La *blockchain* è un database che svolge la funzione di un enorme libro mastro virtuale dove, grazie alla procedura di mining da parte degli utenti, viene registrata ogni singola transazione effettuata nella storia della criptovaluta, garantendo la sicurezza e la certezza di ogni pagamento: nessuno può spendere due volte lo stesso bitcoin. Le varie transazioni, sempre grazie al contributo dei miners, vengono inserite in "blocchi", che automaticamente vengono aggiunti alla blockchain ogni 10 minuti. Una volta che il pagamento è stato inserito nella blockchain, nessuno può modificare la registrazione: agli occhi del sistema BTC la transazione è definitivamente conclusa. É stato questo sistema, secondo molti sostenitori, a garantire il successo di Bitcoin e a differenziarlo radicalmente dai vari progetti di moneta virtuale allora presenti.
Ad ogni utente del sistema BTC viene attribuito un codice alfanumerico che lo identifica agli occhi degli altri utenti, senza bisogno di fornire alcun dato personale. In questo modo, anche se ogni transazione può essere letta sulla blockchain, è possibile soltanto vedere i codici dei vari utenti, non nomi o luoghi di provenienza; la possibilità di rimanere anonimi grazie alla blockchain è stata fin da subito una delle caratteristiche che hanno attirato maggiormente l'attenzione dell'opinione pubblica e, naturalmente, dei criminali.
Il sistema Bitcoin, ricorrendo alla blockchain, si propone di ridurre drasticamente non solo i costi legati al trasferimento del denaro, ma anche le commissioni relative al cambio di valuta. Allo stesso tempo, vengono annullati i rischi legati alla contraffazione o al furto durante la transazione, senza che l'utente debba sostenere costi aggiuntivi per la protezione delle proprie transazioni, indipendentemente dall'entità delle cifre trasferite. Di fatto, però, la maggior parte dei pagamenti presso le attività commerciali che accettano i bitcoin prevede comunque una commissione, anche se in genere inferiore a quella prevista da altri intermediari finanziari per operazioni della stessa entità.

1.3 BITCOIN E CARATTERISTICHE FONDAMENTALI DEL DENARO

Affinchè un bene possa essere utilizzato come moneta nelle transazioni commerciali deve possedere i seguenti requisiti fondamentali attribuiti al denaro:

1. Essere una valida unità di conto;
2. Garantire una riserva di valore;
3. Essere un efficiente mezzo di scambio.

Indubbiamente, Bitcoin ha rappresentato una vera rivoluzione rispetto alle forme di denaro adottate nel corso della storia.

1.3.1 Unità di conto

Come unità di conto, i bitcoin hanno delle caratteristiche superiori al denaro attualmente utilizzato. In genere, le valute aventi corso legale vengono divise al massimo in centesimi, secondo un sistema decimale, mentre la criptovaluta può essere suddivisa in *satoshi*, ognuno dei quali corrisponde a 0,00000001 bitcoin, garantendo una precisione impareggiabile, indipendentemente dal tipo di valuta in cui o da cui viene convertito: un notevole vantaggio offerto dalla smaterializzazione del denaro. In questo modo, anche se il valore dei bitcoin dovesse aumentare enormemente in futuro, nei prossimi anni saranno ancora tecnicamente possibili microtransazioni e micropagamenti in qualsiasi valuta.

1.3.2 Riserva di valore

Come affermò Irwin in un articolo del Washington Post (2013), "*...if a currency can lose 75 percent of its buying power in two days, it may not be the best store of value...*". Sotto questo aspetto, la criptovaluta ha dimostrato una volatilità estrema, che rende i bitcoin inadatti come riserva di valore (si veda sotto-capitolo 3.5). Un soggetto interessato a convertire i propri risparmi in bitcoin non può in alcun modo prevedere quale sarà il loro valore non solo anni dopo, ma anche alla fine della giornata. Anche se il valore dei bitcoin ha subito una crescita notevole negli ultimi anni, non c'è alcuna garanzia che sarà così anche in futuro e per i soggetti non propensi al rischio la maggior parte delle monete aventi corso legale offre una riserva di valore più sicura e stabile.

1.3.3 Mezzo di scambio

Sotto questo aspetto, in particolare, il sistema BTC rappresenta una vera rivoluzione. Per secoli le varie forme di denaro sono sempre state inevitabilmente accompagnate da costi di varia natura: dalle spese di trasporto, quando il denaro era ancora realizzato in forma metallica, alle spese sostenute per contrastare la falsificazione, presenti anche con le moderne banconote. In tutte le transazioni che concludiamo ricorrendo al denaro contante, si presentano dei costi aggiuntivi anche in termini di tempo impiegato, ad esempio, per calcolare il resto da consegnare in seguito a un pagamento (con annesso l'inevitabile rischio di commettere errori). Senza contare che il bene che svolge la funzione di denaro dovrebbe essere in grado di poter essere speso ogni volta che ci sono un venditore e un compratore disposti a concludere una transazione a un determinato prezzo: se il compratore in questione non ha con sè in quel preciso momento abbastanza denaro da spendere, oppure il compratore non può dare il resto, viene persa un'opportunità non solo per le due parti, ma per l'intera economia. Essendo i bitcoin completamente immateriali, chiunque può trasportare il proprio intero patrimonio (anche se pari a miliardi di dollari) sul proprio cellulare e può trasferire a chiunque qualsiasi importo, in qualsiasi momento e in qualsiasi luogo.
Affinchè un simile potenziale sia sfruttato a pieno, però, è fondamentale che un maggior numero di soggetti attribuisca ai bitcoin un valore e, allo stesso tempo, sia disposto ad effettuare pagamenti ricorrendo ad essi. Una maggiore regolamentazione e una maggiore diffusione a livello globale sono forse le necessità più urgenti del sistema BTC, affinchè possa costituire un miglior mezzo di scambio (si veda sotto-capitolo 2.5).

1.4 MONETA O COMMODITY?

1.4.1 Bitcoin e Gold Standard

Bitcoin, pur essendo un prodotto della rivoluzione informatica e della filosofia *open source,* presenta molti delle caratteristiche e dei problemi fondamentali che hanno portato al fallimento del Gold Standard nel secolo scorso. Innanzitutto, il sistema BTC propone che il sistema economico e gli scambi internazionali dipendano da un bene che non possa essere influenzato dai provvedimenti di banche e governi. Il Gold Standard era stato adottato dalle

maggiori potenze economiche del XIX secolo per facilitare il commercio internazionale, vincolando la propria valuta nazionale all'oro e creando così un regime di cambi fissi. Gli stessi Stati lo avrebbero progressivamente abbandonato durante la Grande Depressione proprio per essere liberi di svalutare la propria valuta nazionale, nel disperato tentativo di far crescere le proprie esportazioni e di risollevare la propria economia. Anche in seguito alla sua reintroduzione con gli accordi di Bretton Woods, l'idea di una convertibilità in oro di ogni valuta sarebbe stata abbandonata definitivamente con lo Smithsonian Agreement del 1971 (dopo che gli USA di Nixon avevano sospeso la convertibilità del dollaro in oro sempre per la necessità di svalutare), sottolineando una nuova visione del ruolo del denaro nell'economia globale.

Per molti degli *early adopters* della criptovaluta, l'indipendenza del sistema BTC è una delle basi fondamentali del successo del bitcoin, spesso ignorando, come sottolinea Hadas (2014) in un articolo per il New York Times, che il denaro è uno strumento al servizio della società e che le istituzioni attuali delle principali economie mondiali prendono decisioni in materia di politica monetaria, per quanto criticabili e contestabili, per il bene della società (si veda sotto-capitolo 2.3).

1.4.2 Bitcoin come "commodity currency"

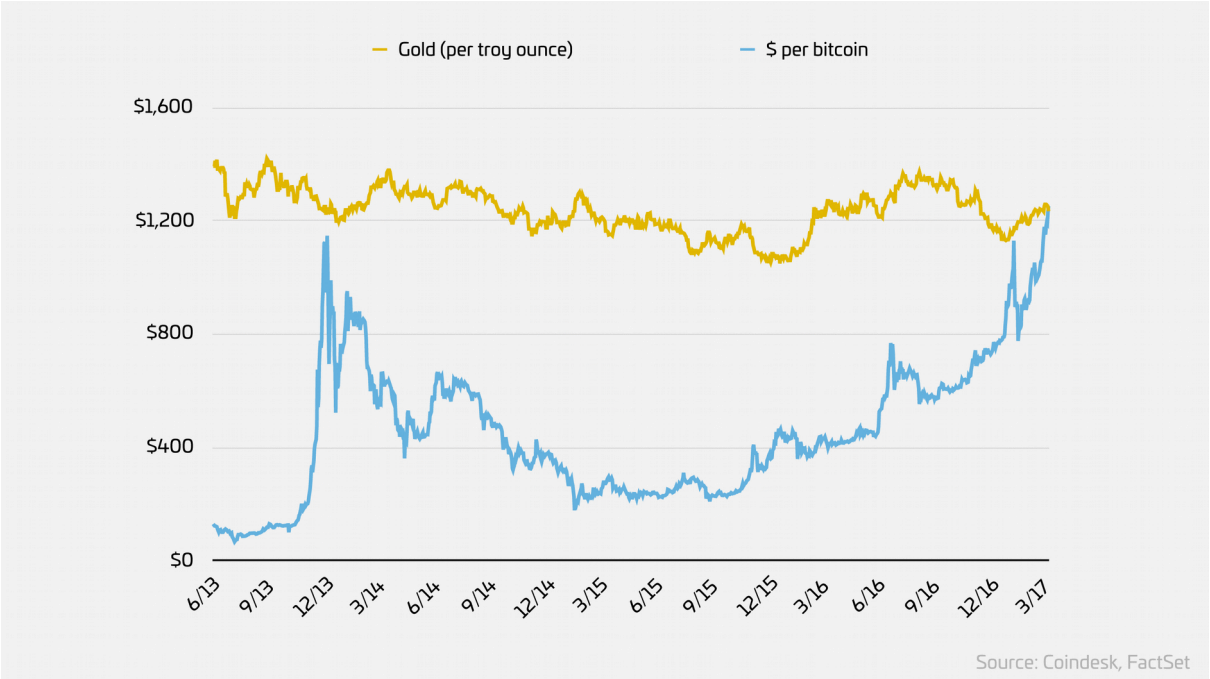
L'assenza di un'autorità centrale che controlli la circolazione della valuta, allontana ulteriormente il Bitcoin dal concetto di denaro che abbiamo riconosciuto e accettato negli ultimi secoli. Essendo inoltre non confiscabile e sovrannazionale, molti analisti tendono ad associarlo sempre di più ai metalli preziosi, arrivando a definirlo l'oro dell'età digitale, piuttosto che un nuovo tipo di moneta. Come l'oro, anche il Bitcoin non ha confini da rispettare, non rischia di deteriorarsi ed è una risorsa disponibile in quantità limitata; gli stessi utenti che permettono la creazione di nuovi bitcoin vengono definiti *miners*. I bitcoin, però, non possono essere utilizzati in ambiti diversi dai pagamenti e dalle transazioni, mentre l'oro, per le sue ben note proprietà fisiche, è utilizzato da secoli in applicazioni pratiche nei settori più diversi (dalla gioielleria all'alta tecnologia). Curiosamente, il prezzo del Bitcoin ha superato quello dell'oncia d'oro, nella prima metà del 2017 (si veda grafico 2.1), un dato che sottolinea ancora una volta il ruolo della domanda e dell'offerta nell'attribuzione del valore di un bene, al di là del valore intrinseco di quest'ultimo.

