Università
Ca'Foscari
Venezia

Corso di Laurea magistrale
(*ordinamento ex D.M. 270/2004*)
in Amministrazione Finanza e Controllo

Ca' Foscari
Dorsoduro 3246
30123 Venezia

Tesi di Laurea

Bitcoin

Analisi tecnica ed economica

Relatore
Ch. Prof. Marco Corazza

Laureando
Alberto Zen
Matricola 821411

Anno Accademico
2014/2015

INDICE

a. INTRODUZIONE

Cosa sono i Bitcoin? Sono la prima valuta digitale decentralizzata. La novità, anche se ormai questa valuta è in circolazione dal 2009, non è tanto nella digitalizzazione dei pagamenti, a cui tutti ormai, nell'era di Internet, siamo abituati, quanto al fatto che sia decentralizzata. Diversamente da tutte le monete tradizionali i bitcoin sfuggono a qualsiasi autorità: a coniarli non ci pensa la zecca dello Stato e non c'è alcuna Banca Centrale che ne controlli il valore né un intermediario finanziario che ne convalidi le transazioni.

Nato con l'intento di rendere più sicure e veloci le transazioni su internet, Bitcoin è un sistema per le transazioni elettroniche che non si basa più sulla fiducia in un'autorità terza, ma sulla matematica e sulla crittografia. La Banca centrale è sostituita dalla rete Bitcoin, un network di tipo *peer-to-peer*[1] (p2p) a cui tutti possono partecipare, a patto che si installi nel proprio computer il software omonimo, che è libero ed *open-source*[2], anche se è necessaria un'elevata potenza di calcolo. I nodi del network, facendo "girare" il software all'interno dei propri dispositivi, contribuiscono in modo diffuso a convalidare e registrare le transazioni tra due utenti che si vogliono scambiare delle unità di questo nuovo tipo di valuta, garantendone inoltre l'anonimato grazie alla crittografia insita nel sistema.

L'attività di validazione e registrazione delle transazioni è detta "*mining*", in italiano minare, un termine che ricalca metaforicamente l'attività di estrazione dell'oro da una miniera, e i nodi che la svolgono sono chiamati appunto "minatori". Tale attività sfrutta la potenza computazionale dei dispositivi dei minatori, ed è remunerata attraverso bitcoin[3] di nuova emissione, secondo un preciso sistema di ricompense.

[1] Peer-to-peer(p2p) o rete paritetica: architettura di rete informatica in cui I nodi sono tra loro paritetici, potendosi comportare sia da client che da server.
[2] Open source: software di cui gli autori rendono pubblico il codice sorgente, permettendone lo sviluppo a chiunque.
[3] Comunemente Bitcoin indica il sistema di pagamento, mentre bitcoin indica la valuta scambiata attraverso tale sistema.

Sono oltre 14 milioni i bitcoin in circolazione al momento (blockchain.info), mentre il valore di 1 BTC oggi[4] è di 236,45$. Tale prezzo è determinato dal mercato, ovvero dal meccanismo della domanda e dell'offerta, tuttavia è caratterizzato da una forte volatilità.

Lo scopo di questo elaborato è fornire un'analisi tecnica ed economica di questo innovativo sistema per i pagamenti. Il primo capitolo sarà dedicato a una presentazione del fenomeno Bitcoin, descrivendone le caratteristiche e le modalità di utilizzo. Nel secondo capitolo saranno approfonditi gli aspetti tecnici alla base del funzionamento del sistema. Nel terzo capitolo verranno approfonditi gli aspetti economici di Bitcoin, mettendone in luce i vantaggi e gli svantaggi derivanti dal suo utilizzo, considerandone infine le prospettive future.

[4] Data di rilevazione del prezzo: lunedì 18 maggio 2015 (Fonte: blockchain.info).

1 COS'È BITCOIN?

Usare bitcoin può sembrare facile come spedire e ricevere delle e-mail, capirne tutte le sfaccettature può risultare invece molto complicato, a seconda del grado di analisi cui si vuole pervenire. Le discipline interessate sono molteplici, tuttavia "*Non c'è nulla a cui lo [Bitcoin] si possa paragonare*", dice il suo stesso ideatore Satoshi Nakamoto[5].

1.1 Cos'è Bitcoin?

"*Bitcoin è la prima valuta digitale decentralizzata*", dice il famoso video introduttivo di bitcoin.org, sito di riferimento della comunità Bitcoin, "*Un'innovativa rete di pagamento e un nuovo tipo di denaro*". Già da queste prime considerazioni si capisce come la parola Bitcoin racchiuda molteplici concetti.

Bitcoin (con la "B" maiuscola) è una rete di pagamento virtuale, ideata per velocizzare e rendere più sicure le transazioni su internet. All'interno di questo network viene scambiato un nuovo tipo di valuta, diverso dalle valute tradizionali a cui siamo abituati: i bitcoin (con la "b" minuscola). Diversità e innovazione risiedono nel fatto che questa "valuta" è decentralizzata, cioè manca un'unità organizzativa centrale che la controlli e ne gestisca l'emissione. La Banca Centrale Europea (BCE) è l'ente centrale che controlla l'euro attraverso l'attuazione della politica monetaria nei paesi dell'Euro Zona, similmente la Federal Reserve (Fed) controlla il dollaro statunitense, mentre in Bitcoin manca un soggetto adibito a tale controllo, sia questi un ente pubblico o privato. Come se non bastasse le transazioni di bitcoin non necessitano di appoggiarsi ad alcuna istituzione finanziaria che funga da terzo garante, presenza essenziale nel commercio online con scambi in valute tradizionali.

[5] Si tratta di un post di Satoshi Nakomoto nell'ambito di una discussione su bitcointalk.org, forum di riferimento per la comunità Bitcoin. Il post è del 5 luglio 2010 e recita: *"Sorry to be a wet blanket. Writing a description for (bitcoin) for general audiences is bloody hard. There's nothing to relate it to*" (Fonte: crypt.la/2014/01/06/satoshi-nakamoto-quotes, data ultima consultazione 18/05/'15).

Tuttavia il controllo c'è, eccome. Tale controllo è diffuso e distribuito nella rete, garantito dall'adesione ad un protocollo comune, un insieme di regole che definiscono il funzionamento del sistema, che si esplica nell'utilizzo del software Bitcoin. Ogni nodo del network, cioè ogni dispositivo hardware su cui lavora il software Bitcoin, e in grado di comunicare in rete con gli altri dispositivi, diventa un soggetto attivo nel processo di gestione della valuta, e tanto più numerosi sono i nodi tanto più il concetto di decentralizzazione è significativo. Si faccia attenzione che per utilizzare i bitcoin, per comprare prodotti o servizi online o semplicemente per inviare del denaro ad un amico o parente, non è necessario essere un nodo di Bitcoin. I nodi sono necessari affinché le transazioni in bitcoin siano possibili, ma per i semplici utilizzatori della valuta non è obbligatorio partecipare attivamente alla rete, basta soltanto crearsi un indirizzo Bitcoin, simile ad un account per le e-mail.

Poiché il protocollo e il software sono stati comunque ideati e rilasciati dallo stesso inventore di Bitcoin, Satoshi Nakamoto, qualche scettico potrebbe benissimo sostenere che è il suo stesso ideatore l'autorità centrale, questione che si smentisce immediatamente considerando la natura libera e open-source del progetto. Bitcoin si pone infatti come aperto agli sviluppatori che vogliano apportare delle migliorie al progetto, tuttavia agli stessi sviluppatori risulta quasi impossibile forzare un profondo cambiamento del protocollo, in quanto ogni nodo è libero di scegliere quale software o versione utilizzare, al patto che siano conformi alle stesse regole e risultino compatibili con i software utilizzati dagli altri nodi. Quest'ultima caratteristica palesa la necessità di un consenso tra utilizzatori e sviluppatori affinché il sistema funzioni correttamente, e conseguentemente risulta assai arduo il tentativo di centralizzare il sistema, ovvero attribuire poteri regolamentari ad un'autorità centrale. Inoltre le qualità di risorsa libera ed aperta, se da un lato hanno aperto la strada allo sviluppo di nuove valute concorrenti sulla falsa riga di Bitcoin, dall'altro risultano essere fondamentali per la maturazione dell'intero sistema, grazie al considerevole valore intellettuale apportato da sviluppatori ed esperti di tutto il mondo.

In sintesi, si può dire che Bitcoin è un nuovo sistema di pagamento, in cui il controllo è distribuito e diffuso in maniera decentralizzata fra i nodi della rete, che facendo girare un apposito software regolato da uno specifico protocollo, rende possibili transazioni elettroniche in una nuova valuta digitale, i bitcoin. Bitcoin infine è un network, un

protocollo ed anche una tecnologia che rende possibile il funzionamento di un sistema innovativo.

1.2 Caratteristiche di bitcoin e principali differenze con le valute legali

Il report della BCE "*Virtual Currency Scheme*" di ottobre 2012 definisce come moneta legale (moneta *fiat*) 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.

La valuta bitcoin viene ricompresa all'interno della 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. Ci diversi tipi di monete virtuali a seconda della loro possibilità di interagire con il mondo reale, intesa come la possibilità di scambiarle con delle monete legali ad uno specifico tasso di cambio o di potervi acquistare beni e servizi nell'economia reale. La *figura 1.1* illustra i tre tipi valuta virtuale classificati dalla BCE; i bitcoin, potendo essere sia comprati che venduti in cambio di moneta legale, e potendo essere utilizzati per l'acquisto di beni e servizi, sono ricompresi all'interno dei sistemi di valuta virtuale di terzo tipo.

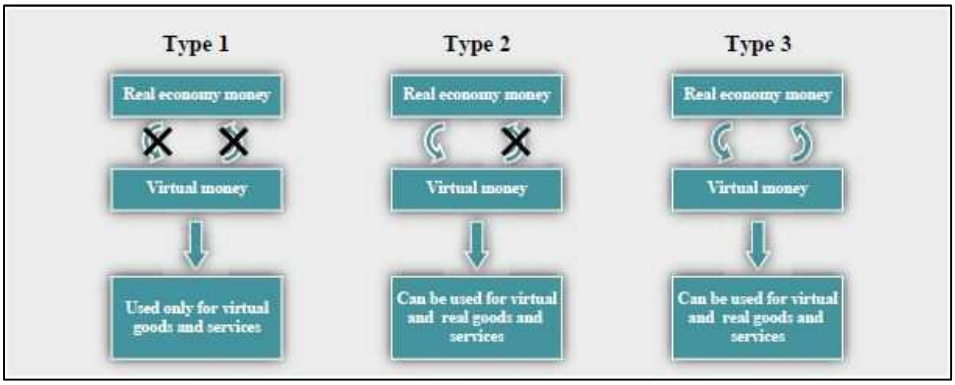

Figura 1.1: i diversi tipi di moneta virtuale (Fonte: BCE, ottobre 2012).

Per essere più precisi di quanto non abbia fatto la BCE nel suo report, bitcoin assieme ad altre valute simili nate a partire dal 2009 sono da ricomprendersi all'interno della categoria delle criptovalute. Le criptovalute 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.

Le principali caratteristiche di bitcoin sono:

- **Decentralizzazione:** bitcoin non è stata istituita, né è controllata da alcuna autorità centrale. Il controllo sulle transazioni è eseguito da tante entità indipendenti in maniera decentralizzata e distribuita, per cui la presenza di banche e altri soggetti regolamentati non è più necessaria.

- **Non soggetta a politiche monetarie:** l'assenza di un'autorità centrale comporta anche l'impossibilità che un qualsiasi soggetto eserciti azioni coercitive sulla valuta, come ad esempio l'aumento o la diminuzione delle unità di valuta in circolazione. L'offerta di moneta è stabilita a priori dal protocollo, in maniera che aumenti progressivamente fino ad arrivare alla soglia massima di 21 milioni di unità.

- **Non ha corso legale:** i bitcoin sono accettati come mezzo di pagamento solo su base volontaria, e dunque non possono essere utilizzati per estinguere delle obbligazioni pecuniarie se il creditore si rifiuta di accettarli.

- **Pseudonima:** le transazioni avvengono tra indirizzi pubblici a partire dai quali è praticamente impossibile risalire alla reale identità della persona fisica o giuridica che processa lo scambio di bitcoin.

- **Trasparente:** tutte le transazioni sono registrate in un registro aperto al pubblico, la *blockchain*, che ognuno può visualizzare. Esplorando la blockchain è possibile sapere quanti di quanti bitcoin dispone un determinato indirizzo in un preciso istante temporale, potendo inoltre risalire agli indirizzi che glieli hanno forniti.

- **Bassi costi di transazione:** l'assenza di soggetti che intermediano nelle transazioni ha la conseguenza di abbatterne i costi. In media le transazioni prevedono un addebito al mittente di 0,0001 BTC (circa 0,02 €) come commissione, ma l'importo

può essere maggiore o nullo a seconda di certe condizioni che saranno illustrate nel prossimo capitolo.

- **Transazioni veloci e irreversibili:** ogni transazione di bitcoin impiega mediamente 10 minuti per essere confermata. Tali transazioni sono irreversibili, ovvero impossibili da annullare.

1.3 Dove si "mettono" i bitcoin, come si ottengono, e dove si possono spendere?

Ci sono diversi modi per ottenere dei bitcoin, alcuni semplici ed immediati, altri che richiedono un po' più di tempo ed organizzazione. Sono in continua crescita gli esercizi commerciali, sia fisici che online dove si possono spendere. Tuttavia prima di pensare a come ottenere e spendere dei bitcoin è necessario mettersi nelle condizioni di poterli ricevere, e una volta ricevuti di poterli tenere al sicuro, senza rischiare di perderli o di farseli "rubare". A questo scopo è necessario possedere un *wallet Bitcoin*, un portafoglio elettronico che, molto metaforicamente, svolge le stesse funzioni di un portafoglio materiale, cioè di custodia del nostro denaro che in questo caso è digitale.

1.3.1 I wallet Bitcoin

I portafogli Bitcoin non sono proprio l'equivalente di un conto corrente, anche se l'interfaccia offerta dai diversi servizi di wallet consente di sapere in ogni momento il totale dei bitcoin posseduti e le movimentazioni in entrata ed uscita, come una sorta di estratto conto in tempo reale. I bitcoin non sono di fatto contenuti all'interno di un portafoglio, ma sono memorizzati in un registro aperto al pubblico, la blockchain, sotto degli specifici indirizzi appartenenti ai diversi utenti. Gli indirizzi sono punti di ricezione e invio, e si presentano sottoforma di codici alfanumerici di 33 o 34 caratteri, generalmente inizianti per 1, come ad esempio "*1G1vTdCYjqb5gucmhNQH7yTBy9uPHC5Aht*", in modo da non contenere alcun riferimento dell'utente utilizzatore, facendo di Bitcoin un sistema di pagamento pseudonimo.

Gli indirizzi derivano algoritmicamente da altri codici, le chiavi pubbliche[6], e queste a loro volta derivano algoritmicamente dalle chiavi private[6], in maniera tale che a partire dall'indirizzo sia impossibile risalire alla chiave pubblica originaria e da questa alla

[6] chiavi private e chiavi pubbliche: le transazioni di bitcoin, come verrà analizzato nel secondo capitolo, si basano sulla tecnologia della crittografia asimmetrica (o crittografia a chiave pubblica/privata), in particolare sul meccanismo delle firme digitali.

chiave privata. Attraverso il meccanismo crittografico delle firme digitali, solo il possesso della chiave privata autorizza l'utente a spendere i bitcoin associati all'indirizzo da essa derivato. Per questo motivo la chiave privata non deve essere resa pubblica, ma deve essere custodita per non correre il rischio di non poter più spendere i bitcoin relativi.