Nel suo articolo, Hadas sottolinea anche un punto debole non indifferente del Bitcoin rispetto

all'oro: mentre quest'ultimo è un bene tangibile, perfettamente in grado di sopravvivere alle peggiori crisi e anche a scenari "post apocalittici", il sistema BTC necessita del buon funzionamento di internet per poter funzionare correttamente, in caso contrario ogni transazione diventa impossibile da effettuare e il Bitcoin non ha più senso di esistere. L'oro ancora in circolazione è sopravvissuto a secoli di conflitti, pestilenze e rivoluzioni, Bitcoin potrebbe non avere le caratteristiche tecniche necessarie per farcela.

La condizione della criptovaluta ricorda curiosamente il caso del Dinaro Iracheno Svizzero , la valuta ufficiale dell'Iraq prima della Prima Guerra del Golfo (si veda Gimigliano 2016, p. 115). Quando tale valuta venne rimpiazzata, nel corso del conflitto, dal Dinaro di Saddam, il Dinaro Iracheno Svizzero continuò a circolare come mezzo di pagamento parallelamente alla nuova valuta e quando la moneta di Saddam iniziò a deprezzarsi (a causa della contraffazione e di una stampa eccessiva da parte del governo iracheno), il valore la vecchia moneta continuò a crescere fino a raggiungere un tasso di cambio pari a 300:1 nel 2003, sebbene ormai fosse completamente priva di valore legale, oltre che di valore intrinseco. In questo modo il Dinaro Iracheno Svizzero era di fatto diventato una "commodity currency", una condizione comparabile a quella del Bitcoin che, pur non essendo garantito da alcun governo o da alcuna merce, continua a circolare in quanto sono proprio è proprio chi lo utilizza gli attribuisce un valore.

Figura 1.2: andamento del prezzo dell'oro e del Bitcoin (in USD). Fonte coindesk.com



1.5 LE ALTRE CRIPTOVALUTE

In seguito al successo di Bitcoin, sono state create centinaia di criptovalute alternative, molte delle quali hanno tentato di risolvere i problemi tecnici dei bitcoin (in primis gli altissimi costi di generazione) proponendo cambiamenti strutturali, mentre molte altre sono di fatto delle semplici copie dei bitcoin e del sistema blockchain originali. La proliferazione di queste nuove valute è dovuta nella maggior parte dei casi alla speranza di facili profitti, nel caso in cui il prezzo della nuova valuta dovesse aumentare vertiginosamente come si è verificato con i Bitcoin, soprattutto considerando che questo genere di attività non richiede nè rilevanti investimenti iniziali nè, tanto meno, protocolli e regolamenti particolari da seguire. Il sistema Bitcoin originale, inoltre, è completamente open source.

In data 19 maggio 2017 , secondo Coin-MarketCap, Bitcoin detiene circa il 46% del mercato delle criptovalute ed è di gran lunga la più famosa e importante.

Tra le criptovalute che si sono diffuse maggiormente negli ultimi anni ci sono Litecoin, GeistGeld, SolidCoin e BBQcoin; queste valute vengono anche chiamate *altcoins*.

Litecoin, creato nel 2011 da Charles Lee, è stato concepito come una versione aggiornata e perfezionata del sistema Bitcoin: il nuovo algoritmo introdotto permette a qualsiasi utente di estrarre la valuta, con consumi di energia di gran lunga più efficienti. In questo modo, inoltre, l'intero sistema impedisce che solo gli utenti che dispongono di una elevatissima potenza computazionale possano trarre profitto dal sistema Litecoin; l'algoritmo permette anche di accorciare le transazioni. L'offerta finale e totale di moneta, inoltre, sarà pari a 84 milioni di unità (e quindi il quadruplo rispetto ai Bitcoin); tuttavia l'offerta, anche se più alta, è comunque limitata e questo non permetterà a Litecoin di evitare i problemi deflazionistici legati anche al sistema Bitcoin. Anche il Feathercoin, introdotto nel 2013 da Peter Bushnell, garantisce un'offerta di valuta che, anche se pari al quadruplo di quella dei Litecoin, è pur sempre limitata.

Criptovalute come Peercoin e Novacoin, invece, propongono un approccio completamente diverso con il sistema *proof-to-stake* come alternativa al *proof-to-work*: quando una unità della criptovaluta viene creata con successo, non viene premiato chi ha risolto il puzzle crittografico, ma viene distribuito una sorta di "dividendo" a tutte le unità già in circolazione, premiando chi ne detiene di più. Di fatto, però, anche nell'estrazione di queste criptovalute

sono gli utenti con hardware più potenti ad ottenere i risultati migliori.

Un caso interessante è quello di Ethereum Project (fondato nel 2014), che propone di utilizzare la tecnologia blockchain anche in ambiti diversi dai pagamenti online e completamente scollegati dall'ambito economico, ad esempio per garantire la sicurezza delle votazioni effettuate via internet. Simili potenziali applicazioni, sebbene l'intero progetto non sia ancora completo, hanno attirato l'attenzione di giganti del settore informatico come Microsoft e Intel, ma anche di società come Airbus e Toyota. Il prezzo della valuta di Ethereum, l'Ether, è cresciuto del 2700% dal mese di gennaio al maggio del 2017, arrivando addirittura a superare gli altissimi tassi di crescita del bitcoin nello stesso periodo (si veda Kharpal 2017).

A queste si aggiungono le cosiddette "digital currencies", tra le quali Liberty Reserve, WebMoney, Perfect Money e CashU, che però non sono basate sulla crittografia e devono obbligatoriamente essere acquistate ricorrendo ad un intermediario (anche se la maggior parte di esse cerca di garantire comunque all'utente il completo anonimato), rinunciando all'attrattività del principio di decentralizzazione. Con la sola eccezione di Litecoin ed Ethereum, però, tutte queste valute sono ancora scarsamente utilizzate in vere e proprie transazioni e i Bitcoin indubbiamente godono ancora dei vantaggi del *first-mover*, che in un ambito come questo potrebbero rivelarsi più rilevante della superiorità tecnologica.

Senz'altro la stragrande maggioranza delle criptovalute non sarà utilizzata in futuro e la crescita degli ultimi anni dell'intero settore è dovuta soprattutto alla massiccia speculazione. Molti utenti, infatti, acquistano decine di criptovalute diverse senza alcuna intenzione di utilizzarle come mezzo di scambio, aspettando di poterle rivendere a prezzi più alti in futuro.

CAPITOLO SECONDO: Le criptovalute e le istituzioni

2.1 LIBERTA' ED INDIPENDENZA DA GOVERNI E BANCHE CENTRALI

La possibilità di fare affari in tutto il globo senza l'ingombrante presenza dello Stato e della legge costituisce davvero una rivoluzione senza precedenti agli occhi di molti, non solo dal punto di vista economico e tecnologico, ma anche dal punto di vista politico. Non bisogna dimenticare che la criptovaluta è stata introdotta durante la crisi economica, in un clima di sfiducia sempre maggiore verso banche e governi in tutto il mondo. Tale pensiero, come sottolineato anche nel documento "Virtual currencies schemes" pubblicato dalla BCE (2012, p. 23) è in linea con quello della Scuola Austriaca, che giudicava negativamente l'intervento delle banche centrali e dei governi attraverso le politiche monetarie. La Scuola Austriaca, infatti, proponeva l'adozione di una tipologia di Gold Standard che impedisse alle banche di influenzare e manipolare l'economia reale con tassi d'interesse artificialmente troppo alti o troppo bassi. Nella sua breve storia la criptovaluta ha dimostrato di essere un fenomeno difficilmente controllabile e gestibile dalle istituzioni, confermando e rafforzando l'idea alla base del sistema BTC e della sua filosofia peer-to-peer: indipendenza da intermediari di qualsiasi genere.

Al di là delle opportunità libertarie offerte dai bitcoin, la criptovaluta potrebbe dimostrarsi un nuovo strumento fondamentale e realmente rivoluzionario per quanti nel mondo (soprattutto nei Paesi in via di sviluppo) non dispongono di un conto in banca, ma possiedono un telefono cellulare o altri dispositivi con connessione ad internet. Dalla nascita del sistema BTC, la diffusione degli smartphone e di internet a livello globale ha visto una crescita senza precedenti, portando cambiamenti radicali in tutto il mondo. La criptovaluta potrebbe essere un nuovo strumento per portare i pagamenti via internet e nuove opportunità di business non solo a chi non vuole, ma anche a chi non ha proprio la possibilità di ricorrere a un intermediario finanziario per portarli a termine (si veda Gimigliano 2016, p. 74).

2.2 BITCOIN E POLITICA MONETARIA

Uno degli obiettivi più ambiziosi del sistema BTC è quello di togliere ad un'autorità centrale il compito fondamentale dell'emissione di denaro. Agli occhi di molti, questo costituisce un'opportunità senza precedenti per tutelare gli interessi dei privati dalle imposizioni (spesso percepite come ingiuste) da parte dei governi e delle banche centrali. In questo modo, però, non c'è neppure un'autorità centrale che possa in qualche modo regolare i tassi di interesse su tale moneta per incrementare o meno consumi e investimenti e, quindi, influenzare fenomeni fondamentali come la disoccupazione e l'inflazione.

Quando le istituzioni condizionano l'economia attraverso politiche monetarie, agiscono con lo scopo di favorire l'andamento dell'economia attraverso l'offerta di moneta, che quindi viene modificata a seconda della condizioni in cui si trova il Paese. Come sottolineano i critici, il metodo con cui questa influenza viene esercitata non è una scienza esatta completamente priva di incertezze: l'intervento da parte delle istituzioni potrebbe avere effetti solo anni dopo e senza garanzie che verranno raggiunti gli obiettivi inizialmente prefissati. Oltre ad attuare le politiche ritenute necessarie, è fondamentale riuscire anche ad influenzare le aspettative riguardo al futuro, un obiettivo che si è storicamente dimostrato arduo da raggiungere. Le istituzioni, inoltre, potrebbero essere tentate di non adottare politiche monetarie necessarie ma estremamente impopolari e di preferire politiche con benefici di breve periodo, ma con gravi conseguenze nel lungo periodo. Storicamente un intervento scorretto da parte delle istituzioni ha portato a fenomeni estremi come l'iperinflazione, che anche se da decenni non sono più presenti nelle economie dei Paesi sviluppati, sono ancora caratteristici di molti Paesi in via di sviluppo.

Diversamente dalla quantità di *fiat currency*, il numero di bitcoin in circolazione è limitato e il suo valore non è in alcun modo controllabile, ma è stabilito dalla domanda e dall'offerta da parte degli utenti. I bitcoin, inoltre, non sono in alcun modo legati alla quantità di beni e servizi prodotti dall'economia di un Paese, ma solo alla quantità di beni e servizi prodotti da quanti utilizzano i bitcoin nelle transazioni. Se Bitcoin fosse l'unica moneta scambiata a livello globale, un Paese in crisi economica non avrebbe alcuna possibilità di attuare le politiche monetarie che sarebbero fondamentali per permetterne la ripresa.

Simili preoccupazioni si erano diffuse anche in passato, con l'introduzione di metodi di pagamento alternativi alla moneta legale: tali sistemi non hanno in alcun modo la possibilità di sostituire il ruolo fondamentale svolto dalla banca centrale attraverso le politiche monetarie, tantomeno una valuta che, come Bitcoin, rinuncia completamente a qualsiasi tipo

di autorità centrale. Come ha scritto Irwin, in un articolo per il Washington Post (2013) "*...bitcoin is a reminder of this fundamental truth: To function in a modern economy, you're always putting your faith in something, whether you like it or not. And you may not like putting that faith in a powerful, independent central bank imbued with power from the state, but the alternatives may just be a lot worse.*".

2.3 IL SISTEMA BTC E LE BANCHE CENTRALI

2.3.1 LA BCE

La BCE aveva iniziato ad analizzare il fenomeno delle cosidette *virtual currencies* già nella prima metà del 2011, prima che Bitcoin attirasse l'attenzione dei media. Nel 2012, la BCE ha pubblicato il rapporto "Virtual currency schemes″, nel quale viene presentato e analizzato il fenomeno delle valute virtuali. Tali valute vengono suddivise e classificate a seconda delle loro caratteristiche tecniche e dell'ambito in cui vengono utilizzate in tre gruppi fondamentali:

1. "closed virtual currency schemes", senza alcun legame con l'economia reale;
2. "virtual currency schemes with unidirectional flows", che possono essere acquistate con monete tradizionali, ma non possono essere riconvertite in denaro reale;
3. "virtual currency schemes with bi-directional flows", che possono anche vendute e acquistate in cambio di moneta legale.

Il Bitcoin, classificabile come moneta virtuale del terzo gruppo, viene descritto e presentato come *Case Study*. Le valute non vengono considerate una minaccia immediata per il sistema economico, per via della loro limitata diffusione e capitalizzazione (anche dopo l'enorme crescita degli ultimi anni, il valore complessivo dei bitcoin in circolazione è insignificante rispetto a quello delle monete avente corso legale). Allo stesso tempo, però, viene sottolineata la necessità di monitorare il numero di utenti attivi e la crescita di servizi connessi alle criptovalute. Viene inoltre ribadita più volte la necessità di regolamentare le varie monete virtuali per impedire che siano impiegate in attività illegali.
Il rapporto individua nelle valute virtuali una potenziale minaccia alla reputazione delle banche centrali, reputazione che ha un ruolo fondamentale nell'influenzare le aspettative e permettere alle politiche monetarie attuate di raggiungere gli obiettivi prefissati. Se le banche

centrali dovessero diventare oggetto di critiche a causa di gravi errori o negligenze, le valute virtuali potrebbero essere percepite da un numero sempre maggiore di utenti come strumenti alternativi e migliori.
Nel 2015, la BCE ha pubblicato un nuovo rapporto sul tema: "Virtual currency schemes – a further analysis". In soli tre anni, il sistema BTC era radicalmente cambiato e il numero delle valute virtuali in circolazione, ciascuna con le proprie caratteristiche distintive, era cresciuto enormemente (il rapporto parla di circa 500 criptovalute con caratteristiche simili ai bitcoin, in continuo aumento). Le criptovalute non vengono riconosciute come moneta proprio per la mancanza di una banca centrale che le controlli. Ne viene anche sconsigliato l'uso, in particolare negli acquisti (posizione condivisa anche da gran parte delle banche centrali a livello globale) sempre nel timore che possa favorire attività illegali. Viene, però, sottolineato che, con un'adeguata regolamentazione e con il supporto di grossi provider di servizi finanziari, le virtual currencies potrebbero raggiungere più rapidamente un maggior numero di utenti, risolvendo gradualmente molti dei maggiori problemi di queste valute.

2.3.2 La Fed

Janet Yellen, intervistata nel 2014 in seguito al collasso di Mt. Gox, ha dichiarato "*Bitcoin is a payment innovation that's taking place outside the banking industry. To the best of my knowledge there's no intersection at all, in any way, between Bitcoin and banks that the Federal Reserve has the ability to supervise and regulate. So the Fed doesn't have authority to supervise or regulate Bitcoin in anyway...*" (si veda Rushe 2014), pur riconoscendo la necessità di una maggiore regolamentazione non soltanto da parte degli USA, ma a livello globale. Successivamente, la Fed ha dichiarato che la tecnologia blockchain del sistema BTC presenta un potenziale notevole, con possibili applicazioni anche nell'innovazione delle transazioni finanziarie e nella cybersecurity (si veda Allison 2016), in grado di portare benefici in particolare nelle nazioni in via di sviluppo: un ulteriore prova del ruolo sempre più determinante dell'informatica nel settore finanziario.

2.4 BITCOIN E ATTIVITA' ILLEGALI

Inizialmente il sistema BTC è stato associato soltanto al lato oscuro della tecnologia moderna, al mondo sommerso del Dark Web, degli hacker e della criminalità organizzata 4.0. In effetti, una valuta che offre a chi la detiene la possibilità di fare acquisti illegali in tutto il mondo, nel più completo anonimato, ha immediatamente attirato l'attenzione degli utenti che ricorrevano al DarkWeb per acquistare beni illegali di varia natura. Simili potenzialità hanno suscitato la preoccupazione di praticamente tutti i governi del mondo, con timori riguardanti soprattutto il finanziamento del terrorismo e il riciclaggio di denaro sporco. Come ha dimostrato il caso WikiLeaks, i bitcoin sono anche un ottimo strumento per aggirare le leggi dei propri governi non solo per vendere sostanze stupefacenti nella parte opposta del mondo, ma anche per condurre attività economiche o raccogliere fondi in Paesi oppressi da regimi autoritari. Gli utenti possono effettuare acquisti con un livello di anonimato paragonabile a quello offerto dal semplice denaro contante, aggirando allo stesso tempo i limiti imposti dagli Stati sui pagamenti contro il riciclaggio (ad esempio in Italia con il limite dei 3000 euro). Bisogna considerare, però, che la stessa blockchain è un vero e proprio elenco open source di tutte le transazioni effettuate nella storia della criptovaluta. Anche se per la maggior parte degli utenti sarebbe estremamente complesso e oneroso cercare di tracciare e individuare gli autori delle transazioni, non è così per le istituzioni. Durante le indagini sul famigerato sito Silk Road, infatti, l'F.B.I. è stata in grado di identificare l'autore del sito riuscendo ad individuare e seguire i flussi di criptovaluta diretti verso il suo account.

I bitcoin, purtroppo, si sono anche dimostrati uno strumento eccellente per effettuare ricatti via internet senza che il ricattatore debba in alcun modo trasmettere i propri dati al ricattato, a parte il proprio codice per la ricezione dei bitcoin. Il 12 maggio 2017, il virus informatico "WannaCry" ha colpito i computer non aggiornati di aziende e organizzazioni di quasi 100 Paesi in tutto il mondo (si veda Pinotti 2017); gli autori del virus minacciavano gli utenti di cancellare tutti i dati contenuti nei computer bloccati, a meno che non fosse pagata loro una cifra pari a 300 dollari in bitcoin, fornendo nella richiesta di riscatto un indirizzo apposito per ricevere il pagamento. L'attacco, fino ad allora, è stato senza precedenti per il numero di utenti colpiti e ha rafforzato la credibilità della criptovaluta anche agli occhi di chi non ne aveva mai sentito parlare prima, contribuendo ancora una volta a riaccendere il dibattito in merito al suo status legale; del resto, è possibile che simili attacchi informatici possano verificarsi anche in futuro.