I portafogli Bitcoin custodiscono le chiavi private dell'utente, che gli permettono di spendere i bitcoin associati al preciso indirizzo che deriva dalla chiave pubblica che a sua volta deriva dalla chiave privata in oggetto; questo è ciò che avviene dietro le quinte. Infatti il wallet offre all'utente un'interfaccia intuitiva, che gli permette di visualizzare il bilancio di bitcoin a sua disposizione di tutti gli indirizzi diversi che egli possiede, dandogli la possibilità di effettuare delle transazioni in uscita verso determinati beneficiari, o di ricevere dei pagamenti ad un determinato indirizzo.

Quando si crea un nuovo wallet, automaticamente vengono generate cento coppie di chiavi private e pubbliche (*key-pool*), per cui l'utente può usufruire di più indirizzi diversi, per godere di maggiori livelli di privacy. Infatti ogni transazione è registrata nella blockchain, e chiunque può vedere tutti i movimenti di un indirizzo; se un individuo è in grado di associare un indirizzo ad un'identità fisica, in seguito per esempio ad una contrattazione in cui si sono scambiati gli estremi per il pagamento, questi può controllarne tutti i movimenti, per questo motivo cambiare spesso indirizzo è garanzia di maggior privacy.

Esistono diversi tipi di portafogli tra cui scegliere, a seconda dei livelli di praticità, sicurezza e complessità desiderata:

- **Desktop Wallet:** software wallet da installare sul proprio computer che permette di memorizzare e custodire le chiavi private all'interno dell'hard disk. L'installazione di questi software, ce ne sono di vario tipo per diversi sistemi operativi, richiede generalmente il download dell'intera blockchain, che al giorno d'oggi pesa circa 33GB (Fonte: blockchain.info, ultima consultazione 02/05/'15). La sicurezza garantita da questo tipo di wallet può essere elevata, ma solo se si prendono delle dovute precauzioni. Se il dispositivo non è protetto da un antivirus e non si provvede a proteggerlo, o banalmente se lo stesso computer non è protetto da alcuna password all'avvio, e neppure il wallet è stato criptato con una password adeguata,

l'utente corre il rischio che qualche hacker rubi le chiavi private dal proprio pc, o comunque se lo stesso venisse perso o lasciato incustodito, chiunque potrebbe avere accesso al suo wallet e spendere i suoi bitcoin. Infine è consigliato effettuare periodici backup del portafoglio, per poter recuperare le chiavi private qualora il pc dovesse subire dei danni irreparabili.

- **Mobile Wallet:** applicazioni wallet per smarphone che rendono possibile custodire, spendere o ricevere bitcoin dal proprio cellulare in modo semplice e veloce. Questo tipo di applicazioni non richiedono il download dell'intera blockchain, ma soltanto di una parte di essa, facendo affidamento sulle informazioni provenienti da altri nodi del network. Come per i desktop wallet è consigliato effettuare periodici backup.

- **Online Wallet:** servizio offerto da siti web, che custodiscono le chiavi private memorizzandole in server online posti sotto la loro tutela. In altri termini l'utente affida la custodia dei propri bitcoin a terzi, in questo caso un sito web. Tipicamente i wallet online sono offerti in via accessoria dagli exchange, piattaforme di compravendita di bitcoin in cambio di valute tradizionali. Considerando gli spiacevoli inconvenienti[7] capitati ad alcuni di questi exchange in passato, probabilmente questo tipo di wallet non è il più sicuro della lista, ma è sicuramente il più semplice e veloce da utilizzare, in quanto è possibile accedervi da qualsiasi dispositivo connesso a internet. Dunque tenere molti bitcoin in questi tipi di wallet non è particolarmente indicato, mentre per piccole ma frequenti transazioni sono senza dubbio i più pratici.

- **Paper Wallet:** le chiavi private e pubbliche possono essere conservate direttamente dallo stesso utente in un supporto cartaceo, e tenute così al riparo da hacker e da eventuali guasti dei propri dispositivi elettronici. I più comuni online wallet consentono di esportare in formato cartaceo i propri codici, o in alternativa bitaddress.org genera casualmente delle nuove coppie di chiavi, privata e pubblica, che potranno essere impiegate per ricevere dei bitcoin, ed in seguito per spenderli. Una volta esportato il proprio wallet in formato cartaceo, la chiave pubblica non è più memorizzata digitalmente da nessuna parte, per cui è consigliato conservarlo in

[7] Frequenti sono stati gli episodi di attacchi ai server delle piattaforme di exchange, al fine di rubare le chiavi private degli utenti e aver accesso ai loro bitcoin; tra i più degni di nota quelli che hanno portato alla chiusura di Mt. Gox nel febbraio 2014.

maniera adeguata e magari crearne alcune copie per sicurezza. L'indirizzo potrà ricevere normalmente dei pagamenti, ma per spendere tali bitcoin l'utente dovrà reimportare la propria chiave privata in un online o software wallet per firmare le transazioni in uscita. Da questo punto di vista la sicurezza offerta da un paper wallet è molto elevata, e funziona benissimo come deposito di bitcoin a lungo termine.

Figura 1.2: Esempio di paper wallet generato su bitaddress.org.

- **Hardware Wallet:** dispositivi creati appositamente per custodire le chiavi private degli indirizzi bitcoin e di altre criptovalute. Rispetto agli altri tipi di wallet non si fa affidamento a entità terze per la conservazione dei codici, non si corre il rischio che gli stessi vengano rubati da un hacker, e non si devono reimportare online o in un software per poter effettuare delle transazioni in uscita. Gli hardware wallet sono dei mini computer aventi un'unica funzione, quella di firmare digitalmente le transazioni con le chiavi private dell'utente. Questi si collegano al computer generalmente via USB, e interagiscono con i software wallet in tutta sicurezza anche se il computer risultasse compromesso. L'utente verifica dal computer la correttezza dell'indirizzo a cui inviare dei bitcoin, e autorizza la transazione inserendo un codice PIN sul proprio hardware wallet, che gli hacker non riescono ad intercettare.

1.3.2 Come ottenere dei bitcoin:

- **Acquistarli da persone disposte a venderli:** localbitcoins.com è un sito che mette in contatto chi vuole vendere bitcoin con chi li vuole comprare e viceversa. Presente in 7.644 città e 240 paesi tra cui anche l'Italia localbitcoins.com rappresenta la piattaforma leader del servizio di scambio *face-to-face*. Chi vuole comprare dei bitcoin

può decidere se effettuare lo scambio online, scegliendo il metodo di pagamento prescelto (bonifico bancario, paypal, postepay, ...), oppure è possibile accordare un incontro fisico con il venditore e scambiare bitcoin in cambio di contanti, in quanto si possono trovare offerte anche relativamente vicine in termini geografici. Gli incontri face-to-face devono svolgersi in luoghi in cui è disponibile l'accesso ad internet, necessario per processare delle transazioni, mentre per gli scambi online è sempre consigliato controllare il feedback del venditore.

Si possono incontrare persone disposte a vendere dei bitcoin anche attraverso bitcoin.meetup.com, social network che riunisce gruppi di persone per aree di interessi, tra cui appunto i bitcoin. Alcuni di questi gruppi organizzano incontri periodici, a cui è possibile partecipare e avere un contatto diretto con l'argomento e con le persone della "comunità". Altra opportunità interessante è rappresentata dai *Satoshi Square*, eventi pubblici che si svolgono per lo più nelle grandi città in cui una piazza o un parco pubblico viene trasformato in un mercato di bitcoin all'aria aperta, un tributo a "Wall Street" secondo Josh Rossi, organizzatore del primo Satoshi Square avvenuto a New York a maggio 2013, che oltre a facilitare gli scambi di bitcoin contribuiscono a darne anche evidenza pubblica e consentono a chiunque lo desideri di capirne qualcosa in più. Quest'ultime due opportunità di ottenere dei bitcoin determinano volumi di scambio esigui se paragonati alle altre modalità che si stanno per illustrare, ma possono essere importanti soprattutto per il loro ruolo di comunicazione e diffusione dell'informazione nell'ambito della criptovaluta.

- **Acquistarli presso gli *Exchange* online:** sul web esistono molti siti che consentono la compravendita di bitcoin in cambio di moneta legale o di altre criptovalute. Tali piattaforme svolgono il ruolo di *market makers* fissando i tassi di cambio a cui l'Exchange compra o vende bitcoin in cambio delle principali valute tradizionali o di altre valute virtuali. A seconda del sito prescelto, le procedure di iscrizione e certificazione dell'identità dell'utente possono richiedere del tempo prima di poter procedere alla compravendita di bitcoin. Le tabelle 1.1 e 1.2 classificano i principali siti di exchange online per volume di bitcoin (BTC) scambiati negli ultimi sei mesi; la prima tabella classifica i primi dieci siti di exchange per volume di bitcoin scambiati verso qualsiasi tipo di valuta legale, mentre la seconda si focalizza sugli exchange con i maggiori volumi di bitcoin scambiati verso euro.

EXCHANGE	Volume in Milioni di BTC	Quota di Mercato	Valute
BTC China	26,75	31,04%	CNY
OKCoin	26,4	30,63%	CNY USD
Huobi	14,89	17,27%	CNY
Bitfinex	6,56	7,61%	USD
LakeBTC	2,85	3,30%	CNY USD
BitStamp	2,8	3,24%	USD
BTC-e	1,85	2,15%	EUR RUR USD
ANX	1,63	1,89%	AUD CAD CHF EUR GBP HKD JPY NZD SGD USD
Coinbase	0,53	0,61%	USD
Localbitcoins	0,47	0,55%	AUD CAD EUR GBP JPY PLN USD

Tabella 1.1: primi dieci exchange per volume di BTC scambiato complessivamente negli ultimi 6 mesi (Fonte: bitcoinity.org, data ultima consultazione 23/03/15).

EXCHANGE	Volume in Migliaia di BTC	Quota di Mercato
Kraken	460	50,27%
ANX	165	17,99%
Bitcoin.de	107	11,67%
HitBTC	71,2	7,77%
Localbitcoins	38,8	4,24%
BTC-e	23,1	2,52%
itBit	22	2,40%
Bitcoin Central	17,8	1,94%
CleverCoin	7,22	0,79%
Altri	3,82	0,42%

Tabella 1.2: primi dieci exchange per volume di BTC scambiato con euro negli ultimi 6 mesi (Fonte: bitcoinity.org, data ultima consultazione 23/03/15).

- **Bitcoin ATMs:** un servizio di acquisto o vendita molto più rapido rispetto agli *exchange online* è offerto dai *Bitcoin ATMs* (o *Bancomat Bitcoin*). Il primo bancomat bitcoin, prodotto dall'americana *Robocoin*, è stato installato nell'ottobre 2013 presso la *Waves Coffee House* di Vancouver, Canada, e già nel suo primo giorno di funzionamento ha registrato ben 81 transazioni per un valore totale di oltre 10.000 $. Ci sono attualmente 371 bancomat bitcoin nel mondo (fonte: coinatmradar.com, ultima consultazione 28/03/15), di cui 10 in Italia[8], ma stando alle stime dello stesso sito tale numero cresce settimanalmente di circa 8 nuove unità. In circolazione si possono trovare diversi modelli, anche se attualmente sono sei i modelli maggiormente diffusi, come si evince dalla tabella seguente, che rappresentano più del 90% del totale.

Produttore ATMs	Nr. Dispositivi	Quota di Mercato
Lamassu	118	31,81%
Skyhook	60	16,17%
BitAccess	48	12,94%
Genesis Coin	45	12,13%
Robocoin Kiosk	36	9,70%
General Bytes	27	7,28%
Altri	37	9,97%
Totali	**371**	

Tabella 1.3: produttori di Bitcoin ATMs per numero di dispositivi nel mondo e quota di mercato (Fonte: coinatmradar.com, data ultima consultazione 28/03/15).

Questi dispositivi sono generalmente di due tipi: unidirezionali, cioè consentono di convertire soltanto moneta legale in bitcoin, e bidirezionali che invece consentono sia di comprare che di vendere bitcoin in cambio di moneta legale.

Rispetto alle opzioni elencate in precedenza, quella rappresentata dai bancomat bitcoin si mostra di più facile ed immediato utilizzo. Se si è già in possesso di un

[8] In Italia si possono trovare due ATM a Roma, uno a Milano, Firenze, Genova, Reggio Emilia, Pisa, Udine, Chiavari e Rovereto (Fonte: coinatmradar.com, data ultima consultazione 28/03/15).

wallet elettronico infatti, acquistare o vendere dei bitcoin può richiedere dai 15 ai 30 secondi, mentre se ci si dovesse trovare di fronte a una *Robocoin Kiosk* o a una *BitAccess* è possibile creare un nuovo portafoglio e comprare dei bitcoin il tutto in meno di 5 minuti, abbattendo così le tempistiche per l'autenticazione richieste normalmente da un exchange online.

In generale il processo di acquisto (o di vendita) di bitcoin attraverso un ATM avviene nelle seguenti fasi:

a) Fase di verifica: questa fase è opzionale, nel senso che non tutti i modelli di ATM in circolazione la prevedono. La verifica può consistere nel semplice inserimento di un codice che la macchina provvede ad inviarci per sms dopo aver inserito il nostro numero di cellulare, oppure in presenza di modelli più sofisticati può consistere nel vero e proprio riconoscimento personale e fisico dell'utilizzatore. Quest'ultimo è il caso della Robocoin Kiosk, a cui si può avere accesso soltanto creandosi un account personale. Il dispositivo al primo accesso del cliente ne catturerà le scansioni del documento di identità o del passaporto, del viso attraverso la fotocamera e del palmo della mano, mentre dal secondo accesso in poi la verifica avverrà appoggiando semplicemente il palmo della mano allo scanner e digitando il PIN numerico scelto.

b) Inserimento dell' indirizzo Bitcoin: questa fase avviene mediante scansione del *Qr Code*[9] associato al wallet elettronico in cui l'utilizzatore desidera ricevere bitcoin, o da cui vuole prelevare bitcoin in cambio di denaro cash. Alcuni ATM consentono anche la generazione di nuovi indirizzi al momento.

c) Selezione del quantitativo di denaro contante che si desidera cambiare in bitcoin, e suo inserimento nello slot. Se l' ATM è bidirezionale è possibile convertire dei bitcoin in valuta legale, mentre sempre a seconda del modello del dispositivo è possibile anche la compravendita di altre criptovalute.

d) Conferma dell'avvenuta operazione tramite scontrino.

- **Vendere beni e servizi in cambio di bitcoin:** attualmente, in Italia, questa opzione è più facilmente percorribile da chi conduce un esercizio commerciale. Sono sempre più numerosi i negozi, sia fisici che online, che accettano pagamenti in bitcoin in cambio di beni e servizi. Il modo più semplice per un commerciante per accettare

[9] Qr Code (quick response code): codice a barre bidimensionale di forma quadrata, impiegato per memorizzare informazioni digitali ed essere letto mediante smartphone (Fonte: wiki/Codice QR).

pagamenti in bitcoin dai propri clienti è comunicare l'indirizzo e aspettare che questi effettuino il pagamento con il proprio smartphone. Tuttavia sono in continua crescita i servizi volti a semplificare e velocizzare le procedure di pagamento in valuta digitale.

- **Mining:** è l'attività di validazione e registrazione delle transazioni di bitcoin che avvengono di continuo nel sistema. Tale attività viene svolta dai nodi del network che sono per questo motivo chiamati minatori, e consiste nel far svolgere al proprio calcolatore dei complessi problemi crittografici in maniera ripetitiva, dispendiosi in termini di consumo di energia elettrica e di usura delle apparecchiature.

  Il mining è incentivato da un preciso sistema di ricompense, consistenti in bitcoin di nuova emissione in quantità e con tempistiche prestabilite dal protocollo, come sarà approfondito nel seguente capitolo, e rappresenta l'unico meccanismo di creazione ed immissione di nuove unità di valuta.

  Ogni nodo lavora autonomamente, contemporaneamente e in competizione con tutti gli altri nodi allo scopo di risolvere per primo il problema ed aggiudicarsi la ricompensa. Da questo punto di vista il mining è una sorta di lotteria.

  Alternativamente i nodi possono collaborare riunendosi in gruppi detti *mining pools*[10], mettendo in comune la propria forza computazionale per avere più probabilità di ottenere le ricompense, in concorrenza con gli altri nodi autonomi o gli altri gruppi.

  La potenza di calcolo complessiva di Bitcoin è data dalla somma delle potenze di tutti i dispostivi messi a disposizione dai nodi, ed è importante perché da questa deriva la difficoltà dei problemi crittografici da far risolvere ai minatori. Infatti tale difficoltà si aggiusta automaticamente in modo che aumentando la potenza totale aumenti anche la difficoltà e viceversa, garantendo che le transazioni siano sempre validate entro un certo lasso di tempo (10 minuti), e allo stesso modo anche le ricompense siano elargite in maniera costante.

  Per questo motivo, se agli inizi di Bitcoin i primi minatori riuscivano a guadagnare anche utilizzando dei comuni computer più o meno recenti, l'aumento progressivo dei minatori e quindi della potenza di calcolo immessa, e la nascita di dispositivi sempre

[10] Mining pool: in una mining pool l'attività di mining è svolta collettivamente; ogni nodo del gruppo mette a disposizione la propria potenza di calcolo, e le ricompense per la risoluzione dei problemi vengono spartite tra i partecipanti in proporzione alla potenza apportata.

più potenti costruiti appositamente per questo scopo (*ASICs*[11]), il tutto trainato dalla progressiva diffusione di Bitcoin come sistema di pagamento alternativo e conseguentemente dalla crescita del suo prezzo, hanno dato vita a veri e propri business legati al mining, portandolo ad una difficoltà troppo elevata da supportare se non attraverso degli ingenti investimenti in hardware specifici ed energia. Quest'ultima opzione esposta è sicuramente la più complicata per ottenere dei bitcoin.

1.3.3 Dove si spendono?

Come affermato in precedenza sono in continuo aumento gli esercizi commerciali, sia fisici che online, che permettono di comprare beni e servizi in cambio di Bitcoin. Attualmente, stando alle cifre fornite da Coinmap.org, in tutto il mondo sono 6.501 gli esercizi commerciali in cui ci si può recare ed acquistare beni o servizi in cambio di bitcoin (ultima consultazione: 06/05/'15), di cui poco più di 250 in Italia. Sempre grazie allo stesso sito si può sapere se nel luogo in cui ci troviamo siamo vicini o meno a uno di questi negozi.

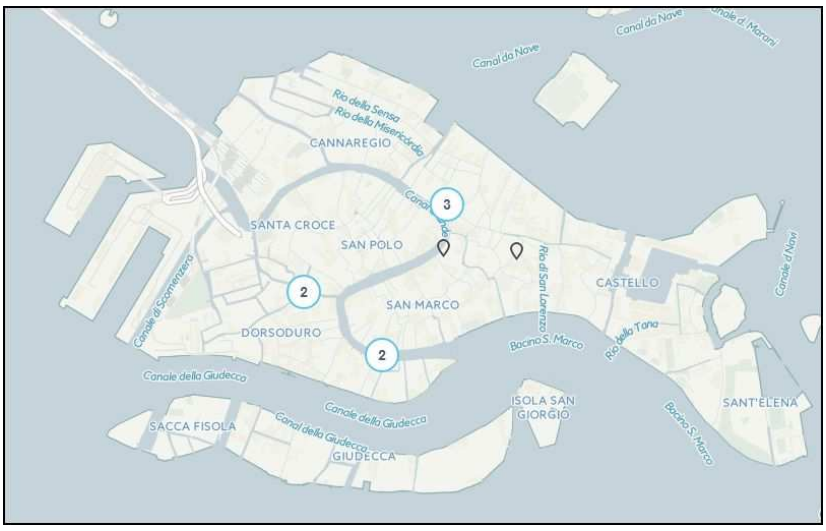

Figura 1.3: a Venezia ci sono 9 esercizi commerciali che accettano bitcoin (Fonte: Coinmap.org, data ultima consultazione 31/05/'15).

[11] ASIC (application specific integrated circuit): circuito integrato creato appositamente per risolvere un'applicazione di calcolo precisa, in questo caso i problemi crittografici del mining (Fonte: wiki/ASIC).

Per quanto riguarda il web sono moltissimi i siti in cui si possono spendere dei bitcoin. La pagina bitcoin.it/wiki/Trade elenca migliaia di siti web in cui è possibile acquistare beni e servizi delle più diverse categorie in cambio di bitcoin, mentre sempre wikipedia elenca una serie di progetti e fondazioni che accettano donazioni in bitcoin a cui è possibile partecipare anche con un piccolo contributo.

1.4 Storia

"*Ho lavorato ad un nuovo sistema di moneta elettronica che è completamente peer-to-peer, senza nessuna terza parte fidata*" annuncia Satoshi Nakamoto il 1 novembre 2008 nella *Cryptography Mailing List* del sito metzdowd.com, una mailing list che accoglie discussioni in merito allo sviluppo di tecnologie riguardanti la crittografia e il loro impatto dal punto di vista politico e sociale, allegandovi il documento pdf "*Bitcoin: a peer-to-peer electronic cash system*" in cui ne spiega il funzionamento. "*Bitcoin v0.1*" è il nome del primo software Bitcoin, il cui rilascio a gennaio 2009 segna l'inizio dell'era delle criptovalute.

Anche se i primi anni di vita di Bitcoin non sono stati molto entusiasmanti dal punto di vista della diffusione e dell'utilizzo di questo nuovo tipo di valuta, l'anno 2009 può essere considerato come una sorta di data spartiacque: da un lato rappresenta il raggiungimento di un importante traguardo tecnologico frutto dei numerosi progressi in ambito crittografico e informatico e di alcuni tentativi di valute alternative falliti o mai effettivamente implementati; dall'altro lato segna la nascita attorno a Bitcoin di un vero e proprio ecosistema, e il successivo proliferare degli *altcoins* ovvero valute digitali alternative nate a partire dal progetto Bitcoin.

1.4.1 Prima di Bitcoin

A partire dagli anni '70 la ricerca in ambito crittografico conduce a importanti sviluppi, in un periodo in cui il progressivo avanzamento verso l'era digitale accentua i bisogni di sicurezza e di privacy individuale. La crittografia da prerogativa dei governi per la sicurezza delle comunicazioni torna ad essere di pubblico dominio, per garantire alti livelli di privacy nei nuovi sistemi digitali, tra i quali appunto quelli riguardanti i pagamenti.

Negli anni '80 il crittografo americano *David Chaum* introduce il sistema delle *blind signatures* (firme cieche[12]) allo scopo di migliorare la privacy dei servizi di pagamento elettronici offerti dalle banche dell'epoca, che secondo la sua opinione, se da un lato potevano meglio contrastare la criminalità rispetto al contante grazie alla perfetta tracciabilità, dall'altro lato rischiavano di mettere a repentaglio le normali abitudini degli individui onesti. Chaum estende le sue ricerche nell'ambito dei sistemi di pagamento elettronici, che culminano con la fondazione della *DigiCash Inc*. ad Amsterdam e il lancio del sistema *e-cash* nei primi anni '90. Il sistema di pagamento elettronico e-cash utilizzava del denaro virtuale da tenere nel computer, controllato crittograficamente dalle banche associate, e consentiva di effettuare acquisti anonimi e sicuri su Internet o nei negozi che li accettavano, senza la necessità di scambiare le credenziali delle carte di credito. Nonostante questo sistema venne venduto a diverse banche, queste si mostrarono comunque conservative in un mercato dominato dalle carte di credito, per cui e-cash non decollò mai in maniera significativa, e DigiCash fallì nel 1998. Nonostante e-cash fosse un sistema centralizzato in quanto controllato dalla banca emittente, era comunque fondato su solide basi crittografiche che avrebbero in seguito fornito degli spunti per i successivi tentativi di decentralizzazione.

Sempre nel 1998 nasce *PayPal* che, a differenza di e-cash, consentiva anche il trasferimento di denaro tra due utenti comuni, e non solo tra utente e commerciante, ma questa è un'altra storia, che poco centra con le radici di Bitcoin.

Un'altra esperienza interessante, anche se durata poco più di una decina danni (1996-2009), l'ha fornita *e-gold*, una valuta digitale scambiabile istantaneamente su Internet, emessa dalla società privata *Gold & Silver Reserve Inc.* in cambio di depositi in oro o argento. Questa valuta veniva scambiata tra account e-gold, e detenerla significava detenere una certa quantità di metalli preziosi custoditi dalla *G&SR* come riserva. A partire dal 1999 il mercato di e-gold decollò, culminando con la nascita nel 2000 delle prime piattaforme di exchange indipendenti. E-gold poteva essere usata sia per trasferimenti di denaro tra privati, sia per gli acquisti online, aprendo inoltre alla possibilità di effettuare micropagamenti. Nel 2007 il governo statunitense accusò e-gold di permettere il riciclaggio del denaro, chiudendo alcuni exchange e arrivando al

[12] Firme cieche: rappresentano una particolare forma di firma digitale, in cui il firmatario firma il messaggio in modo cieco, ovvero non conoscendo il contenuto del messaggio. Lo scopo è garantire l'autenticità del messaggio a chi lo riceve, ma in maniera non identificabile (Fonte: wiki/Blind_signature).

definitivo blocco degli account e delle transazioni nel 2009. Il sistema e-gold era infatti diventato lo strumento di pagamento preferito dai criminali.

Infine nel 1998, *Wei Dai* e *Nick Szabo* propongono entrambi, a poca distanza l'uno dall'altro, due diversi sistemi di pagamento decentralizzati, che più di tutti si avvicinano a ciò che concepirà Nakamoto dieci anni più tardi, anche se entrambi i progetti rimasero solo teorici.

Wei Dai con *b-money* si basa sull'idea che esista un network anonimo in cui gli utenti siano identificati da pseudonimi, che ogni utente conservi in modo separato un registro delle transazioni (o in alternativa che lo stesso sia tenuto solo da alcuni di questi utenti, chiamati server, e che questi abbiano degli incentivi per tenerlo in modo onesto), che la creazione di moneta avvenga mediante la risoluzione di problemi attraverso l'impiego di una certa potenza di calcolo, e che infine le transazioni avvengano tra indirizzi mediante il meccanismo della firma digitale.

Se già b-money sembrava avvicinarsi al futuro Bitcoin, se non altro come idea di base, la ricerca di Nick Szabo, in cui spiega il funzionamento del suo *bit-gold*, sembra essere dal punto di vista tecnico più completa. La creazione di bit-gold consiste nel trovare una stringa di bit, chiamata "*challenge string*" mediante il meccanismo del *proof-of-work*[13] (o prova di lavoro, essenzialmente far fare dei calcoli al processore). Ogni challenge string trovata fornisce una sorta di input per trovare la successiva, per cui una particolare challenge string può essere trovata solo una volta e solo da un unico utente, ovvero il primo in ordine cronologico che risolve il problema e che lo autorizza poi a spenderla. Le transazioni avvengono mediante la firma digitale di queste stringhe di bit, e i riceventi possono verificarne l'autenticità consultando il registro distribuito delle transazioni.

A questo punto c'è da chiedersi se e in che modo Satoshi Nakamoto ha tratto insegnamento da queste precedenti esperienze.

Bisogna ricordare che verso la fine degli anni '80 nasceva il *cypherpunk*, un movimento che poneva al centro proprio la crittografia come la tecnologia in grado di sconvolgere lo

[13] Proof-of-work (pow): letteralmente prova di lavoro, è un meccanismo che impone al richiedente del servizio l'esecuzione di un lavoro o compito, che viene svolto dal computer e che richiede tempo di elaborazione ed energia elettrica; un esempio di pow è rappresentato dal sistema hashcash, finalizzato a rendere dispendioso l'invio "aggressivo" di spam via e-mail (Fonte: wiki/Proof-of-work).

status quo, conducendo ad un cambiamento politico e sociale. Gli sviluppi crittografici di quegli anni e gli studi di Chaum furono fatti propri dagli esponenti del movimento, la cui missione fu descritta da *Eric Hughes* in "*A Chyperpunk's Manifesto*" nel 1993: "*I cypherpunks sono dediti alla costruzione di sistemi anonimi... La privacy è necessaria per una società aperta nell'era digitale... Non possiamo aspettarci che i governi, le società, o altri grandi organizzazioni senza volto ci concedano la privacy... Difenderemo la nostra privacy con la crittografia, con sistemi anonimi di invio dei messaggi, con le firme digitali, e con la moneta elettronica*".

Nella *cypherpunk's mailing list*, piattaforma per la discussione e la condivisione delle idee, sono diversi gli informatici ed esperti di crittografia ad essersi messi in evidenza per importanza ed innovatività del contributo intellettuale apportato, tra i quali i fondatori del movimento *Tim May*, *Eric Hughes* e *John Gilmore*, gli stessi *David Chaum* e *Wei Dai* citati in precedenza, ed inoltre *Phil Zimmerman* (creatore di PGP[14]) e *Adam Back* (ideatore di hashcash, sistema di proof-of-work) solo per citare i più importanti.

Cosa centra Bitcoin con tutto questo? Bitcoin dal canto suo sembra proprio mettere in pratica le idee e gli obiettivi per cui è nato il movimento dei cypherpunks, ovvero per difendere il diritto alla privacy con la creazione di un sistema di pagamento anonimo alternativo a quelli tradizionali, attraverso la matematica e la crittografia, tanto più che proprio nel suo paper Nakamoto cita sia Wei Dai per b-money, che Adam Back per hashcash.

Ma chi è realmente Satoshi Nakamoto? Non si sa, e probabilmente mai si potrà sapere l'identità dell'ideatore di Bitcoin, o forse del gruppo di persone che l'ha creato e che si nasconde dietro questo pseudonimo. Numerose ricerche sono state fatte in proposito, e numerosi sono gli esperti a cui è stato accostato, tra cui anche Nick Szabo, ideatore di bit-gold, che ha comunque smentito di essere Satoshi Nakamoto. Risalgono al 2011 le ultime notizie in merito a questo misterioso personaggio: una mail mandata agli sviluppatori e alla comunità Bitcoin in cui dice "*Sono passato ad altro. È* (Bitcoin) *in buone mani con Gavin* (Andresen, uno tra i primi sviluppatori ad unirsi a Bitcoin) *e tutti gli altri*", passando in qualche modo il testimone.

[14] Pretty Good Privacy (PGP): programma di protezione della privacy che si serve della crittografia a chiave pubblica (Fonte: wiki/Pretty_Good_Privacy).

1.4.2 Bitcoin dal 2009 a oggi

Come affermato in precedenza Bitcoin nasce ufficialmente il 3 gennaio 2009, con l'uscita del primo client che dà avvio all'attività di mining e conseguentemente alla creazione di nuove unità di valuta. Il 12 gennaio viene registrata nella blockchain la prima transazione in cui Satoshi invia 10 BTC ad Hal Finney, cypherpunk ed esperto di crittografia.

Nel 2010 nascono i primi Bitcoin Exchange, mentre a maggio dello stesso anno avviene il primo acquisto di un bene "reale": all'interno di bitcointalk.org, forum di riferimento della comunità bitcoin, il programmatore Laszlo Hanyecz offre 10.000 BTC (pari all'epoca a 25$) in cambio di una pizza.