Agli occhi di molti utenti, come scrive De Angelis (2017) in un articolo de Il Sole 24 Ore

"*...le automobili sono usate per le rapine in banca, ma non é una buona ragione per vietarle e tornare alle carrozze...*". Inoltre, nonostante la crescita incredibile dell'economia Bitcoin degli ultimi anni, il suo peso nell'economia illegale è ancora infinitesimale e per attività come il riciclaggio di denaro sporco (per il quale il sistema BTC presenterebbe vantaggi notevoli) vengono utilizzati servizi finanziari "tradizionali".

2.5 REGOLAMENTAZIONE INTERNAZIONALE

Già nel 1816, Thomas Jefferson scriveva "*Laws and institutions must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths disclosed, and manners and opinions change with the change of circumstances, institutions must advance also, and keep pace with the times.*". Un simile obiettivo era ambizioso già due secoli fa, agli attuali livelli di innovazione e continue rivoluzioni su scala globale, la distanza tra le nuove tecnologie e la legge si fa sempre più marcata (si veda Wadhwa 2014).

Sono sempre più numerosi gli utenti della criptovaluta che auspicano un maggior livello di regolamentazione da parte dei legislatori di tutto il mondo. Secondo la maggior parte dei sostenitori del sistema BTC, le potenzialità di questa nuova tecnologia potranno essere davvero sfruttate su scala globale solo se verranno regolate in maniera adeguata.

I provider di servizi legati ai Bitcoin, in particolare, finora hanno sempre trovato difficoltà di natura legale nell'esercizio della propria attività. Alcune di queste società hanno ricavi per milioni di dollari, ma operano in un settore che non è ancora stato di fatto riconosciuto o neppure considerato dalla stragrande maggioranza dei legislatori: per queste società può rivelarsi problematico o addirittura impossibile ottenere prestiti, adeguata assistenza legale ecc.

Ulteriori controversie, sviluppatesi in particolare da quando i bitcoin si sono affermati come strumento speculativo, riguardano l'aspetto fiscale. Quando è stato introdotto, del resto, Bitcoin era stato soltanto concepito come un mezzo di pagamento, senza alcuna considerazione per fiscalità e altri aspetti legali. Ora la criptovaluta è sempre più utilizzata e diffusa, ma la stragrande maggioranza dei Paesi del mondo non ha ancora previsto una forma di tassazione adeguata.

Non bisogna dimenticare che il sistema BTC, grazie alla sua natura decentralizzata, potrà

funzionare anche senza l'approvazione da parte dei governi. Dal punto di vista tecnico, l'unico sistema per fermare le transazioni in bitcoin sarebbe chiudere internet. Indubbiamente, però, se i governi si schierassero contro la criptovaluta, cercando di limitarla o addirittura abolirla, potrebbero rallentarne la diffusione. Finora, i governi delle maggiori economia mondiali hanno adottato approcci diversi alla regolamentazione del sistema BTC, mentre in molti Paesi (come l'India e l'Italia) i legislatori non si sono ancora espressi sul tema; quanti si stanno occupando o si occuperanno di regolamentare la criptovaluta, dovranno considerare che una realtà come il sistema Bitcoin costituisce una sfida senza precedenti, in quanto potrebbe facilmente modificarsi anche nel giro di pochi mesi, rendendo facilmente obsolete legislazioni in materia.

2.5.1 Gli Stati Uniti

.

Negli USA, già nel novembre 2013 si erano tenute, in Senato, udienze in merito al sistema BTC: fin da subito ne sono stati discussi gli aspetti critici, senza avviarne però una vera e propria regolazione. Il Bitcoin è talmente diverso dalle fiat currencies e dai vari strumenti finanziari, che per i legislatori è un problema anche solo attribuire ad esso uno status dal punto di vista giuridico. Neli USA e in molti altri Paesi, i bitcoin sono considerati una commodity (si veda Baraniuk 2016) e proprio negli Stati Uniti il Department of Financial Services of the State of New York ha proposto di assegnare una *BitLicense* agli utenti della criptovaluta: una sorta di patente per cercare di regolare in qualche modo di sistema BTC, anzichè abolirlo o limitarlo. Un progetto, però, che si potrebbe rivelare estremamente difficoltoso da realizzare.

Gli USA sono tra i pochi Paesi ad aver cominciato a prevedere modalità per la tassazione dei bitcoin. Nel 2014, l'IRS ha pubblicato delle linee guida per tassare le criptovalute classificandole come *intangible property* (si veda Green 2017). L'imposta colpisce il capital gain generatosi in seguito alle transazioni (quando presente); tutti i soggetti residenti in America sono tenuti al pagamento dell'imposta indipendentemente da dove sia stata effettuata la transazione. Simili modalità di tassazione, per la natura dell'oggetto trattato, sono senza precedenti e potrebbero dimostrarsi estremamente complesse da attuare.

2.5.2 L'Europa

Nella maggior parte dei Paesi europei (tra i quali anche l'Italia), la priorità delle istituzioni è

stata quella di mettere in guardia gli utenti della criptovaluta dai rischi connessi al finanziamento del terrorismo e altre attività illegali e alla volatilità del prezzo; nonostante questo, in nessun Paese dell'Area Euro, i bitcoin sono stati ancora dichiarati illegali.
La criptovaluta non è ancora stata riconosciuta come moneta legale da nessuno Stato membro, in quanto non ne presenta i requisiti fondamentali.
Il Ministero delle Finanze tedesco, tuttavia, ha riconosciuto ai bitcoin lo status di *Rechnungseinheit*, ovvero di unità di conto che possono essere considerate strumenti finanziari; in altri Paesi, tra i quali la Svezia, le criptovalute sono al momento considerate degli asset.
Nel caso "Skatteverket v. David Hedqvist", la Corte di Giustizia Europea ha stabilito che la VAT non è applicabile sulla conversione degli euro in bitcoin: dal punto di vista fiscale la criptovaluta non viene considerata un bene da acquistare, ma un vero e proprio mezzo di scambio. Paesi come Estonia e Polonia, stanno cercando di tassare le attività di mining e di scambio di bitcoin.
In Italia l'Agenzia delle Entrate, con la risoluzione n. 72/e del 02/09/2016 (disponibile su www.agenziaentrate.gov.it) ha di fatto riconosciuto i bitcoin come mezzo di pagamento utilizzabile anche in atti notarili ufficiali e, dall'aprile del 2017, a Roma si possono acquistare legalmente 123 appartamenti mediante pagamento in bitcoin: si tratta del primo caso al mondo di abitazioni messe in vendita in cambio di criptovalute (si veda Moraca 2017). La risoluzione conferma l'esenzione ai fini dell'Iva delle conversioni di monete "tradizionali" in bitcoin.
Nell'aprile 2017, la Bank of England ha annunciato che darà il via a un piano di ampliamento dell'accesso al sistema interbancario dei pagamenti, tra i quali anche il Bitcoin sarà coinvolto.

2.5.3 La Cina

La Cina costituisce un caso particolare: il governo cinese aveva cercato di abolire ogni tipo di valuta digitale già del 2009, temendo che la loro diffusione avrebbe portato a una fuga incontrollabile di capitali all'estero. La Banca Popolare Cinese ha però consentito dal 2013 l'uso dei bitcoin, pur non riconoscendoli come moneta legale e proibendo alle banche di accettarli come valuta. La Cina è tutt'ora uno dei Paesi dove Bitcoin ha una maggiore diffusione, sia come mezzo di pagamento che come forma di investimento. Si stima che nel 2016 circa il 90% dei bitcoin in circolazione sia stato scambiato in Cina; anche se dall'inizio del 2017, con l'introduzione di norme anti riciclaggio più restrittive, il numero delle

transazioni in Cina è calato. Storicamente, il prezzo dei bitcoin è stato condizionato direttamente dai tentativi di regolamentazione da parte delle autorità cinesi. Senza dubbio, una diffusione globale della criptovaluta dipenderà significativamente da come sarà regolata dal governo cinese nei prosimi anni.

2.5.4 La Russia

La Federazione Russa, nel febbraio 2014, è stato uno dei pochi Paesi a cercare di mettere fuori legge il sistema BTC, accusato di essere uno strumento al servizio del terrorismo internazionale. Successivamente il divieto è stato però ritirato e adesso la banca centrale russa sta considerando l'idea di classificare i bitcoin e le altre criptovalute come beni digitali, tassandoli di conseguenza (si veda Suvorova 2017). La banca centrale ha anche sottolineato l'urgenza di una maggiore regolazione internazionale del fenomeno, per impedire che una crescita incontrollata della capitalizzazione di mercato del sistema BTC possa avere effetti negativi sui mercati finanziari. Le imposte previste andrebbero a colpire non solo il possesso e il trasferimento dei bitcoin, ma anche la loro generazione attraverso le attività di mining.