Nel febbraio 2011 il prezzo di 1 BTC arriva per la prima volta a quota 1$. Prezzo che a giugno passerà dai 10$ per 1 BTC al massimo di 31,91$ in soli quattro giorni, in quella che è chiamata "*The Great Bubble of 2011*", salvo poi scendere e stabilizzarsi attorno ai 5$ nei mesi successivi. Il 2011 è anche l'anno dell'apertura di *Silk Road*, piattaforma online di compravendita di droga e altri prodotti illegali in cambio di bitcoin per sfruttarne l'anonimità dei pagamenti, e dell'inizio dei primi attacchi hacker verso i siti di exchange, incentivati anche dall'aumento di prezzo della criptovaluta, che vedono sottrarre dai propri server decine di migliaia di bitcoin, senza la possibilità di rintracciare i responsabili. Episodi che certamente non contribuiscono alla diffusione di Bitcoin.

Negli anni 2012 e 2013 aumentano progressivamente i commercianti disposti ad accettare bitcoin, grazie anche alla diffusione di servizi volti a semplificarne le procedure di pagamento, e aumenta il numero di associazioni e progetti che li accettano in donazione. Ad inizio aprile 2013 il prezzo di 1 BTC supera quota 100$, arrivando circa dieci giorni dopo ad un massimo di 266$. Ad ottobre l'FBI impone la chiusura di Silk road, mentre da metà novembre il prezzo passa da 270$ a oltre 1000$ in pochi giorni, registrando il picco più alto dalla sua nascita a oggi.

Nel 2014 chiude per bancarotta MtGox, exchange leader fino ad allora del palcoscenico Bitcoin, oggetto di numerosi attacchi hacker che hanno complessivamente causato una

perdita stimata attorno alle 850 mila unità di bitcoin, con gravi danni per i portafogli dei propri clienti.

Nonostante un brutto inizio il 2014 è stato sicuramente un anno positivo per quanto riguarda la diffusione e il progresso dell'economia di bitcoin, mentre il suo prezzo è andato progressivamente e stabilmente riducendosi. Importanti società come *Microsoft*, *Dell* hanno deciso di accettare i bitcoin come mezzo di pagamento, ma soprattutto *Pay Pal* decide di aprire al mondo della criptovaluta attraverso una partnership con *BitPay*, *Coinbase* e *GoCoin*, società che offrono servizi alle imprese per l'accettazione di bitcoin. Infine il 2014 è stato un anno importante per gli investimenti di *venture capital* nell'ecosistema Bitcoin, stanziati per un totale di 335 milioni contro i 96 dell'anno precedente (fonte: BitPay).

L'inizio del 2015 continua con la crescita degli investimenti, mentre il prezzo dopo un'iniziale discesa, negli ultimi mesi sembra dare maggiori segnali di stabilità.

1.4.3 Gli Altcoins:

La caratteristica di open-source del progetto Bitcoin ha permesso la partecipazione di molti sviluppatori, che dal 2009 ad oggi hanno fornito un importantissimo contributo nello sviluppo del software e nella correzione delle vulnerabilità che via via si sono presentate.

La stessa caratteristica ha inoltre dato avvio alla nascita di numerose criptovaltute alternative e in competizione con Bitcoin, dette anche *altcoins*. Secondo coinmarketcap.com ci sono attualmente 555 criptovalute diverse in circolazione, tuttavia ne nascono di nuove ogni giorno mentre altre invece scompaiono. Nella *tabella 1.4* sono indicate le prime dieci criptovalute alternative per capitalizzazione di mercato dopo Bitcoin, che rimane la più importante e la più preziosa, considerando che il suo prezzo di mercato di 236,45$ è il più alto tra tutti gli altcoins, con una capitalizzazione di mercato che supera i 3,35 miliardi di dollari.

Nome Criptovaluta	Capitalizzazione di mercato (USD)	Prezzo (USD)	Unità di valuta in circolazione	Volume inviato 24h (USD)
Ripple	$237.657.445	$0,007448	XRP 31.908.551.587	$715.704
Litecoin	$57.684.385	$1,48	LTC 38.848.104	$1.471.130
Dash	$14.985.904	$2,80	DASH 5.349.568	$42.339
Stellar	$14.150.569	$0,00293	STR 4.829.282.081	$40.281
Nxt	$9.202.163	$0,009202	NXT 999.997.096	$17.446
BitShares	$9.194.230	$0,003664	BTS 2.509.520.303	$44.858
Dogecoin	$9.126.525	$0,000092	DOGE 99.318.595.763	$40.272
BanxShares	$7.680.477	$1,50	BANX 5.129.586	$15.153
Peercoin	$5.063.280	$0,227064	PPC 22.298.910	$5.479
Bytecoin	$4.875.509	$0,000028	BCN 172.613.729.301	$5.383

Tabella 1.4: Prime dieci criptovalute, dopo Bitcoin, per capitalizzazione di mercato in dollari statunitensi (Fonte: coinmarketcap.com, data ultima consultazione 08/05/'15).

La maggior parte di queste criptovalute replicano molto similmente i meccanismi alla base di Bitcoin, mentre altre propongono diverse ed innovative funzionalità. Di seguito si propone un elenco dei principali altcoins, delle loro caratteristiche e delle principali differenze con Bitcoin, senza entrare nelle specifiche del loro funzionamento.

Il ***Litecoin***, attualmente la terza criptovaluta più importante, nasce nel 2011 con l'obiettivo di migliorare quanto proposto da Nakamoto, senza tuttavia apportare alcuna grossa modifica a livello strutturale. Nella pratica Litecoin è come Bitcoin, però quattro volte più veloce e quattro volte più grande. Mentre Bitcoin è progettato per validare le nuove transazioni ogni 10 minuti, ed emettere nuove unità di valuta fino ad arrivare ad un massimo di 21 milioni, in Litecoin le nuove transazioni impiegano soltanto 2,5 minuti[15] per essere confermate e registrate, mentre il tetto di unità prestabilito è di 84 milioni.

Il ***Dash***, conosciuto in precedenza come ***Darkcoin***, è una criptovaluta nata nel 2014 sulla base di Bitcoin per migliorarne la velocità e la privacy delle transazioni. Dash permette

[15] Il fatto che Bitcoin richieda 10 minuti mentre alcuni altcoins siano più veloci, non significa che Bitcoin sia meno efficace; la scelta dei 10 minuti è stata un compromesso tra velocità e sicurezza.

infatti transazioni istantanee e impossibili da tracciare, a differenza di Bitcoin dove gli scambi, seppur pseudonimi, possono esser visualizzati da chiunque.

La proposta di ***Ripple*** ha invece un contenuto decisamente più innovativo. Come Bitcoin, Ripple è sia un sistema per i pagamenti elettronici, sia una valuta digitale (XRP), che sfrutta la rete peer-to-peer e la crittografia per permetterne la decentralizzazione. La novità risiede nel fatto che attraverso la rete Ripple è possibile scambiare qualsiasi tipo di valuta, compresi i bitcoin, grazie transazioni molto più rapide che non richiedono alcuna attesa per la loro conferma. Ripple non si pone dunque come un sistema concorrente a bitcoin, ma anzi può essere utile a una sua maggiore diffusione, grazie alla semplicità delle transazioni in valuta diverse e i bassi costi di transazione.

Anche se la maggior parte o forse tutti gli altcoins in circolazione non riusciranno mai a raggiungere e superare la diffusione che ha raggiunto Bitcoin dalla sua nascita ad oggi, contribuiscono comunque, ciascuna in maniera più o meno importante, all'innovazione e al miglioramento delle criptovalute e dei sistemi di pagamento in generale. Gli sviluppatori e l'intera comunità Bitcoin possono prendere spunto dai tentativi proposti dai nuovi progetti per apportarvi modifiche e renderlo migliore con il passare del tempo.

2 COME FUNZIONA BITCOIN?

2.1 Introduzione

Il funzionamento di Bitcoin è nelle mani dei nodi del network detti "*miners*" (minatori). Questi, attraverso il processo di mining, collezionano le transazioni che avvengono in continuazione, ovviamente in bitcoin, all'interno di specifici recipienti chiamati blocchi. Questi blocchi sono uniti tra loro a formare la *blockchain* (o block chain, catena dei blocchi), che rappresenta l'organo più importante e innovativo dell'intero sistema. La blockchain è un grande registro aperto agli utenti e condiviso, contenente ogni transazione avvenuta in bitcoin dalla sua nascita ad oggi al fine di risolvere il probelma del *double-spending*[16], e viene sottoposta a continuo aggiornamento da parte dei minatori. Chiunque può visualizzare una versione completa della blockchain, installando il software Bitcoin o più semplicemente sul web grazie ad appositi siti detti *block explorer*. Ciò nonostante Bitcoin garantisce alti livelli di anonimità, in quanto le transazioni avvengono tra indirizzi pseudonimi a partire dai quali è molto difficile risalire all'identità del suo utilizzatore.

Come affermato in precedenza, le transazioni di bitcoin avvengono tra indirizzi creati appositamente per questo scopo. Un bitcoin di fatto non esiste come unità a sé stante, come può esserlo una stringa di bit nel mondo digitale. Esistono solo transazioni tra indirizzi, con i rispettivi bilanci che aumentano o diminuiscono. Possedere dei bitcoin significa possedere la chiave privata associata ad almeno uno di questi indirizzi tale per cui, all'interno di un qualsiasi blocco "risolto[17]" dal lavoro dei minatori, è stata in precedenza registrata una transazione a favore di quello specifico indirizzo. Ogni transazione di bitcoin è perfettamente tracciabile, in quanto ad ogni istante in cui si

[16] Double-spending (doppia spesa): è la possibilità di spendere una stessa unità di valuta digitale più volte; nei sistemi di pagamento tradizionali questo problema è risolto dalla presenza degli intermediari finanziari che controllano le operazioni. In Bitcoin, mancando di un'autorità centrale, tale problema è risolto dalla presenza della blockchain e dal lavoro dei minatori, che conoscendo tutte le passate transazioni valide sono in grado di rigettare gli scambi che tentano di spendere dei bitcoin già spesi in passato.

[17] Come accennato in precedenza i minatori devono risolvere dei problemi crittografici; la risoluzione di questi problemi conduce alla creazione di un nuovo blocco, detto appunto "risolto".

visualizzi la blockchain è possibile sapere quanti bitcoin appartengono ad un determinato indirizzo, ed inoltre è possibile risalire a quale indirizzo glieli abbia forniti, e da chi quest'ultimo li abbia a sua volta ricevuti, ... La blockchain rappresenta dunque la traccia, lo storico di tutte le transazioni. È uno strumento affidabile, che fa prova poiché nessuna transazione può risultare in conflitto con un'altra, poiché ogni transazione è irreversibile, cioè impossibile da annullare, e viene registrata e marcata temporalmente, per cui nessun utente può inviare bitcoin che non possiede o che ha già inviato a un altro indirizzo, risolvendo così il problema del *double-spending*.

In questo capitolo si propone un'analisi degli aspetti tecnici che permettono il funzionamento di Bitcoin.

2.2 La tecnologia Bitcoin

La tecnologia che permette il funzionamento di Bitcoin è in realtà una combinazione di più tecnologie preesistenti. In questo paragrafo si propone un elenco delle tecnologie più importanti alla base di Bitcoin e un breve accenno al loro funzionamento, propedeutico per poter in seguito scendere nei particolari più tecnici del sistema.

2.2.1 La crittografia

Crittografia deriva dalle parole greche kryptós e graphía, e significa quindi scrittura nascosta. È una scienza dalle radici antichissime che fornisce dei metodi per la cifratura delle informazioni, affinché le stesse risultino incomprensibili ai soggetti non autorizzati a conoscerle. La crittografia nell'era di Internet svolge un ruolo fondamentale nella protezione e messa in sicurezza delle informazioni, e deve rispondere alle seguenti esigenze di:

- Confidenzialità: le informazioni scambiate tra mittente e destinatario non devono essere carpite da terze parti durante il loro passaggio attraverso il canale di comunicazione;
- Integrità: sempre durante il passaggio le informazioni non devono subire modifiche;
- Autenticità: si è certi che l'informazione è stata generata o inviata da un determinato utente;
- Non ripudiablità: certezza che l'informazione arriverà al destinatario.

Bitcoin, che poggia interamente su Internet, si serve della crittografia, in particolare della *crittografia a chiave pubblica* (*o asimmetrica*), per rendere sicure le transazioni di valuta digitale.

Crittografia a chiave pubblica

Nella crittografia a chiave pubblica ogni utente possiede una coppia di chiavi, una chiave privata e una chiave pubblica, utilizzate per la codifica e decodifica delle informazioni che gli stessi si scambiano in un messaggio. Questo tipo di crittografia risulta molto più

efficace rispetto alla *crittografia simmetrica*, in cui i corrispondenti cifrano e decifrano i dati scambiati utilizzando un'unica chiave segreta (ma in questo caso sorge il problema di come scambiarsi in maniera sicura la chiave stessa).

La chiave privata è, appunto, tenuta segreta dal suo possessore, mentre chiave la pubblica può essere resa nota. La chiave pubblica è generata a partire dalla chiave privata attraverso una funzione non iniettiva, ovvero dalla chiave pubblica è impossibile risalire alla chiave privata da cui deriva. Infine chiave privata e chiave pubblica hanno una specifica e diversa funzione: la chiave pubblica serve cifrare le informazioni da inviare, informazioni che possono essere decifrate soltanto con la relativa chiave privata. Vediamo di illustrare meglio il funzionamento attraverso un esempio.

Ipotizziamo che l'utente **A** debba inviare un documento all'utente **B**. **B** comunicherà ad **A** la sua chiave pubblica. **A** cifrerà il documento da inviare con la chiave pubblica di **B**. Il documento viaggerà attraverso il canale di comunicazione tuttavia non può essere letto da nessuno perché cifrato. Infine **B** riceverà il documento che verrà decifrato solo ed esclusivamente con la propria chiave privata.

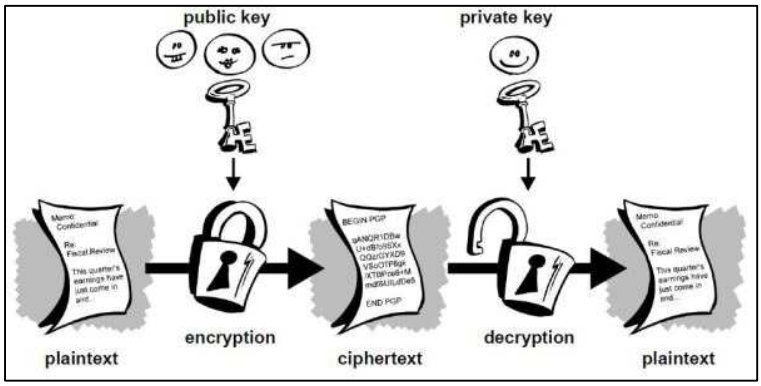

Figura 2.1: schema della crittografia a chiave pubblica. (Fonte: chrispacia.wordpress.com).

Per semplificare ulteriormente la spiegazione ipotizziamo che la chiave pubblica sia un lucchetto, mentre la chiave privata sia la chiave che apre quel lucchetto. **B** invierà ad **A** il proprio lucchetto, che chiuderà la valigetta contenente il documento da inviargli. La valigetta sarà recapitata a **B** che potrà aprirla perché possiede la chiave del lucchetto.

Supponiamo che dentro la valigetta ci sia a sua volta il lucchetto di **A**. **B** riconsegnerà il documento chiudendo la valigetta col lucchetto di **A** in totale sicurezza.

Oltre ad essere utilizzata nel modo sopra descritto, la crittografia a chiave pubblica ha un'altra importante applicazione, cioè la *firma digitale*, in cui la crittografia assume la funzione di metodo di identificazione informatica. Prima di vedere come funziona la firma digitale, occorre fare un passo indietro e introdurre il concetto di *funzione di hash*.

Funzione crittografica di hash

La funzione di hash trasforma delle informazioni di lunghezza arbitraria (ad esempio un messaggio), in codici alfanumerici di lunghezza determinata. Il codice o hash risultante è detto *impronta digitale* del messaggio (o *message digest*), ed è di una lunghezza fissa di bit a seconda dell'algoritmo[18] utilizzato per la conversione.

Le caratteristiche della funzione crittografica di hash sono:

- Dato una qualsiasi informazione in input è semplice ricavarne l'hash;
- Dall'hash è quasi impossibile risalire all'informazione originaria;
- È quasi impossibile che informazioni diverse abbiano un medesimo hash;
- Data un'informazione in input e il relativo hash, anche una minima modifica dell'input cambia totalmente anche il suo hash.

Si osservi che più corto è l'hash a cui vengono ridotte delle informazioni, e più è probabile una collisione, ovvero che due informazioni diverse abbiano la stessa impronta digitale. Gli algoritmi di conversione delle informazioni in hash di molti bit sono per questo motivo più sicuri.

Nell'esempio esposto dalla *tabella 2.1*, utilizzando un comune convertitore online, si possono notare due input relativamente simili produrre due output totalmente diversi.

[18] Algoritmo di hash: un algoritmo di hash trasforma delle informazioni digitali di lunghezza arbitraria (per esempio un messaggio o un documento) in una stringa di lunghezza definita (la lunghezza dipende dall'algoritmo utilizzato) a partire dalla quale non è più possibile risalire all'informazione originale. L'algoritmo maggiormente utilizzato da Bitcoin è lo SHA-256, che a partire dall'informazione produce un'impronta digitale di 256 bit.

SHA1(“ciao”)
1e4e888ac66f8dd41e00c5a7ac36a32a9950d271

SHA1(“cioa”)
3391669ba1e451395a2244a7f1ce6f46abbe544c

Tabella 2.1: l’esempio mostra le differenti impronte del messaggio che si ottengono con l’inversione di due vocali in una parola. L’algoritmo di hash utilizzato è in questo caso lo SHA1, che restituisce un output di 160bit.

La firma digitale

L’utilizzo della crittografia a chiave asimmetrica permette di firmare digitalmente dei documenti, ma l’utilizzo di chiave privata e pubblica avviene in modo inverso rispetto all’utilizzo analizzato in precedenza. Ora è la chiave privata che serve a firmare (o cifrare) un documento, mentre la relativa chiave pubblica è resa nota al destinatario che decifrando con quest’ultima la firma, può constatare o meno l’identità del mittente.

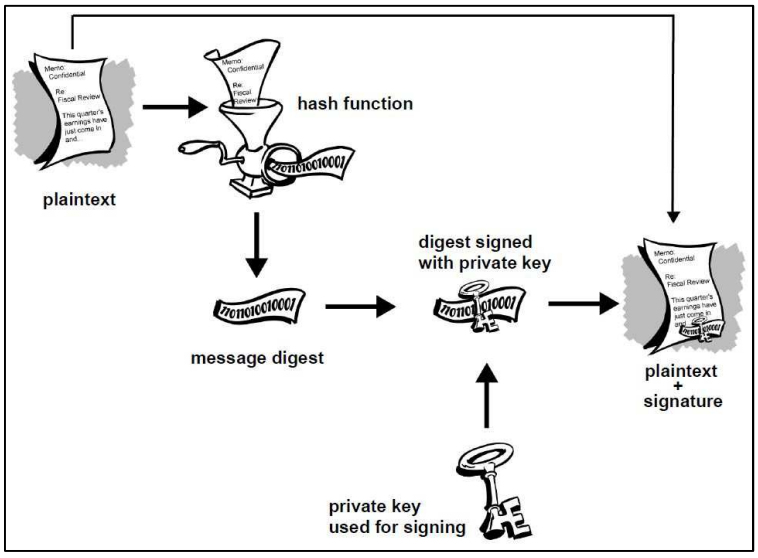

Figura 2.2: schema della firma digitale. (Fonte: chrispacia.wordpress.com).

L’utente per firmare un documento per prima cosa utilizza un algoritmo di hash per produrre un’impronta digitale del documento stesso. L’impronta digitale viene cifrata con la sua chiave privata producendo così una firma su quel documento. Poi invia il

documento al destinatario allegando la propria chiave pubblica. Il destinatario decifrando la firma con la chiave pubblica del mittente verificherà che l'hash risultante corrisponde all'impronta digitale di quel documento, e di conseguenza:

- L'identità del mittente sarà verificata (autenticità);
- Il mittente non potrà negare di aver firmato quel documento (non ripudiabililità);
- Il documento non potrà essere modificato da terzi dopo la firma, o comunque non potrà essere modificato dal destinatario stesso pena la nullità della firma (integrità). La firma è infatti legata all'impronta digitale, e quindi al documento stesso. Una modifica del documento produrrebbe un'impronta digitale totalmente diversa.

2.2.2 La rete peer-to-peer e il calcolo distribuito

La rete peer-to-peer è una particolare architettura di rete informatica in cui il calcolatore di un singolo utente dialoga direttamente con i calcolatori degli altri utenti.

In una rete peer-to-peer, i nodi sono tra loro equivalenti, potendo svolgere funzioni sia da clienti che da servienti verso tutti gli altri nodi della rete, a differenza della più comune architettura di tipo client-server, in cui la comunicazione avviene solo tra client e server, e non anche tra client e client.

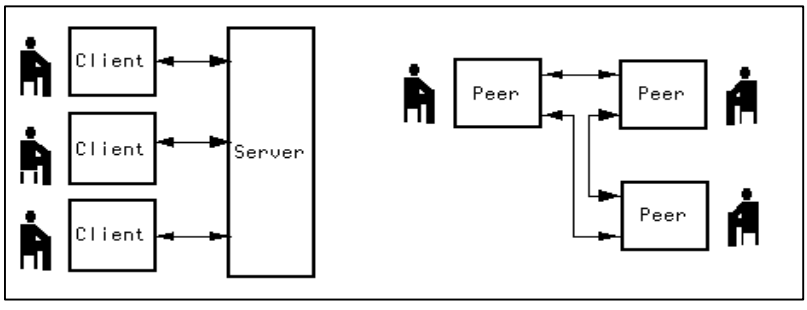

Figura 2.3: architettura client/server (sinistra) e architettura p2p (destra) a confronto.

L'assenza di un server centrale che svolge il ruolo di custodia delle risorse gestite e scambiate fa della rete p2p un sistema decentralizzato, in cui appunto il controllo è trasferito ad ogni singolo nodo, e le informazioni sono distribuite e condivise tra gli stessi attraverso l'applicazione di specifici algoritmi.

Il modello p2p è comunemente associato ai programmi di condivisione dei file, ma non è l'unica applicazione a cui può essere destinato. Una di queste può essere il ***calcolo distribuito***, che consiste nella risoluzione di problemi computazionali di elevata complessità sfruttando la capacità di calcolo fornita nel complesso da un insieme di calcolatori autonomi interconnessi da una rete, come appunto la rete p2p.

Il termine distribuito ha un'accezione ampia, e vuole indicare sia la disposizione fisica in diverse aree geografiche dei calcolatori, sia l'autonomia dei processi che eseguono.

Per questo motivo Bitcoin è di fatto un sistema distribuito, un insieme di calcolatori autonomi collegati attraverso la rete Internet da un'architettura di tipo peer-to-peer, che permette la sincronizzazione e il controllo del registro delle transazioni attraverso la sua condivisione tra i nodi. Tale controllo è decentralizzato e distribuito, in quanto realizzato attraverso la risoluzione di complessi calcoli crittografici da parte di una rete di calcolatori autonomi tra loro, che forniscono la forza computazionale necessaria a questo scopo.

2.3 Chiavi private, pubbliche e indirizzi

Generalmente usufruendo dei servizi offerti dai tanti e diversi fornitori di wallet Bitcoin, l'utente si vede attribuire un indirizzo pubblico che deve rendere noto se vuole ricevere e possedere dei bitcoin, preoccupandosi soltanto di ricordare la password di protezione per accedere al suo wallet e di compiere altre procedure necessarie alla messa in sicurezza degli stessi, in modo di non perdere la possibilità di spendere il proprio denaro digitale. Per capire meglio ciò che succede realmente dietro le quinte di Bitcoin, partiamo dalla spiegazione della funzione e della provenienza di tali codici.

Una chiave privata è un codice casuale di 256 bit che serve per firmare digitalmente le uscite di bitcoin. Solo possedendo la chiave privata è possibile spendere dei bitcoin a questa associati. La chiave privata o le chiavi private sono memorizzate nel nostro computer o smartphone o presso server a seconda del tipo di wallet di cui si usufruisce. Perdere le chiavi private o non poter più recuperare il file in cui sono memorizzate in seguito alla distruzione del pc comporta la perdita dei bitcoin associati a quelle chiavi e l'impossibilità di recuperarli. Allo stesso modo subire il furto delle chiavi private, da parte di un hacker per esempio, può esporci al rischio che qualche malintenzionato spenda i nostri bitcoin.

La chiave pubblica discende dalla chiave privata, e si presenta sottoforma di un codice di 512 bit generato dal particolare algoritmo crittografico ECDSA (Elliptic Curve Digital Signature Algorithm). 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.

Infine dalla chiave pubblica è generato l'indirizzo Bitcoin (160 bit), attraverso dei particolari algoritmi di hashing sempre finalizzati a garantirne la sicurezza.

2.4 La Blockchain

La blockchain è tecnicamente un insieme di blocchi, e ogni blocco è un insieme di transazioni. Le transazioni avvengono di continuo nel sistema, e mediamente ogni 10 minuti un nuovo blocco viene prodotto e agganciato alla catena, in modo che i blocchi risultino disposti in sequenza cronologica a partire dal blocco di origine, il genesis block.

Lo stesso meccanismo della catena è replicato anche per le transazioni che sono contenute nei blocchi, anche se con qualche differenza. Ogni transazione non è collegata alla sua precedente in ordine cronologico, ma alla sua "transazione-input", ovvero al precedente scambio, o ai precedenti scambi, che hanno fornito dei bitcoin al ricevente così da poter diventare ora il mittente nella transazione in questione.

Quello della blockchain può essere considerato un sistema la cui particella più piccola e centrale è rappresentata dalla singola transazione, e procedendo verso l'esterno troviamo il blocco, che racchiude molteplici di queste transazioni, e infine i molteplici blocchi che contengono la storia di Bitcoin dalla sua nascita. La struttura e il funzionamento della blockchain rappresentano la maggiore innovazione tecnologica nell'ambito dei sistemi distribuiti. Per capire il funzionamento dell'intero sistema partiamo dall'analisi della singola transazione, espandendoci progressivamente nella spiegazione.

2.4.1. La struttura delle transazioni:

Satoshi Nakamoto definisce un "*Gettone elettronico*"come *"una catena di firme digitali*". "*Ogni proprietario trasferisce il gettone firmando digitalmente l'hash della transazione precedente e la chiave pubblica del futuro proprietario, e aggiungendo queste informazioni al termine del gettone*" (Nakamoto, 2008). La *figura 2.4* schematizza la struttura delle transazioni di bitcoin, molto simile alla figura proposta da Nakamoto nel suo *paper* "*Bitcoin: a peer-to-peer electronic cash system*".

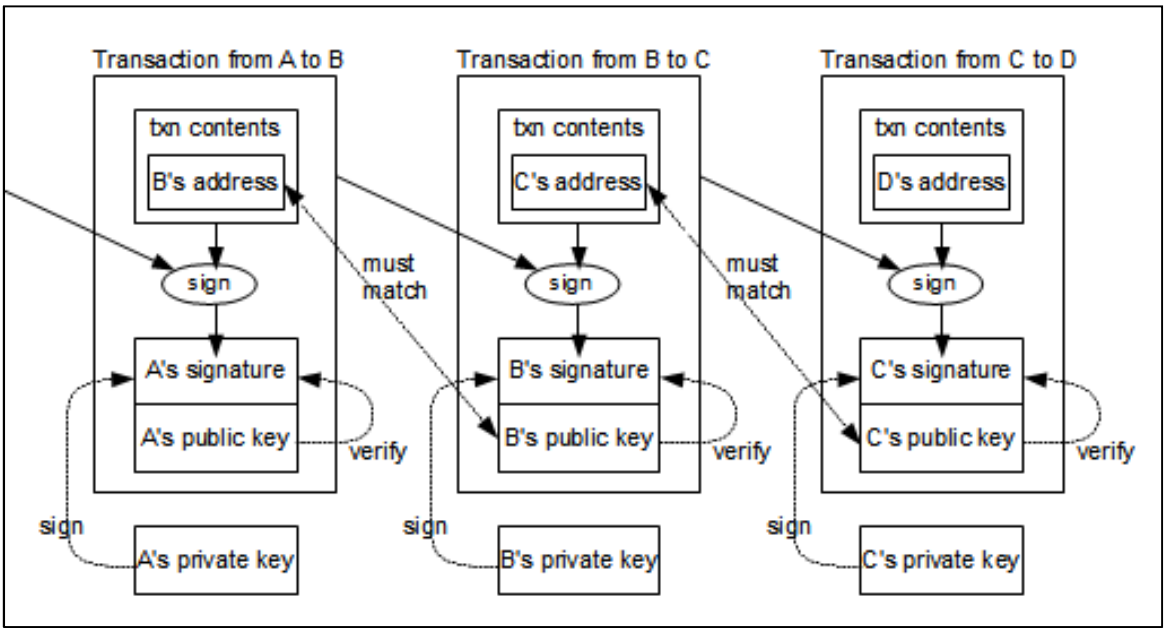

Figura 2.4: Struttura delle transazioni di Bitcoin (Fonte: http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.htm).

Aiutandoci con la figura sopra si può capire meglio cosa si intende per "catena di firme digitali". Considerando la transazione centrale, ovvero lo scambio da **B** a **C**, possiamo dedurre quanto segue:

- La transazione "da **A** a **B**" costituisce l'input, che consente poi a B di mettere in atto la transazione da "**B** a **C**"; l'indirizzo di **B** memorizzato nella transazione input deve corrispondere con la chiave pubblica di **B** inclusa nella transazione in oggetto dalla quale deriva.
- **B** autorizza la transazione firmandola con la sua chiave privata, verificando che la chiave pubblica di prima corrisponda. La chiave pubblica di B entra in gioco solo quando **B** decidere degli input che gi appartengono.
- In questo caso particolare **B** utilizza un solo input, derivante dal precedente scambio con **A**, ma nella realtà le transazioni avvengono riscattando diversi input e verso molteplici output, creando catene di legami tra una transazione e l'altra molto più fitte. Per esempio **B** avrebbe potuto mandare un numero maggiore di bitcoin a **C**; in questo caso avrebbe dovuto riscattare interamente l'input ricevuto da **A**, ed inoltre altri input ricevuti da altri individui in precedenza, fino a che il numero di bitcoin da inviare a **C** non è raggiunto.

Questa particolare struttura delle transazioni implica che le unità di bitcoin non esistono come entità a sé stanti; ogni bilancio positivo di bitcoin associato ad un indirizzo può essere visto come un insieme di mattoncini di grandezza diversa rappresentanti ciascuno un bilancio di bitcoin di grandezza diversa. Aiutandoci con la *figura 2.5*, il mattoncino più grande possibile è quello derivante dalla ricompensa percepita dai miners che sono di nuova emissione (per la spiegazione si rimanda al parag. 2.5); a questo punto il minatore ***A*** può spendere parte della ricompensa, inviando un certo ammontare all'utente **C**; l'utente **C** compra un bene dal negozio di **E** e frazionа ulteriormente i bitcoin originariamente appartenuti al minatore; le operazioni appena descritte sono svolte parallelamente anche dal minatore **B** e poi dall'utente **D**; E deterrà un certo bilancio di bitcoin, ma derivanti da diverse fonti primarie (**A** e **B**). Ogni bilancio che un determinato utente viene a detenere può essere fatto di innumerevoli mattoncini di colori diversi (chiamati input), di cui si è sempre tenuto traccia ad ogni frazionamento, allo scopo di ricollegarli tutti ad una fonte e conoscere tutte le operazioni storiche, risolvendo così il problema del double-spending. Un utente può certamente dire di possedere per esempio 10 bitcoin, ma ciò che si nota "dietro le quinte" è che quello specifico utente possiede degli input di bitcoin che sommati danno 10 bitcoin; tale soggetto potrebbe per esempio avere 1 bitcoin derivante da **X** (che a sua volta deriva da …), 5 bitcoin che derivano da **Y** (che a sua volta derivano da …) e 4 bitcoin derivanti dal minatore **Z** (che in questo caso non derivano da nessuno perché di nuova emissione).