2.5.5 Il Giappone

Recentemente, uno sviluppo fondamentale è stata la decisione da parte del Giappone di legalizzare i bitcoin come mezzo di pagamento nell'aprile del 2017. Tale provvedimento ha permesso al Giappone di diventare uno dei protagonisti delle transazioni in bitcoin nel giro di pochi giorni e ha contribuito all'incredibile aumento del prezzo della criptovaluta nel maggio 2017. Nel giro di poche settimane, un numero sempre maggiore di business giapponesi regolari ha cominciato ad accettare pagamenti in bitcoin. Il governo giapponese ha dichiarato di vedere opportunità, piuttosto che minacce, in una maggiore diffusione della criptovaluta: una posizione ferma, diversamente dalle opinioni in materia della stragrande maggioranza degli altri legislatori a livello globale. La regolamentazione è stata sostenuta anche dalla Financial Services Agency (FSA) giapponese per venire incontro ai grandi investitori interessati alla tecnologia del sistema BTC e ai servizi ad esso legati (si veda Lewis 2017), ma finora scoraggiati dalla "anarchia" che caratterizzava il mondo delle criptovalute. Per esempio, le società che trattavano bitcoin, non sapendo come inserirli nei propri bilanci, spesso evitavano completamente di inserirli, con una inevitabile distorsione dei dati. Con il

"Crypto Currency Act", la FSA indica la nozione fondamentale di "criptovaluta", sottolineando il ruolo imprescindibile di una "electronic information processing organization" che ne regoli il trasfermento. Vengono inoltre indicate le linee guida fondamentali per la "Crypto Currency Exchange Industry", ovvero per l'insieme dei provider di servizi legati alle criptovalute: ora, tali società devono rispettare dei requisiti minimi di capitale al pari di provider di servizi finanziari tradizionali, sono tenute a redigere correttamente i propri bilanci e devono sottoporsi a periodiche revisioni contabili da parte società esterne qualificate (si veda IIMA 2017). Le autorità giapponesi vogliono evitare che eventi come l'attacco a Mt. Gox si possano ripetere e in questo modo viene garantita una tutela senza precedenti agli utenti della criptovaluta, anche se indubbiamente ne viene sacrificato il principio libertario.

2.6 OGGI: IL BITCOIN COME INVESTIMENTO SPECULATIVO

Oggi, la criptovaluta non è più al centro dei dibattiti solo per il suo impiego in attività illegali, ma anche per l'ascesa senza precedenti del suo prezzo. Durante il maggio 2017, il prezzo del Bitcoin ha superato i 2700 dollari, spinto da una crescente domanda nel mercato asiatico, dopo che nell'aprile 2017 il governo giapponese aveva approvato l'uso della criptovaluta come mezzo di pagamento legale (si veda Soldavini 2017). Ma, dopo una crescita del 45% del valore nell'arco di una sola settimana, il prezzo è diminuito di 300 dollari nel giro di poche ore e si sono verificate oscillazioni di prezzo superiori anche al 15% nell'arco di una sola giornata (si veda Cheng 2017).

Molti tra quanti stanno speculando sui bitcoin, pur sapendo che la criptovaluta è completamente priva di qualsiasi valore intrinseco e che il suo prezzo potrebbe scendere a zero in poche ore, continuano a detenerne e ad acquistarne perchè sanno che il valore del loro investimento potrebbe centuplicarsi nel giro di pochi anni, come si è verificato dal 2010 al 2017.

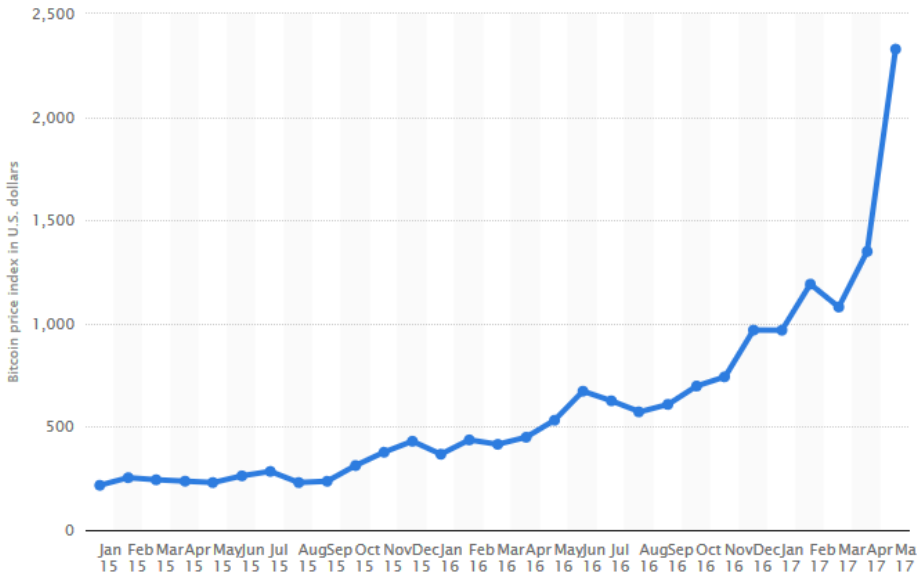
Risultati simili sono la vera causa del successo di criptovalute più recenti: la startup polacca Gnosis, nell'aprile 2017, ha raccolto ben 12 milioni di dollari in soli 12 minuti emettendo una propria criptovaluta per autofinanziarsi, come alternativa ai classici conferimenti di capitale da parte di *venture capitalists* (si veda Lops 2017). Dati apparentemente sconvolgenti come questi, sono comprensibili considerando il punto di vista di quanti investono in queste nuove valute. Nel peggiore dei casi, indubbiamente, perderanno quanto speso per acquistare la criptovaluta, nel migliore dei casi potrebbero guadagnare milioni nel giro di pochi anni:

difficilmente le azioni di una società regolarmente quotata potrebbero offrire simili prospettive di arricchimento facile e veloce. Quanti si stanno ancora mordendo le mani per non essere riusciti ad arricchirsi grazie ai bitcoin, hanno centinaia di nuove criptovalute che potrebbero avere performance anche migliori nei prossimi anni e in molti decidono di rischiare, più o meno consapevoli che potrebbero essere coinvolte in una nuova tipologia di Schema Ponzi, in cui non sono le opportunità di sviluppo futuro a giustificare la crescita del valore, ma soltanto la domanda sempre più alta di bitcoin per scopi esclusivamente speculativi.

Di fronte a un fenomeno simile, è inevitabile pensare che Bitcoin e molte delle criptovalute di maggior successo siano una bolla destinata a scoppiare (si veda Garber 2017), per molti il problema fondamentale è capire se si verificherà a breve o se davvero il prezzo di un singolo bitcoin è destinato a raggiungere il mezzo milione di dollari entro il 2030, come ipotizzato da Jeremy Liew (uno dei primi investitori dell'app Snapchat). Il miliardario Warren Buffett ha vivamente sconsigliato di investire in Bitcoin, definendo l'intero sistema "un miraggio". Buffett ha riconosciuto il potenziale tecnologico del sistema BTC come semplice mezzo per la trasmissione di denaro, privo però di qualsiasi valore intrinseco (si veda Kitonyi 2017).

Secondo molti sostenitori, la natura decentralizzata del Bitcoin dovrebbe essere una garanzia che l'intero sistema non è un semplice schema truffaldino: non c'è un organizzatore centrale che, una volta raggiunto il maggior profitto possibile, potrebbe semplicemente decidere di scappare con i soldi ottenuti. Senza contare che tutti coloro che hanno creato bitcoin, in particolare negli ultimi anni, prima di poterli rivendere hanno dovuto sostenere costi non indifferenti in elettricità e hardware.

Figura 2.1: Il prezzo dei bitcoin negli ultimi anni. Fonte: blockchain.info



CAPITOLO TERZO: Opportunità e criticità

3.1 PROBLEMI STRUTTURALI

3.1.1 Tempi di trasferimento

Come descritto in precedenza, affinchè il blocco contenente le transazioni possa essere aggiunto alla blockchain sono necessari almeno 10 minuti, che aumentano con l'aumentare del numero di transazioni: tali tempistiche, necessarie per il sistema affinchè sia garantita la sicurezza delle transazioni, sono percepite come una limitazione e suscitano preoccupazione per molti utenti (si veda Battanta 2017a). Infatti, una delle priorità delle criptovalute che sono state introdotte dopo i bitcoin è stata proprio la riduzione di queste tempistiche (Litecoin, ad esempio, è riuscita a ridurle a 2,5 minuti). In un mondo iperconnesso, dove gli utenti ricorrono alle nuove tecnologie aspettandosi di ottenere operazioni immediate, la velocità delle transazioni del sistema BTC è di gran lunga inferiore anche ai pagamenti tradizionali in contanti.
Come sottolinea il professor Ametrano in un'intervista de Il Sole 24 Ore (si veda Battanta 2017b), si sta verificando una progressiva divisione tra gli utenti che vorrebbero mantenere le transazioni nella loro condizione attuale (sacrificando velocità ed efficienza in cambio di una maggiore sicurezza e riservatezza) e tra quanti ritengono sarebbe necessaria una maggiore centralizzazione per la validazione delle transazioni che, anche se in parte tradirebbe il progetto originale del "peer-to-peer electronic cash system", permetterebbe di velocizzare il sistema dei pagamenti e al momento sembra l'alternativa più probabile. Basti pensare che, attualmente, il sistema BTC consente tre transazioni al secondo, mentre VISA arriva a circa 60000: condizioni che erano ammissibili quando i bitcoin erano poco più di un esperimento, cominciano a star strette a un fenomeno che ha raggiunto i livelli attuali di diffusione e rilevanza economica.

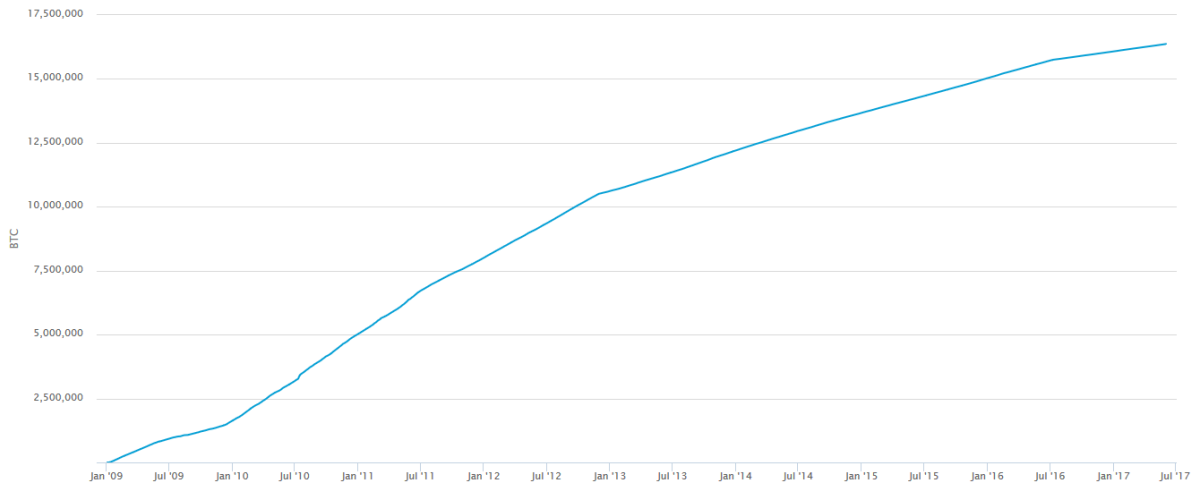
3.1.2 Limite dei 21 milioni di unità e deflazione

Il fatto che il numero complessivo di bitcoin estraibili sia limitato a 21 milioni, è stato

percepito da molti come una garanzia della tenuta del valore della criptovaluta: i bitcoin possono essere creati in numero limitato che, si stima, ai livelli attuali di estrazione sarà raggiunto attorno al 2140. Questo li rende una risorsa "scarsa", che prima o poi non potrà più essere creata. Questo aspetto fondamentale distingue radicalmente la criptovaluta dalle monete aventi corso legale, avvicinandola a minerali preziosi come l'oro ed è stato chiaramente introdotto per evitare i problemi legati all'inflazione che il ricorso una tipologia di valuta come questa (virtuale e priva di qualsiasi valore intrinseco) avrebbe potuto comportare.

Se in futuro il numero degli utenti del sistema BTC continuerà ad aumentare, una domanda maggiore di bitcoin accompagnata da un'offerta limitata, potrebbe causare un aumento del prezzo della criptovaluta. Gli utenti che già ne detengono, infatti, sarebbero spinti a evitare di scambiarli, preferendo aspettare che il valore dei propri bitcoin salga ulteriormente. Questo potrebbe portare a una spirale deflazionistica che, come illustrato prima, non potrebbe in nessun modo essere risolta attraverso apposite politiche monetarie, dato che la criptovaluta non può essere emessa o regolata da banche centrali.

Figura 3.1: numero complessivo di bitcoin creati. Fonte: blockchain.info



3.1.3 Il "51% hash power attack"

Questa fenomeno si potrebbe verificare nel caso in cui più della metà della potenza computazionale coinvolta nella regolazione delle transazioni in bitcoin finisse sotto il controllo di un unico utente che, in questo modo, otterrebbe il potere di regolare a proprio piacimento l'approvazione di tutte le transazioni.

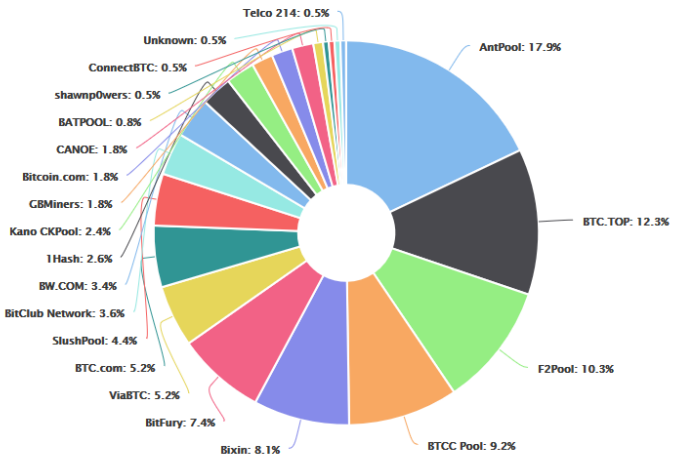
Tale utente potrebbe ad esempio, spendere due volte lo stesso bitcoin (compromettendo l'intera blockchain, garante crittografico contro il *double spending*) o addirittura impedire a tutti gli altri utenti di effettuare nuove transazioni, paralizzando l'intero sistema e rendendolo inutilizzabile. Un simile problema distingue in maniera ancora più radicale il Bitcoin da ogni altra forma di valuta tradizionale, per le quali fenomeni del genere sono considerati impossibili. Una simile eventualità, potenzialmente catastrofica, secondo molti utenti è destinata a rimanere puramente teorica anche nel lungo termine: arrivare a controllare una simile potenza computazionale richiederebbe investimenti iniziali elevatissimi e un continuo ed oneroso potenziamento dell'hardware utilizzato nelle operazioni di mining.

Negli ultimi anni, però, la necessità di ricorrere a macchine sempre più costose e performanti per ottenere profitti, sta spingendo un gran numero di piccoli miners fuori dal mercato, premiando un numero sempre più ristretto di utenti (si veda figura 3.2) e rendendo l'ipotesi di un "51% hash power attack" sempre meno improbabile. Nel 2014, la "mining pool" Ghash.io è arrivata a controllare per un breve periodo una percentuale pari a circa il 50% della potenza computazionale impiegata; anche se Ghash.io ha dichiarato di essere arrivata a simili livelli senza intenzioni ostili, ha dimostrato che una simile eventualità non è più semplice teoria, ma una potenziale minaccia a un sistema che ormai riguarda transazioni per miliardi di dollari.

Come scriveva lo stesso Nakamoto già nel 2009, tuttavia "*...if a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or by using it to generate new coins. He ought to find it moreprofi table to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth...*".

Figura 3.2: Percentuale di mercato dei gruppi di miners più popolari (data 02/06/2017).

Fonte: blockchain.info



3.1.4 Costi di generazione

Anche tra molti degli utenti più fedeli della criptovaluta, una delle maggiori critiche mosse verso il sistema BTC è legato agli elevati consumi di energia. Il processo di estrazione dei bitcoin è talmente complesso da richiedere una potenza computazionale e una quantità di energia tali da renderne economicamente poco vantaggiosa l'estrazione per la maggior parte degli utenti. Quanti nel mondo sono coinvolti attivamente nel processo di mining, infatti, hanno dovuto sostenere costi per l'acquisto di computer potenti adatti allo scopo, generalmente in località caratterizzate da una grande offerta di energia a basso costo come l'Islanda, dove ormai sono diffuse attività di estrazione su vastissima scala, grazie ai prezzi molto competitivi dell'energia elettrica (si veda Popper 2013). I profitti degli estrattori, chiaramente, saranno vincolati all'andamento del valore dei bitcoin. Se il prezzo al quale la criptovaluta viene scambiata dovesse scendere, come è successo in passato, tali utenti vedrebbero ridursi drasticamente i propri profitti anche nel giro di poche ore e potrebbero non essere più in grado di coprire le spese iniziali o addirittura di sostenere i costi dell'elettricità impiegata. Anche nel caso in cui il valore della criptovaluta continuasse a crescere, i miners sarebbero in competizione sempre maggiore tra di loro, in quanto il sistema BTC garantisce profitti maggiori per chi mette a disposizione una potenza computazionale anche leggermente superiore rispetto a quella dei competitors; allo stesso tempo, però, maggiore potenza computazionale comporta maggiori consumi in termini di energia.

Come ha scritto Paul Krugman nel suo articolo per il New York Times "Adam Smith Hates Bitcoin" (2013), la criptovaluta, al pari di materiali preziosi come oro e argento, richiede degli elevati costi di estrazione sia in termini di lavoro che di capitale, pur svolgendo una funzione simbolica (e quindi per la quale potrebbero essere scelti beni meno dispendiosi da ottenere), e causando quindi uno spreco di risorse che potrebbero essere applicate in ambiti diversi. Krugman sottolinea anche l'ironia della situazione: in un mondo le cui moderne tecnologie permettono una progressiva smaterializzazione del denaro come lo conosciamo, il sistema Bitcoin propone un nuovo utilizzo intensivo di risorse, che Adam Smith considerava inutile e superato già nel 1776.

3.2 SICUREZZA

Nonostante l'assenza di un intermediario qualificato che si occupi di gestire le transazioni, la blockchain si è dimostrata un eccellente sistema per regolarle, tanto che molti esperti prevedono che in futuro "libri mastri digitali" come il sistema blockchain potranno essere applicato anche in altri contesti, dove la tecnologia crittografica permetterà di garantire la massima sicurezza dei dati trattati senza la necessità di ricorrere a intermediari. Uno dei progetti più ambiziosi è quello legato alla cosiddetta *Liquid Democracy*, ovvero il progetto di diffondere a livelli sempre maggiori la democrazia diretta ricorrendo alla crittografia.

Uno dei maggiori problemi legati al denaro digitale, prima della nascita del sistema BTC, era dovuto ai rischi di falsificazione: in un sistema decentralizzato, il denaro potrebbe essere creato con la stessa facilità con cui creiamo la copia di un file. Basti pensare a fenomeni come la pirateria online di file musicali, che sono arrivati a rivoluzionare l'intero settore: è possibile per chiunque creare un numero pressochè infinito di copie illegali partendo da un singolo file regolarmente ottenuto. Grazie alla blockchain, è impossibile che un utente spenda lo stesso bitcoin due volte, rendendo impossibile qualsiasi forma di falsificazione o di errore nel trasferimento. Il Bitcoin non può essere falsificato in alcun modo e questo lo distingue da banconote, monete ecc, ma anche da metalli preziosi o vari beni rifugio. Non occorre rivolgersi a test o ad esperti che ne confermino l'autenticità: è il sistema blockchain a garantirla. Per la loro natura, i Bitcoin non necessitano di cassaforti, guardie armate e sistemi di videosorveglianza per essere conservati e trasportati con sicurezza, indipendentemente dall'ammontare di criptovaluta detenuta.