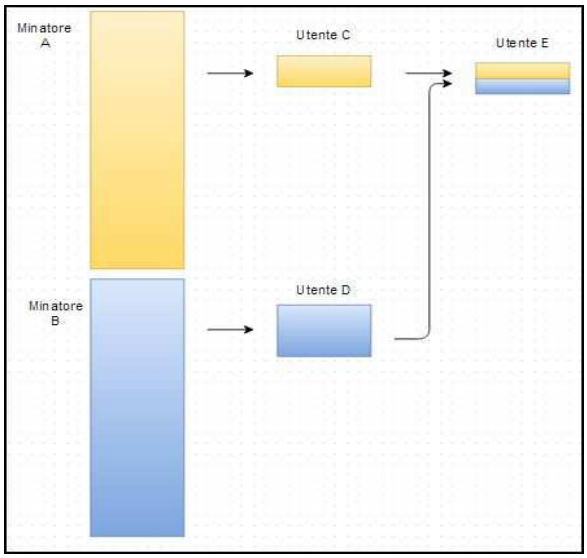

Figura 2.5: struttura degli scambi di bitcoin.

Scendendo nei dettagli ed esplorando la blockchain attraverso blockexplorer.com, si può notare che ogni transazione memorizzata in un blocco risulta un insieme di tre principali informazioni:

1) **Header** o carta di identità della transazione, a sua volta contenente i seguenti dettagli:
   a) Hash della transazione: hash identificativo di una specifica transazione, ovvero che ricomprende e sintetizza tutte le informazioni che concernono la specifica transazione. Tale codice riassume nel complesso le seguenti informazioni: numero di versione (necessario a verificare l'adesione alla versione del sistema di regole stabilita dal consenso), lista di input e output e l'orario di chiusura del blocco in cui è inserita (*lock time*).
   b) Numero del blocco risolto in cui questa transazione è stata memorizzata;
   c) Numero di inputs: numero delle diverse precedenti transazioni fornitrici complessivamente dell'ammontare di bitcoin impiegato nella transazione in oggetto;
   d) Totale dei BTC riscattati: somma dei bitcoin risultanti dalle transazioni di cui illustrato al punto c);
   e) Numero degli outputs: numero dei diversi indirizzi Bitcoin a cui sono inviati i BTC in uscita;
   f) Totale dei BTC in uscita: somma dei bitcoin in uscita nella transazione in oggetto;
   g) Size: misura di memoria dei dati della transazione in termini di spazio fisico occupato sul disco. Il sistema Bitcoin utilizza questa misura per valutare il limite di misura dell'intero blocco e le spese di transazione;
   h) Commissione: ammontare di BTC attribuiti al miner del blocco come commissione di transazione, se prevista, rappresentata dalla differenza tra il totale dei BTC riscattati e il totale dei BTC in uscita.

2) **Dettaglio degli input**: tabella elencante il dettaglio delle transazioni fornitrici dell'ammontare di bitcoin impiegato nella transazione in oggetto. In ogni riga si trovano hash di ogni transazione-input, ammontare trasferito e indirizzo Bitcoin del ricevente. Per ogni input si trova anche l'informazione *Script Sig*, che rappresenta la prima metà di uno script, la cui funzione è spiegata in seguito.

3) **<u>Dettaglio degli output</u>**: tabella elencante gli indirizzi Bitcoin destinatari complessivamente dell'ammontare in uscita. In ogni riga sono indicati indirizzo del destinatario, rispettivo ammontare a questi inviato ed hash dell'eventuale transazione di cui questa in oggetto ne rappresenta l'input. Per ogni output si trova anche l'informazione *Script Public Key*, che invece rappresenta la seconda metà di uno script, la cui funzione è spiegata in seguito.

Proviamo a illustrare la struttura delle transazioni attraverso un semplice esempio: **A** vuole inviare a **B** 50 BTC. **A** è sicuro di possedere o di non aver già speso quei 50 BTC, che gli sono stati inviati da **X** in una precedente transazione (l'esempio prevede un solo input ed un solo output, anche se nella realtà non è sempre così). **A**, **B** e **X** sono gli indirizzi utilizzati in queste due transazioni, la transazione **t1** è lo scambio tra **A** e **B**, mentre la transazione **t0** è lo scambio precedente tra **X** e **A**.

Andando ad ispezionare la blockchain le due transazioni appariranno rispettivamente come le due tabelle seguenti:

Transazione 1 (t1): A invia a B 50 BTC

Inputs:			
Precedente Output	**Ammontare**	**dall' Indirizzo**	**Script Sig**
t0	50 BTC	X	…

Outputs:			
Riscattato all'Input	**Ammontare**	**all'indirizzo**	**Script PubKey**
Non ancora riscattato	50 BTC	B	...

Tabella 2.2: Struttura delle transazione come apparirebbe nella blockchain.

Transazione 0 (t0): X invia a A 50 BTC

Inputs:			
Precedente Output	**Ammontare**	**dall' Indirizzo**	**Script Sig**
-	-	-	-

Outputs:			
Riscattato all'Input	**Ammontare**	**all'indirizzo**	**Script PubKey**
t1	50 BTC	A	…

Tabella 2.3: Struttura delle transazione come apparirebbe nella blockchain.

Partendo dalla transazione **t0** vediamo che **X** ha inviato 50BTC ad **A**. **A** per poter riscattare tale output, trasformandolo in input nella transazione **t1**, deve provare di possedere la chiave privata, da cui proviene la chiave pubblica da cui a sua volta proviene l'indirizzo **A**. Lo ***Script PubKey*** rappresenta una condizione per poter spendere i bitcoin riferiti a quell'output, ed è creato dal mittente, in questo caso **X**. **A** desidera inviare 50BTC a **B**, quindi metterà in piedi una transazione aggiungendo tanti output che ritiene di possedere quanto è la somma da inviare. In **t1**, **A** aggiungerà l'input **t0**, sufficiente a inviare a **B** la somma desiderata. Affinché la transazione vada a buon fine è necessario che A provi di possedere l'ouput in questione, e a questo scopo entra in gioco lo ***ScriptSig*** di **t1**, che deve "combaciare" con lo ***Script PubKey*** di **t0**. **X** crea uno ***Script PubKey*** a partire dall'indirizzo di **A** che conosce, sapendo che un indirizzo non è altro che un hash creato a partire dalla sua chiave pubblica corrispondente. **A** proverà di avere il diritto di reclamare quei bitcoin fornendo all'output di **t0** la chiave pubblica corrispondente a quell'indirizzo, e firmandolo con la rispettiva chiave privata, da cui la chiave pubblica deriva. Sempre all'interno di **t1**, **A** provvedrà a costituire lo ***Script PubKey*** che **B** a sua volta dovrà rispettare per poter spendere tale output.

Alcune ulteriori considerazioni:

- **Il "*change*" o resto di una transazione**: un utente può disporre di diversi output derivanti da diverse e precedenti transazioni. All'utente del wallet risulterà intuitivo conoscere il bilancio di bitcoin in suo possesso, in modo da poterli spendere a suo piacimento. Tuttavia i bitcoin sono memorizzati nella blockchain sottoforma di

output di differenti transazioni, per cui i vari output non sono uniti a formare il bilancio che invece appare all'interno di un wallet.

Ritornando all'esempio precedente, supponiamo che **B**, oltre a possedere i 50 BTC inviatigli da **A**, possieda anche ulteriori 30BTC inviatigli in passato da **Y** (attraverso la transazione **t00**), e decida a questo punto di inviare 60 BTC a **C** (attraverso la transazione **t2**). **B** può certamente effettuare questa nuova transazione, perché possiede complessivamente 80 BTC, tuttavia dovrà riscattare entrambi gli output in suo possesso (cioè prendere tali output e firmarli con la propria chiave privata), perché non posside né un unico output da 60BTC, né un insieme di output che sommati diano quello stesso ammontare. Come sarà strutturata allora questa transazione?

Transazione 2 (t2): B invia a C 60 BTC

Inputs:			
Precedente Output	**Ammontare**	**dall' Indirizzo**	**Script Sig**
t1	50 BTC	A	-
t00	30BTC	Y	-

Outputs:			
Riscattato all'Input	**Ammontare**	**all'indirizzo**	**Script PubKey**
Non ancora riscattato	60 BTC	C	-
Non ancora riscattato	20 BTC	B	-

Tabella 2.4: Struttura delle transazione come apparirebbe nella blockchain.

Entrambi i precedenti output di B derivanti da **t1** e **t00**, saranno i nuovi input di questa transazione, in cui in assenza di commissioni il totale di BTC riscattati sarà pari al totale di BTC in uscita, cioè 80 BTC. Tuttavia 60 BTC sono effettivamente "spesi" perché passano da **B** a **C**, mentre i 20 BTC ritornano al proprietario **B** come resto e sottoforma di nuovo e diverso output di cui poter disporre. In altri termini non è possibile disporre dei propri output in modo parziale. Questi saranno riscattati per intero e tutt'al più sarà attribuito un nuovo output come resto risultante. Lo scopo di questa struttura delle transazioni è che ogni outnput contenga i riferimenti della chiave pubblica del suo proprietario, in modo che quando il proprietario li

vorrà spendere, firmandoli con la sua chiave privata, la validità sarà confermata dal corretto abbinamento tra chiave pubblica e privata.

Generalmente i wallet Bitcoin, in presenza di resti provvedono a inviare tali quantitativi a nuovi indirizzi associati allo stesso utente, che vengono "pescati" dalla key-pool a disposizione di ogni wallet, anche per esigenze di anonimità delle transazioni.

La questione del resto delle transazioni assume rilevanza quando si vuole compiere delle analisi in merito al volume degli scambi di bitcoin all'interno del network. Poiché la voce "*totale bitcoin in uscita*" tiene conto anche dei bitcoin che ritornano al mittente come resto, e che quindi non sono effettivamente spesi, ecco che un'analisi basata su questo dato potrebbe risultare parecchio distorta dal reale volume speso nel sistema, perché infatti sarebbero computati tutti gli output di tutte le transazioni, senza considerare che spesso il secondo output rappresenta il change che ritorna nella disponibilità del mittente.

- **Le transazioni di bitcoin sono divisibili:** si possono inviare anche frazioni di bitcoin, e ciò rende possibile anche transazioni di importi molto bassi a seconda del tasso di cambio con le altre valute tradizionali. L'unità più piccola è chiamata "*satoshi*" in onore del suo stesso ideatore, corrispondente a 10^{-8} BTC (0,00000001 BTC). Nella *tabella 2.5* sono elencate le frazioni di bitcoin, i rispettivi simboli e valori decimali.

Unità	Abbreviazione	Decimale (BTC)
megaBitcoin	MBTC	1.000.000
kiloBitcoin (raro)	kBTC	1.000
decaBitcoin (raro)	daBTC	10
Bitcoin	BTC	1
deciBitcoin (raro)	dBTC	0,1
centiBitcoin (raro)	cBTC	0,01
milliBitcoin	mBTC	0,001
microBitcoin	µBTC	0,000001
Finney	-	0,0000001
Satoshi	-	0,00000001

Tabella 2.5: Lista delle unità di bitcoin più usate e rispettivi simboli e valori decimali. (Fonte: bitcoin/wiki).

2.4.2. La struttura dei blocchi

Ogni blocco è composto da due parti principali: il block header, e la lista di transazioni ricomprese nel blocco. Di seguito si illustrano soltanto le informazioni contenute in un blocco, lasciando al paragrafo 2.5 la spiegazione di cosa sono e della loro funzione.

Block 351360

Short link: http://blockexplorer.com/b/351360

Hash:
00000000000000012b2d7193a952e6a4afaabe8147fce6af6e0981e4652231b

Previous block:
000000000000000001246da72e1a85dea04574f6da0de565a109c13a1f1f5857e

Time: 2015-04-09 08:10:42

Difficulty: 49 446 390 688.241438 ("Bits": 18163c71)

Transactions: 1992

Total BTC: 19179.50396074

Size: 749.066 kilobytes

Merkle root:
023880f95a57e3a94e083987b2c57633c7c6fb46a98fb53f703d7f2169fe1d64

Nonce: 1662219264

Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
d30fd91ad4...	0	0.127	Generation: 25 + 0.28260436 total fees	1PE7LXcntsLvavM2KXpJGNu51UbDhC3u63: 25.28260436

Figura 2.5: Struttura del blocco (Fonte: blockexplorer.com).

1. **Block Header**: rappresenta il documento di identità del blocco e contiene le seguenti informazioni:
   a) Numero o altezza del blocco: numero progressivo del blocco aggiunto alla catena. La blockchain inizia con il *genesis block*, avente numero 0.
   b) Hash: hash identificativo di uno specifico blocco. Tale codice risulta dall'hashing dell'insieme delle seguenti informazioni: numero di versione (riguarda la versione del software utilizzato, necessario a verificare l'adesione al sistema di regole stabilite dal protocollo), hash del blocco precedente in modo da risultarvi collegato, merkle root, lock time, misura della memoria e nonce.
   c) Hash blocco precedente: riassume tutte le informazioni del blocco precedente;
   d) Hash blocco successivo: riferimento al blocco successivo (se si apre il blocco corrente tale riferimento non si trova, in quanto deve ancora venire agganciato alla blockchain);
   e) Tempo: data e orario (UTC) in cui il blocco è stato risolto;
   f) Difficoltà: parametro che misura la difficoltà di risolvere il blocco, intesa come tempo di elaborazione necessario a risolvere il problema crittografico nell'operazione di mining;
   g) Transazioni: numero di transazioni ricomprese nel blocco.
   h) BTC totali: numero totale dei bitcoin inviati nelle transazioni del blocco, comprese le commissioni di transazione;
   i) Size: memoria occupata complessivamente dai dati di tutte le transazioni ricomprese nel blocco;
   j) Merkle Root: hash che sintetizza tutte le transazioni ricomprese nel blocco. Le diverse transazioni rappresentano le "foglie" del *merlke tree*[19]. Gli hash delle diverse transazioni sono a loro volta hashati a coppie fino ad arrivare ad unico hash che ricomprende tutti gli altri;
   k) Nonce (number used once): particolare campo utilizzato nel processo di *mining*, a cui si rimanda.

[19] Merkle tree: dati diversi hash derivanti da diverse informazioni, attraverso il merkle tree si possono sintetizzare tutte le informazioni in modo collegato in un unico, in modo che verificando la correttezza dell'hash risultante, si può constatare velocemente che si sono ricomprese adeguatamente tutte le informazioni. Merkle tree deriva appunto dalla struttura ad albero genealogico delle informazioni, che sono sintetizzate a coppie fino a giungere alla radice.

2. **Lista di transazioni**: una tabella con tutte le transazioni ricomprese nel blocco, in cui per ogni transazione diversa sono indicati: relativo hash, importo della commissione, misura della memoria occupata, lista degli indirizzi rappresentanti l'input della transazione e rispettivi quantitativi riscattati, indirizzi riceventi e rispettivi quantitativi ricevuti.

La prima transazione che compare in ogni lista di un qualsiasi blocco è generalmente una transazione particolare, diversa da tutte le altre, chiamata *coinbase*. Questa transazione rappresenta la ricompensa dovuta al miner che ha risolto il blocco, cioè ha validato e ricompreso le ultime transazioni avvenute all'interno di un blocco, svolgendo l'attività di mining, che analizzeremo più dettagliatamente nel prosieguo di questo capitolo. Al miner sono dovute tutte le commissioni delle transazioni impacchettate nel blocco più una somma fissa che attualmente è di 25 BTC. Quest'ultimo importo rappresenta bitcoin di nuova emissione, che va dunque ad aumentare il numero totale dei bitcoin presenti nel sistema. La coinbase è una transazione diversa in quanto priva di input, mentre la ricompensa più le commissioni possono essere inviate sia ad un unico indirizzo che a più indirizzi, perciò dal punto di vista degli output questa transazione è uguale ad ogni altra transazione standard. Per ogni blocco c'è un'unica coinbase, tuttavia questa non può essere spesa fino a che non ha ottenuto almeno 100 conferme[20], ovvero occorre attendere la produzione di almeno altri cento blocchi, che in termini di tempo equivale ad un'attesa nell'ordine delle 16 ore e 40 minuti.

Il motivo di questa attesa è precauzionale, per la possibilità che si verifichi il fenomeno della *biforcazione* della blockchain (*fork*). Poiché l'attività di mining è di fatto una sfida a chi tra i nodi riesce a risolvere il blocco corrente per primo allo scopo di aggiudicarsi la coinbase, può succedere che due o più nodi riescano a trovare una diversa e valida soluzione di chiusura del blocco corrente in un arco di tempo molto ravvicinato. Di conseguenza al blocco precedentemente prodotto vengono agganciati due o più blocchi diversi e validi, creando una biforcazione nella blockchain. La *figura 2.6* propone uno schema della blockchain, che ha origine dal blocco genesi (verde) e si sviluppa in lunghezza nei blocchi blu; a volte possono capitare delle biforcazioni (in corrispondenza dei blocchi grigi).

[20] Conferma: una transazione riceve una conferma quando viene memorizzata all'interno di un blocco; ad nuovo blocco prodotto ed agganciato a quest'ultimo, tale transazione riceve una conferma in più.

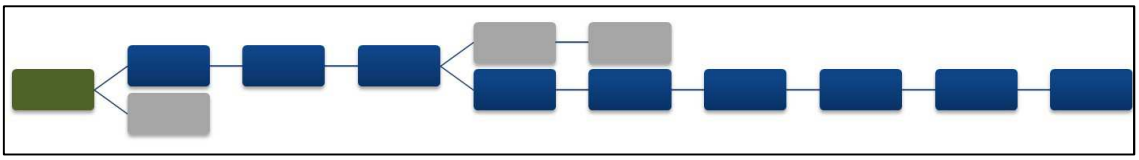

Figura 2.6: La Blockchain di Bitcoin (in blu) che ha origine dal blocco genesi (verde). I blocchi in grigio rappresentano i blocchi orfani frutto di biforcazioni. (Fonte: paymentobserver.com).

I miners comunicano la soluzione per la chiusura del blocco a tutti gli altri nodi del network, che procedono a verificare che non vi siano transazioni inconsistenti tra quelle incluse nell'ultimo blocco e le precedenti registrate nella blockchain. Se uno dei due blocchi ricomprende transazioni contrastanti le precedenti, allora quel blocco non riceve conferme, altrimenti se entrambi validi (può capitare perché i problemi crittografici svolti dai miners contemplano più soluzioni valide) i nodi ne scelgono uno dei due, solitamente il primo che compare loro nei rispettivi dispositivi.

La conferma di un blocco è espressa dai minatori semplicemente scegliendo da quale dei due partire per agganciare il blocco successivo. Può succedere che per brevi periodi di tempo si sviluppino due biforcazioni parallele, ma tra le due prevarrà quella dove sarà stata impiegata la maggioranza della forza computazionale complessiva, e i minatori che inavvertitamente stavano lavorando a quell'altra, torneranno allo sviluppo della principale.

I blocchi che non fanno parte della catena principale sono detti blocchi orfani, e i minatori che li hanno creati non hanno diritto a ricevere ricompense. Per la possibilità che si generino biforcazioni dalla sua accettazione come pagamento, anche la coinbase attribuita al minatore del genesis block non è immediatamente spendibile.

2.5 Il Mining:

Come rendere possibile un sistema di pagamento decentralizzato? Come sopperire alla mancanza di un'autorità centrale che stabilisca la politica monetaria per quella determinata valuta? Come garantire e alimentare la fiducia in un sistema così diverso dai sistemi di pagamento tradizionali, soprattutto per la sensibilità del tema trattato, ovvero la sicurezza del nostro denaro? La risposta a tutte queste domande è il mining.

Spesso erroneamente si ricollega l'attività di mining alla sola produzione ed emissione di nuovi bitcoin, tuttavia non è questo il suo scopo principale. Il vero obiettivo di tale processo è mantenere l'integrità e l'autenticità della blockchain, che per gli utenti di Bitcoin rappresenta un vero e proprio conto bancario. Solo se questo registro mantiene le caratteristiche menzionate, chiunque possieda dei bitcoin può stare tranquillo che quel denaro gli appartiene; se invece si rivelasse fragile a tentativi di contraffazione, finalizzati per esempio a convalidare più transazioni tra loro inconsistenti (double-spending), la fiducia nel sistema svanirebbe e Bitcoin sarebbe destinato a fallire.

Ma da chi e come viene svolta questa attività? Teoricamente può essere svolta da tutti, a patto che si installi il client Bitcoin sul proprio computer. Il mining sfrutta la potenza di calcolo dei dispositivi hardware messi a disposizione dai nodi della rete, ed è stato ideato dallo stesso Nakatomo difficile e dispendioso in termini di tempi di elaborazione del calcolatore, in modo che vengano prodotti un certo numero di nuovi blocchi in un intervallo di tempo prefissato, a prescindere dal numero di transazioni che avvengono nel network. Infatti se nel network avvengono poche transazioni, queste non possono essere messe in attesa fino a che non si raggiunge una determinata soglia, altrimenti la praticità come sistema di pagamento svanirebbe; inoltre i primi blocchi minati non contenevano transazioni, eccetto le coinbase, allo scopo di creare e mettere in circolazione le prime unità di valuta.

Ad ogni produzione di un nuovo blocco viene emessa una quantità stabilita di nuovi bitcoin, che spettano al minatore che per primo l'ha prodotto. A tale quantità prestabilita va a sommarsi anche il totale delle commissioni delle transazioni registrate nel blocco.

In sintesi il mining è ideato per rendere sicura la blockchain, e tale sicurezza è resa possibile da quanti più nodi "onesti" sono presenti nel network, in modo da rendere difficile se non impossibile il lavoro dei nodi "disonesti" che vogliono invece modificare il registro a loro vantaggio per spendere più volte dei bitcoin già spesi. L'onestà dei nodi è "comprata" dallo stesso protocollo attraverso un particolare sistema di attribuzione di ricompense, che incentivano tale onestà.

Il motivo per cui questo processo si chiami mining vuole sottolineare la relazione tra i cercatori d'oro che impiegano sempre più sforzi per trovare nuove pepite d'oro, e i nodi che similmente impiegano sempre più potenza computazionale, costosa in termini di energia consumata, per aumentare i bitcoin in circolazione.

2.5.1. Le regole alla base del mining:

La produzione di nuovi blocchi da agganciare alla blockchain e l'emissione di nuova moneta sono strettamente collegati, tali che ogni produzione di un nuovo blocco corrisponde ad una nuova emissione di un quantitativo prefissato di bitcoin. Tutto in Bitcoin è stabilito. Indipendentemente da quante transazioni avvengono nel sistema, ogni due settimane si devono produrre mediamente 2.016 nuovi blocchi, circa 1 ogni 10 minuti, anche se nessuno effettuasse alcuna transazione. Ogni due settimane inoltre, se i nuovi blocchi prodotti si discostano dal numero obiettivo di 2.016, la difficoltà di produzione di un nuovo blocco viene rivista verso il basso o verso l'alto, a seconda che l'output di nuovi blocchi sia stato inferiore o superiore a 2.016. Il tetto massimo di bitcoin in circolazione è anch'esso prestabilito, ed è (o meglio sarà) di circa 21 milioni di unità. Infine anche la quantità di nuovi bitcoin emessi ad ogni produzione di un nuovo blocco è fissata. Tale ricompensa si attestava originariamente in 50 BTC per blocco, e viene dimezzata progressivamente ogni 210.000 nuovi blocchi che equivalgono a circa 4 anni. Il primo dimezzamento si è verificato il 28 novembre 2012, per cui attualmente la ricompensa è quantificata in 25 BTC.

Quando in futuro la ricompensa sarà prossima allo zero, l'unica remunerazione per i minatori saranno le commissioni di transazione. Nel 2040 la ricompensa per ogni blocco sarà inferiore a 0,5 BTC, per cui il futuro di Bitcoin dipenderà dalla diffusione che riuscirà ad ottenere come sistema di pagamento, in quanto solo se avverranno numerose

transazioni i minatori potranno essere incentivati a continuare la loro fondamentale attività.

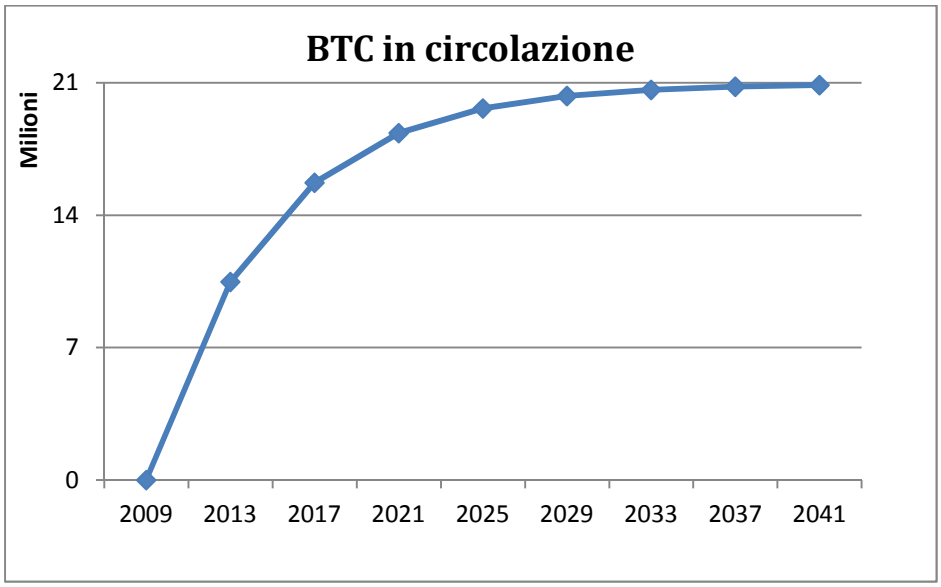

Grafico 2.1: Curva di emissione di bitcoin nel corso del tempo. Il numero di bitcoin per blocco generato decresce geometricamente, dimezzandosi ogni 4 anno. Il numero di bitcoin in circolazione non supererà mai i 21 milioni di unità.

2.5.2. Cos'è e come funziona:

Il mining consiste in un insieme di attività finalizzate alla corretta e costante registrazione delle transazioni che avvengono nel sistema. Tali attività si basano sulla risoluzione di un proof-of-work (prova di lavoro), una sorta di compito da far svolgere al proprio calcolatore che richiede tempo di elaborazione. In particolare Bitcoin impone la risoluzione di una algoritmo crittografico molto simile alla funzione hashcash, un sistema di prova di lavoro proposto da A. Back nel 1997, utilizzato per rendere costoso in termini di tempo di elaborazione, e quindi di energia consumata, l'invio di spam via e-mail. Il problema ha la caratteristica di essere difficile e dispendioso da risolvere, ma una volta trovata la soluzione verificarne la validità è molto facile.

Tale compito consiste nel sottoporre ad hashing una serie di dati specifici componenti il block header; l'hash risultante per essere valido deve rispettare dei criteri. I campi di informazione da sottoporre ad hashing sono elencati nella tabella seguente:

Block Header	Size (bytes)
Version Number	4
Hash Blocco Precedente	32
Merkle Root	32
Time	4
Bits	4
Nonce	4
	Tot. 80

Hash Nuovo Blocco

Tabella 2.7: dettaglio dei campi da sottoporre ad hashing per produrre l'hash del nuovo blocco. (fonte: en.bitcoin.it/wiki).

Il *merkle root*, come visto in precedenza, è l'hash che sintetizza la lista di transazioni ricomprese nel blocco, compresa la coinbase. Minare un blocco contenente una sola transazione non rende il mining più veloce, per cui i minatori saranno incentivati a includere un numero ampio di transazioni, in modo da far proprie le relative commissioni.

Il *bits* è la codifica del *target*, un numero di 256 bit. L'hash del nuovo blocco per essere ritenuto valido deve essere inferiore o uguale al target. In altri termini il minatore deve trovare un hash che sintetizzi le informazioni della *tabella 2.7* che inizi con tanti zeri (da sinistra a destra) almeno quanti quelli con cui inizia il target; il lavoro che dovrà compiere il processore sarà esponenziale al numero di zeri che compongono il target. Il parametro del target esprime dunque quello della difficoltà[21] del mining, parametro di riferimento che misura appunto lo sforzo computazionale richiesto per la risoluzione di un blocco; la difficoltà è legata in maniera inversamente proporzionale al target.

Il *nonce* (*number used once*) è un parametro che viene modificato ogniqualvolta l'hash ottenuto è maggiore del target (in genere il parametro parte da 0 e viene incrementato progressivamente). Per le proprietà dell'hashing, una piccola modifica di un solo dato in input, comporterà un hash in output totalmente diverso dal precedente. Inoltre l'informazione nonce è inclusa anche nella coinbase (*extraNonce*), per cui una modifica del nonce comporta anche una modifica del merkle root.

[21] La difficoltà è soltanto una rappresentazione più intuitiva del target. La difficoltà corrente esprime quanto più tempo è richiesto per risolvere un blocco rispetto alla situazione in cui la difficoltà è impostata al minimo cioè 1.

Per fare un esempio, senza considerare la reale lunghezza (bit) delle stringhe che caratterizzano tali informazioni, se il target corrente fosse di *00000111*, e dopo aver sottoposto il block header ad hashing il risultato è *003e84n4*, il minatore non avrebbe trovato una soluzione valida, perché il target ha 5 zeri iniziali e il risultato solo 2; il minatore deve aumentare progressivamente il nonce ad ogni nuovo tentativo, finché il risultato non inizia con almeno 6 zeri.

Trovare un hash che rispetti il target equivale a vincere una lotteria, poiché ad ogni nuovo tentativo (ad ogni incremento del nonce) la probabilità di risolvere il blocco rimane sempre la stessa. Il mining è un problema che va risolto per *brute-force*, cioè per continui tentativi fino a che non si trova una soluzione accettabile.

Questo sistema di regole che i minatori devono rispettare per produrre un nuovo blocco è necessario affinché le tempistiche prestabilite (10 minuti) siano rispettate. In sintesi il mining può essere scomposto nelle seguenti fasi:

- Le transazioni sono trasmesse ai nodi grazie alla tecnologia p2p;
- Ogni nodo colleziona le transazioni e procede alla produzione di un nuovo blocco, elaborando il merlke root di quella specifica lista a cui va aggiunta la prossima coinbase, e costruendo la tabella di input (block header) che andrà sottoposta ad hashing;
- L'hardware è sottoposto alla prova di lavoro, che può esser considerata risolta quando l'hash è inferiore al target. La soluzione viene comunicata agli altri nodi che stavano contemporaneamente lavorando alla soluzione del medesimo blocco;
- I nodi controllano che il nuovo blocco non comprenda transazioni inconsistenti, e convalidano il blocco utilizzandone l'hash per procedere alla produzione del blocco seguente, continuando lo sviluppo della blockchain.