Molti utenti, tuttavia, sono sempre più preoccupati dall'eventualità di attacchi hacker su vasta scala (che si sono già verificati in passato, come nel caso di Mt. Gox citato in precedenza), tanto che sono sempre più diffusi servizi dove è possibile depositarli con maggiore sicurezza. Nei pagamenti online con valute tradizionali, infatti, il denaro depositato è garantito da un intermediario che, presumibilmente, dispone dei mezzi per difendersi da questo genere di attacchi, diversamente dalla maggior parte degli utenti privati. Negli ultimi anni si stanno diffondendo servizi come il "Bitcoin ETF" (ovvero Exchange-Traded Fund) proposto dai gemelli Winklevoss, permetterebbero agli investitori interessati alle opportunità offerte dal sistema BTC senza le competenze tecniche e i rischi di hacking legati al possesso della criptovaluta.

C'è sempre il rischio che i bitcoin vengano smarriti o dimenticati, infatti si sono verificati casi in cui degli utenti hanno perso vere e proprie fortune in hard disk andati distrutti o a causa di

password dimenticate. Sul sito internet www.bitcoin.org, agli utenti viene consigliato non solo di aggiornare frequentemente il software del proprio portafoglio elettronico, ma anche di fare in modo che i propri dati di accesso, in caso di morte improvvisa del proprietario, possano essere recuperati dai familiari.
Il sistema Bitcoin, non essendo ancora stato regolamentato adeguatamente, al momento non può fornire le garanzie e le tutele (risarcimenti in caso di furto ecc.) garantiti invece da altri intermediari finanziari.

3.3 DIFFUSIONE ED ECONOMIE DI RETE

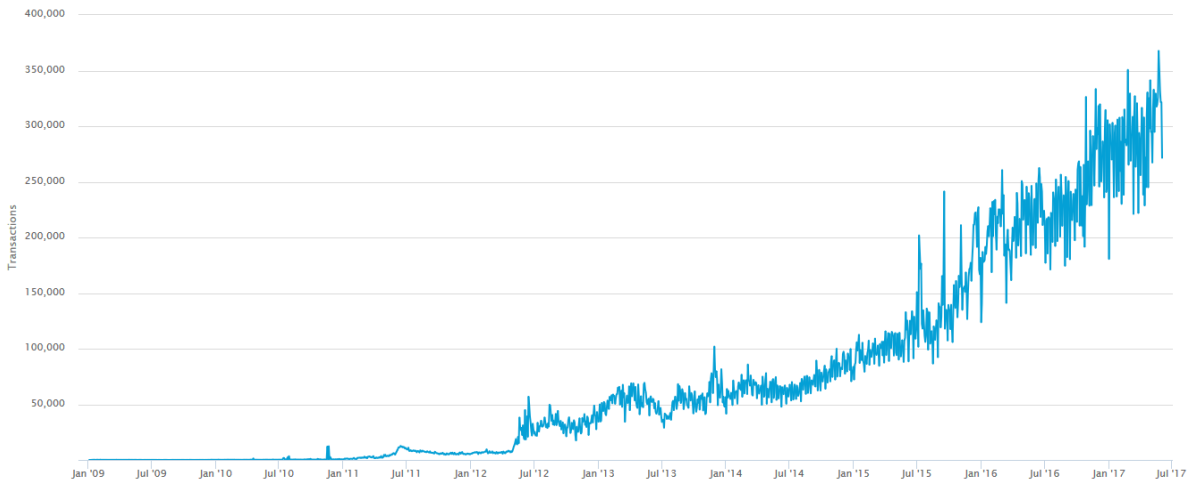
Negli ultimi anni, una delle priorità fondamentali di prodotti e servizi tecnologici altamente innovativi è stato il raggiungimento del maggior numero di utenti possibile in tempi limitati, per poter sfruttare al meglio i cosiddetti *network effects*: tale prodotto o servizio si rivela maggiormente profittevole se il numero degli utenti che lo adoperano è elevato e in crescita. Era stato così ai tempi della diffusione del telefono e lo è stato in tempi recenti con social network come Facebook, che inizialmente ha sacrificato i profitti pubblicitari per poter raggiungere una *critical mass* di iscritti che gli permettesse di affermarsi sul mercato.
Lo stesso principio si applica per una moneta avente corso legale. Durante il Rinascimento, il ruolo economico fondamentale di Firenze e Venezia, portò alla graduale diffusione in tutta Europa del fiorino e del ducato nelle transazioni commerciali: i mercanti preferivano essere pagate in valuta italiana e questo portò all'esclusione di numerose altre valute fino ad allora utilizzate. Quando nel 1773 venne introdotto il tallero di Maria Teresa, in onore dell'imperatrice austriaca, la moneta ebbe una diffusione e un successo tali che, anche dopo la morte dell'imperatrice, la moneta continuò ad essere coniata, in quanto in molti contesti era ormai diventata l'unica moneta accettata. Persino nel 1937, in seguito all'invasione dell'Abissinia da parte dell'Italia, le popolazioni locali rifiutavano qualsiasi genere di valuta sostitutiva, spingendo il governo fascista a coniare i propri talleri di Maria Teresa; richieste analoghe provenivano dalle popolazioni di gran parte delle colonie dell'epoca. Gli ultimi talleri sarebbero stati dal governo austriaco nel 1975, ovvero oltre due secoli dopo la loro introduzione iniziale.
Sotto questo aspetto, le valute del passato non sono troppo diverse dai bitcoin: quando e se questi ultimi saranno riconosciuti e accettati da un maggior numero di soggetti come moneta

per le transazioni, allora ulteriori soggetti saranno incentivati ad utilizzare la criptovaluta. Di fronte a un sistema talmente rivoluzionario come quello BTC, bisogna inoltre considerare che le innovazioni radicali, per quanto vantaggiose e prive di elevati *switching costs*, spesso incontrano diffidenza e perplessità da parte dei consumatori. In Occidente, perfino le banconote impiegarono tempi lunghissimi per diffondersi, sebbene fossero indubbiamente più pratiche e comode da trasportare delle tradizionali monete in metallo e anche le carte di credito, negli ultimi decenni, hanno raggiunto un numero così elevato di utenti anche grazie alla spinta degli istituti bancari, piuttosto che in seguito a vere e proprie richieste da parte dei consumatori. Allo stesso tempo, se le carte di credito e di debito non si fossero diffuse, i consumatori non avrebbero potuto beneficiare dei vantaggi offerti di questa tecnologia che si sono sviluppati anche negli anni successivi (possibilità di acquisti online ecc.).

Attualmente, la scarsa diffusione dei bitcoin e in particolare il fatto che vengano utilizzati raramente nelle transazioni commerciali, è considerato uno dei maggiori limiti della criptovaluta. Il numero complessivo delle transazioni in bitcoin è in aumento (si veda figura 3.2), ma si stima che la stragrande maggioranza di queste transazioni si verifichi in Cina e negli Stati Uniti, mentre in molte aree del mondo è quasi completamente inutilizzato.

Figura 3.2: numero di transazioni in bitcoin giornaliere confermate.

Fonte blockchain.info



3.4 VOLATILITA'

Molti potenziali utenti di Bitcoin sono scoraggiati dalla criptovaluta proprio a causa della sua estrema volatilità: negli ultimi dieci anni, il valore della moneta virtuale è passato da pochi centesimi a circa 1800 euro, con massicce oscillazioni che hanno portato anche al dimezzamento del proprio valore nell'arco di una settimana (come nel caso dell'attacco hacker a Mt.Gox nel 2014).

Intermediari come Coinbase (si veda Rampini 2013) propongono servizi di "hedging" alle maggiori società interessate ai Bitcoin: ricorrendo a strumenti finanziari come derivati, Coinbase riesce ad isolare i bitcoin nei portafogli elettronici dai rischi di eccessive fluttuazioni di prezzo. In questo modo, però, gli utenti sono costretti ad affidarsi ad un intermediario (anche se differente da quelli tradizionali) che offra questo genere di servizi finanziari, "tradendo" il concetto di peer-to-peer electronic cash system. I derivati, in particolare, sono stati tra i protagonisti dell'ultima crisi finanziaria e godono di una pessima reputazione da parte dell'opinione pubblica, che li considera uno dei simboli dell'avidità delle banche e della scarsa trasparenza degli istituti finanziari verso i clienti.

Per quanti sono interessati alla criptovaluta esclusivamente come strumento di pagamento e non come mezzo di speculazione, la soluzione più immediata rimane ancora la rapida conversione dei bitcoin (dopo ogni transazione) in moneta avente corso legale, ricorrendo a provider di servizi di cambiovaluta.

3.5 CONCLUSIONI E POSSIBILI SVILUPPI FUTURI

Il sistema BTC è un fenomeno che indubbiamente non può più essere ignorato o sottovalutato e non solo dalle istituzioni e dagli informatici. Indipendentemente dal suo sviluppo futuro, Bitcoin ha presentato un nuovo concetto di denaro, rispetto a quello che l'umanità ha conosciuto e accettato per millenni, ma è ancora presto per stabilire se questa nuova visione delle transazioni e dei pagamenti sia davvero destinata a cambiare il mondo. Senza dubbio presenta problemi e caratteristiche intrinseche che potrebbero renderne impossibile la grande diffusione su scala globale, ma visti i risultati incredibili (e imprevedibili) ottenuti nel giro di pochi anni, nessuno può davvero prevedere con certezza come questa realtà si evolverà in

futuro.

Bitcoin ha saputo dimostrare le incredibili potenzialità di un'idea rivoluzionaria resa reale e funzionante non solo grazie alla tecnologia, ma soprattutto grazie agli utenti che l'hanno resa possibile e contribuiscono al suo sviluppo. L'introduzione del sistema blokchain, in particolare, ha dimostrato un potenziale che altri soggetti nei settori più diversi (come si è già verificato, ad esempio, con Ethereum) hanno già cominciato a sfruttare, permettendo di rivoluzionare le transazioni grazie alle possibilità offerte del mondo interconnesso.

Un tale risultato non può essere liquidato come un semplice Schema Ponzi, anche se la massiccia speculazione degli ultimi anni ha indubbiamente cambiato il modo in cui i bitcoin vengono considerati dall'opinione pubblica, visti come opportunità per fare soldi facili piuttosto che come mezzo di scambio. La rapidissima evoluzione delle criptovalute nell'arco degli ultimi dieci anni è una dimostrazione delle potenzialità illimitate delle moderne tecnologie applicate al transazioni di denaro e, anche se la rivoluzione politica ed economica proposta da Bitcoin sembra ancora un traguardo molto lontano, non si può escludere che nei prossimi anni i bitcoin avranno un ruolo sempre più rilevante a fianco delle valute tradizionali.

Bibliografia (in ordine alfabetico)

AGENZIA DELLE ENTRATE, 2016. Risoluzione n. 72/e del 02/09/2016

ALLISON, I., 2016. *Federal Reserve Chair Janet Yellen meets with blockchain experts in Washington DC* [online], 6 giugno. Disponibile su <http://www.ibtimes.co.uk/federal-reserve-chair-janet-yellen-meets-blockchain-experts-washington-dc-1563970> (Data di Accesso 04/06/2017)

BARANIUK, C., 2016. *Bitcoin: Is the crypto-currency doomed?* [online], 19 gennaio. Disponibile su <http://www.bbc.com/news/technology-35343561> (Data di Accesso: 20/04/2017)

BATTANTA, L., 2017a. Bitcoin, la cripto-valuta vittima del suo successo. *Il Sole 24 Ore* [online], 31 marzo. Disponibile su <http://www.ilsole24ore.com/art/finanza-e-mercati/2017-03-31/bitcoin-crypto-valuta-vittima-suo-successo--135605.shtml?uuid=AEDtx9w> (Data di Accesso: 20/04/2017)

BATTANTA, L., 2017b. Chi governa il bitcoin? Tredici domande per capire quale vincerà tra le visioni a confronto. *Il Sole 24 Ore* [online], 5 aprile. Disponibile su <http://www.ilsole24ore.com/art/finanza-e-mercati/2017-04-05/chi-governa-bitcoin-tredici-domande-capire-quale-vincera-le-visioni-confronto-131100.shtml?uuid=AEqPCqz> (Data di Accesso: 20/04/2017)

BILTON, N., 2013. Disruptions: Betting on a Coin With No Realm. *The New York Times* [online], 22 dicembre. Disponibile su <https://bits.blogs.nytimes.com/2013/12/22/disruptions-betting-on-bitcoin/?_r=0> (Data di accesso 24/05/2017)

CHENG, E., 2017. *Bitcoin plunges more than $300, goes negative after earlier hitting all-time high* [online], 25 maggio. Disponibile su <http://www.cnbc.com/2017/05/25/bitcoin-surges-10-percent-to-all-time-high-above-2700.html>
(Data di accesso 25/05/2017)

DE ANGELIS, T., 2017. Sei comuni errori dei giornalisti sul bitcoin. *Il Sole 24 Ore* [online], 4 agosto. Disponibile su <http://www.econopoly.ilsole24ore.com/2017/04/08/sei-comuni-errori-dei-giornalisti-sul-bitcoin/> (Data di accesso 23/04/2017)

EUROPEAN CENTRAL BANK, 2012. "Virtual currency schemes". Disponibile su <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

EUROPEAN CENTRAL BANK, 2015. "Virtual currency schemes – a further analysis". Disponibile su <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>

GARBER, G., 2017. *Bitcoin just soared to a new $1,600 high — but the first investor in Snapchat thinks it could hit $500,000 by 2030* [online], 4 maggio. Disponibile su <http://www.businessinsider.com/bitcoin-price-could-be-500000-by-2030-first-snapchat-investor-says-2017-3?IR=T> (Data di accesso 26/05/2017)

GIMIGLIANO, G., a cura di., 2016. *Bitcoin and Mobile Payments: Constructing a European Union Framework*. Londra: Palgrave Macmillan

GREEN, A., 2017. If You Traded Bitcoin, You Should Report Capital Gains To The IRS. *Forbes* [online], 21 febbraio. Disponibile su <https://www.forbes.com/sites/greatspeculations/2017/02/21/if-you-traded-bitcoin-you-should-report-capital-gains-to-the-irs/#78ab1105e3d8> (data di accesso 04/06/2017)

HADAS, E., 2014. Bitcoin a Fool's Gold Standard. *The New York Times* [online], 22 gennaio. Disponibile su <https://dealbook.nytimes.com/2014/01/22/bitcoin-a-fools-gold-standard/> (Data di accesso 26/05/2017)

HALABURDA, H. e SARVARY , M., 2016. *Beyond Bitcoin: The Economics of Digital Currencies*. Londra: Palgrave Macmillan

IIMA, 2017. "Enforcement of Japanese Law on Crypto Currency and Future Issues". Disponibile su <http://www.iima.or.jp/Docs/column/2017/0410_e.pdf.>

IRWIN, N., 2013. Bitcoin is ludicrous, but it tells us something important about the nature of

the money. *The Washington Post* [online], 12 aprile. Disponibile su <https://www.washingtonpost.com/news/wonk/wp/2013/04/12/bitcoin-is-ludicrous-but-it-tells-us-something-important-about-the-nature-of-money/?utm_term=.f15ecc4bf116> (Data di Accesso: 20/04/2017)

KHARPAL, A., 2017. *Ethereum is headed for a 38% correction after big price rally, analyst says* [online], 26 maggio. Disponibile su <http://www.cnbc.com/2017/05/26/ethereum-price-correction-bitcoin.html> (Data di accesso 26/05/2017)

KITONYI, N., 2017. Is Warren Buffett Wrong About Bitcoin? [online], 17 gennaio. Disponibile su <https://finance.yahoo.com/news/warren-buffett-wrong-bitcoin-205400770.html> (Data di accesso 26/05/2017)

KRUGMAN, P., 2013. Adam Smith Hates Bitcoin. *The New York Times* [online], 12 aprile. Disponibile su <https://krugman.blogs.nytimes.com/2013/04/12/adam-smith-hates-bitcoin/> (Data di Accesso: 20/04/2017)

LEWIS, L., 2017. Japan eyes prize in regulating bitcoin. *Financial Times* [online], 17 maggio. Disponibile su <https://www.ft.com/content/f102c906-3a23-11e7-821a-6027b8a20f23> (Data di Accesso: 12/06/2017)

LOPS, V., 2017. Bitcoin clone raccoglie 12 milioni in 12 minuti. *Il Sole 24 Ore*, 18 maggio, 5.

MORACA, S., 2017. L'Italia è il primo paese in cui puoi comprare una casa con i bitcoin. *Wired* [online], 5 aprile. Disponibile su <https://www.wired.it/economia/finanza/2017/04/05/prima-casa-bitcoin/> (Data di accesso: 26/05/2017)

NAKAMOTO, S., 2009. *Bitcoin: A Peer-To-Peer Electronic Cash System.* Disponibile su <www.bitcoin.org> (Data di Accesso: 19/04/2017)

PINOTTI, F., 2017. Hacker, allarme globale «Mai un colpo così» Ferma anche la Renault. *Il Corriere della Sera*, 14 maggio, 11-12.

PLATEROTI, A., 2017a. *Banche centrali, guerra ai Bitcoin* [online], 23 febbraio. Disponibile su <http://www.ilsole24ore.com/art/finanza-e-mercati/2017-02-23/banche-centrali-guerra-bitcoin-214809.shtml?uuid=AEsnwUa> (Data di accesso 23/04/2017)

PLATEROTI, A., 2017b. Da Nakamoto a Wright: chi si cela dietro l'inventore. *Il Sole 24 Ore* [online], 24 febbraio. Disponibile su <http://www.ilsole24ore.com/art/finanza-e-mercati/2017-02-23/da-nakamoto-wright-chi-si-cela-dietro-l-inventore-220157.shtml?uuid=AEezWQb> (Data di accesso 26/05/2017)

POPPER, N., 2013. Into the Bitcoin Mines. *The New York Times* [online], 21 dicembre. Disponibile su <https://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines/> (data di accesso 08/05/2017)

RAMPINI, F., 2013. Il volo del Bitcoin e la sfida alla volatilità. Così la moneta virtuale è diventata reale. *La Repubblica* [online], 23 novembre. Disponibile su <http://www.repubblica.it/economia/2013/11/23/news/bitcoin_moneta_virtuale_internet-71714714/> (Data di accesso 08/05/2017)

RUSCONI, G., 2017. Bitcoin ai valori massimi ma le startup non sfondano. *Il Sole 24 Ore,* 19 maggio, 31.

RUSHE, D., 2014. 27 febbraio. Janet Yellen: Federal Reserve has no authority to regulate Bitcoin. *The Guardian* [online]. Disponibile su <https://www.theguardian.com/business/2014/feb/27/janet-yellen-federal-reserve-no-authority-regulate-bitcoin> (Data di accesso 04/06/2017)

SOLDAVINI, P., 2017. Il bitcoin non si ferma più: raddoppiato da inizio anno. *Il Sole 24 Ore*, 23 maggio, 23.

SUVOROVA, N., 2017. *Russian Central Bank Suggests Tax on Bitcoins* [online], 30 maggio. Disponibile su <https://www.bna.com/russian-central-bank-n73014451627/> (Data di accesso

04/06/2017)

VALSANIA, M., 2017. Bitcoin, nuovi record ad altissima volatilità. *Il Sole 24 Ore*, 27 maggio, 22.

WADHWA, V., 2014. Laws and Ethics Can't Keep Pace with Technology [online], 15 aprile. Disponibile su <https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/> (Data di accesso 01/06/2017)

Conteggio parole (esclusa bibliografia): 11597 parole.