2.5.3 Solo-mining, pool-mining e cloud-mining:

Attualmente è possibile partecipare al mining mediante tre principali alternative:

- **Solo-mining:** l'attività di mining è svolta individualmente, allo scopo di far proprie la ricompensa e la somma delle commissioni delle transazioni incluse nel nuovo blocco. L'elevata competitività attuale del mining richiede per questa specifica alternativa

degli importanti investimenti in potenza computazionale. Maggiore è la potenza di cui si dispone, maggiore è la probabilità di risolvere dei blocchi e ottenere dei profitti. Il solo-mining tuttavia non garantisce flussi di cassa continui, e può trascorre molto tempo tra un'entrata e l'altra.

- **Pool-mining:** invece che minare individualmente è possibile farlo collettivamente, unendosi ad una mining pool, in cui più soggetti mettono a disposizione la propria potenza di calcolo e si suddividono i profitti proporzionalmente al contributo fornito. Il pool-mining permette di partecipare al mining anche se non si dispone di un'elevata capacità di calcolo, necessaria invece per il solo-mining. Generalmente questa seconda alternativa garantisce flussi di entrate di bitcoin minori ma continui.
- **Cloud-mining:** è possibile partecipare all'attività di mining senza possedere materialmente i dispositivi hardware necessari, eliminando i problemi relativi alla manutenzione e alla collocazione fisica di tali apparecchiature. Attraverso il cloud-mining è possibile prendere a noleggio in un determinato ammontare di potenza computazionale e farne propri i profitti in cambio di un canone di locazione.

2.5.4 Le commissioni di transazione:

Una delle più importanti caratteristiche di Bitcoin sono le basse commissioni di transazione rispetto a tutti gli altri strumenti per i pagamenti elettronici già esistenti. La somma delle commissioni delle transazioni verificate e registrate in un blocco vanno a remunerare, unitamente alla quota fissa di nuovi bitcoin, il lavoro svolto dai minatori. Poiché in futuro tale quota fissa è destinata a ridursi gradualmente fino a diventare prossima allo zero in quanto è previsto un tetto massimo di circa 21 milioni di bitcoin in circolazione, la remunerazione dei minatori sarà costituita soltanto dalle commissioni di transazione. A quel punto Bitcoin continuerà il suo corretto funzionamento solo se la sua diffusione ed utilizzo come strumento per i pagamenti saranno tali da garantire ai minatori un'adeguata remunerazione, affinché saranno incentivati al prosieguo della loro fondamentale attività anche in futuro.

Tali commissioni sono a carico del mittente, ma molte transazioni possono anche non prevedere nessuna commissione, a patto che rispettino determinate condizioni. L'entità

della commissione dipende dalla priorità attribuita alla transazione, e la priorità è stabilita attraverso la ponderazione dei seguenti fattori:

- "Età" degli input: un input è più vecchio di un altro se non viene speso da più tempo;
- Dimensione (size) della transazione: dipende dal numero di input che verranno spesi nella transazione e dal numero di output destinatari, compreso l'output del change.

Le transazioni che spendono input più vecchi e che hanno output più elevati avranno priorità più elevata rispetto a transazioni che spendono input più recenti e hanno output di piccoli importi.

Una transazione può essere processata senza includere una commissione se rispetta le seguenti condizioni:

- Ha una dimensione inferiore a 1000 bytes;
- Gli output sono almeno di 0,01 BTC;
- La priorità raggiunge un determinato livello.

Tecnicamente, anche tutte le altre transazioni, pur non rispettando i parametri di cui sopra, possono essere processate senza includervi una commissione, tuttavia il loro esito positivo o negativo dipenderà soltanto dai minatori, in quanto potrebbero non essere mai accettate e quindi non venire mai incluse in un blocco. Le recenti versioni del client Bitcoin, per quanto riguarda i wallet, sono programmati per includere automaticamente una commissione a seconda della transazione che si sta per processare, mentre per quanto riguarda il mining sono in grado di riconoscere se tale transazione possiede o meno una commissione adeguata.

Una transazione standard prevede generalmente una tassa di 0,0001 BTC (circa 0,02€). Per standard si intende entro la soglia di 1.000 bytes, posto che ogni input pesa 148 bytes, ogni output 34 bytes, e che al totale vanno aggiunti 10bytes di default. Si tenga presente che mediamente le transazioni pesano circa 500 bytes. Per transazioni che ricomprendono più input o che inviano denaro a più destinatari, superando la soglia dei 1.000 bytes, è consigliato includere una commissione più alta.

L'esistenza di una micro tassa, oltre che come modo per incentivare i minatori a prendere in considerazione la transazione in oggetto e includerla al più presto in un blocco, serve anche a negare la cosiddetta *dust spam*. Questo tipo di spam è un attacco di

tipo *denial of service*, che può essere apportato da chiunque abbia interessi al malfunzionamento del sistema e voglia minarne la stabilità, e consiste nel processare numerosissime transazioni che verso altrettanti indirizzi ma di volumi di bitcoin irrisori (per esempio inferiori al centesimo di dollaro), aumentando la dimensione della blockchain e rendendo il mining più dispendioso senza un effettivo scopo di trasferimento di denaro.

2.5.5 L'onestà e la disonestà dei nodi

Il funzionamento di Bitcoin come sistema decentralizzato dipende dall'onestà dei nodi che ne verificano e convalidano le transazioni, escludendo ogni possibilità di double-spending. Un nodo è onesto se impiega la propria forza computazionale per produrre blocchi che non contengano transazioni inconsistenti tra loro o con quelle precedentemente registrate nella blockchain, ed inoltre se concorrono al mining dei blocchi da agganciare alla catena progressivamente più lunga.

La catena dei blocchi più lunga, quella che va dal blocco genesi al blocco corrente, manifesta la maggioranza, intesa come la sequenza di blocchi che ha richiesto il maggior sforzo computazionale per essere prodotta (data la somma dei proof-of-work risolti per arrivare a quel punto) nonché l'adesione ed accettazione di quella traccia blocco dopo blocco, e la volontà di continuare ad allungarla.

Diversamente un nodo potrebbe comportarsi in maniera disonesta, ma cosa potrebbe fare?

Un nodo, non possedendo le chiavi private relative agli indirizzi di alti utenti di Bitcoin, non può semplicemente sottrarre fondi altrui e accreditarli nel proprio indirizzo. Il suo lavoro è collezionare le transazioni e registrarle, ma per esempio gli risulterebbe impossibile manomettere una singola transazione e accreditare l'importo al proprio indirizzo, perché la crittografia a protezione del sistema è praticamente ineludibile, considerando che è impossibile ricavare la chiave privata a partire da quella pubblica o dall'indirizzo. L'unico modo per rubare i fondi di un utente azzerandogli l'indirizzo, bensì occorre sferrare un attacco ai servizi connessi a Bitcoin come i wallet o gli exchange tentando di rubare le chiavi private come già capitato in passato. In questi

attacchi non è infatti la blockchain ad essere presa di mira, ma computer, i server o qualsiasi "luogo" in cui possa essere memorizzata una chiave privata.

Ci sono due tipi di attacchi che un nodo disonesto potrebbe tentare di mettere a segno, il *double-spending attack* e il *51% attack*:

1. **Double-spending attack**

Con questo tipo di attacco il minatore disonesto ha l'obiettivo di frodare uno specifico commerciante, che crede di aver ricevuto il pagamento salvo scoprire in un successivo momento che la transazione non è andata a buon fine; il minatore in questione è il cliente del commerciante obiettivo dell'attacco, per cui lo chiameremo nodo/cliente. Il double-spending è la possibilità di spendere una stessa unità di valuta digitale più volte, problema risolto in maniera decentralizzata da Bitcoin attraverso la tenuta della blockchain, che tuttavia si mostra vulnerabile a questo tipo di attacco.

Quando un blocco viene risolto, le transazioni in esso contenute si dicono confermate una volta, e ad ogni blocco che si aggiunge a quest'ultimo ricevono via via una conferma in più (per esempio una transazione processata e inclusa in un blocco un'ora fa avrebbe in questo momento sei conferme, ovvero cinque blocchi sarebbero stati progressivamente agganciati a quello in cui è inclusa). La conferma è sostanzialmente la prova che i minatori hanno accettato quella versione della blockchain, e stanno lavorando per continuarne la "storia". Poiché esiste la possibilità che si creino delle biforcazioni nella catena e risulti successivamente prevalere una versione della blockchain piuttosto di quell'altra, una transazione non può essere ritenuta sicura dal double-spending fino a che non ha ricevuto un certo numero di conferme.

Sfruttando questo aspetto il nodo disonesto nonché cliente del commerciante bersaglio della frode, potrebbe mettere a segno un double-spending attack nel seguente modo:

- Il nodo/cliente processa una transazione a favore del commerciante (chiamiamola transazione **A**), per esempio nell'ambito di un acquisto online;
- Il commerciante vedrà comparire nella blockchain la transazione a suo favore dopo una decina di minuti, e quindi avrà ricevuto una conferma;

- Il commerciante che ignora le cattive intenzioni del cliente potrebbe già procedere alla spedizione del bene, incurante che una o due conferme non gli garantiscano il pagamento al 100%;
- Ancora prima che la transazione che **A** sia inclusa in un blocco, il nodo/cliente lavora segretamente (strategia detta *selfish mining*[22]) alla produzione di un altro blocco contenente una transazione (**B**) che invia gli stessi bitcoin a un diverso che pur gli appartiene, ed escludendo **A** che risulterà a questa inconsistente;
- Il nodo/cliente comunicherà al network solo la transazione **A**, poiché starà già lavorando segretamente al blocco che andrà a includere **B**, altrimenti i nodi vedrebbero che **A** è inconsistente con **B** e il commerciante non vedrebbe alcuna conferma;
- Si produrrà quindi una biforcazione formata da un blocco contenente la transazione **A**, e un altro contenente invece **B**, come illustrato nella figura seguente;
- Affinché l'attacco abbia successo è necessario che la biforcazione originata dal blocco contenente **B** sia più lunga dell'altra, per il fatto la catena più lunga rappresenta il maggior sforzo speso dal blocco genesi a quello corrente e quindi la maggioranza, e perché ciò accada potrebbe richiedere al nodo/cliente di minare ulteriori blocchi successivi in modo da battere la catena parallela;
- A quel punto gli altri nodi onesti passeranno a lavorare alla catena in cui è presente **B**, mentre i blocchi dell'altra biforcazione diverranno orfani, e poiché **A** è inconsistente con **B**, e **B** ha già ricevuto delle conferme, sarà rigettata dal network, con conseguenze negative per il commerciante che avrà già spedito il prodotto (*figura 2.7*).

[22] Selfish-mining: strategia attraverso cui un minatore crea intenzionalmente una biforcazione nella blockchain, risolvendo un blocco ma non comunicando la soluzione agli altri minatori. In questo modo i minatori onesti continueranno ad allungare la catena pubblica, mentre il selfish-miner produrrà nuovi blocchi da agganciare alla sua catena privata, allo scopo di rilasciarla nel network nel momento in cui sarà più lunga di quella pubblica. Se vi riuscisse renderebbe vano tutto il lavoro apportato dai minatori onesti dall'inizio della biforcazione fino a quel punto, facendo proprie tutte le ricompense per la risoluzione dei nuovi blocchi. Il selfish-mining è una particolare strategia di mining, difficile da attuare ma comunque possibile, rappresentando così una vulnerabilità di sistema.

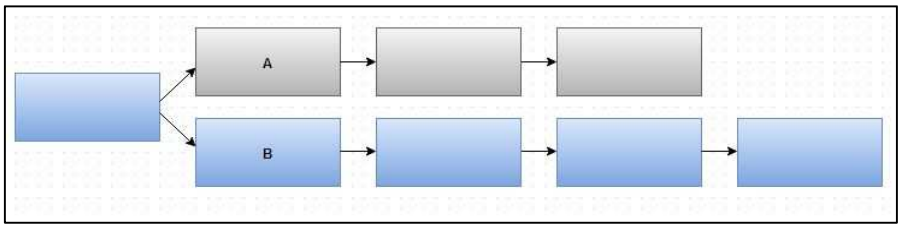

Figura 2.7: double-spending attack andato a buon fine, in cui la transazione B è registrata correttamente, mentre la transazione A che doveva pagare il commerciante no.

A questo punto è opportuno chiederci quante conferme dovrebbe attendere un commerciante prima di essere sicuro che la transazione a suo favore sia andata a buon fine, e che non corra il rischio di essere defraudato.

Il double-spending attack è una gara tra il nodo/cliente disonesto e tutti gli altri nodi onesti del network a chi produce più blocchi a partire da quello corrente prima che avvenga la transazione **A**. I nodi onesti stanno allungando la catena con il blocco contenente **A**, mentre il nodo/cliente sta contemporaneamente minando blocchi in maniera segreta da agganciare alla catena **B**, aspettando che il commerciante abbocchi e invii il prodotto. Ma quali sono le probabilità che un double-spending attack vada a buon fine?

All'interno del suo paper Satoshi Nakamoto descrive questo problema da un punto di vista statistico, affermando che la probabilità che l'attacco abbia successo dipende dalla capacità di calcolo del nodo/cliente (*h*, percentuale della potenza di calcolo totale del network detta *hashrate*[23]) e dal numero di conferme (*n*) che il commerciante attende prima di "abboccare", e giungendo alle seguenti conclusioni:

- Se la potenza del nodo/cliente *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* (fattispecie di 51% attack che sarà illustrata in seguito);
- Dato un numero *n* di conferme, maggiore è la capacità di calcolo *h* posseduta dal nodo/cliente, maggiore è la probabilità che l'attacco abbia successo; data *h* (inferiore al 50%), all'aumentare di *n* la probabilità di successo dell'attaco diminuisce.

[23] hashrate: esprime la quantità di hash che il dispositivo è in grado di produrre al secondo. La potenza di 1GH/s corrisponde alla capacità di produrre 1 miliardo di hashes in un secondo.

- Dati i diversi livelli di potenza di calcolo del nodo/cliente, un commerciante dovrebbe aspettare di attendere le seguenti *n* conferme perché il rischio di essere defraudato scenda sotto lo 0,1%:

Potenza di calcolo *h* (% dell'hashrate complessivo)	**Numero di conferme *n***
10%	6
15%	9
20%	12
25%	16
30%	25
35%	42
40%	90
45%	341

Tabella 2.8: Numero di conferme *n* ad ogni livello di potenza di calcolo h posseduta dal nodo/cliente, affinché la probabilità di un double-spending attack sia inferiore allo 0,1% (Fonte: Nakamoto, *Bitcoin: a peer-to-peer electronic cash system*).

La "*Bitcoin developer guide*", consultabile su bitcoin.org, fornisce importanti informazioni riguardanti il funzionamento di Bitcoin, destinata soprattutto agli sviluppatori che desiderano proporre delle modifiche o sviluppare nuove applicazioni basate sul progetto di Nakamoto. In merito alla possibilità di un double-spending attack, la Guida ritiene che si dovrebbero attendere almeno sei conferme per ritenere un pagamento sicuro da tale tipo di attacco, considerando l'enorme potenza di calcolo (e quindi il capitale investito in hardware specifico) che dovrebbe possedere il nodo/cliente per poter rimpiazzare sei blocchi, ma sta ad ogni commerciante decidere quante conferme attendere, soprattutto in relazione all'importo della transazione stessa.

2. 51% attack

Situazione in cui un singolo nodo (o un insieme organizzato) viene a disporre di più della metà della potenza computazionale complessiva del network. Si consideri che non

è necessario detenere precisamente il 51% dell'hashrate, basta superare la maggioranza per essere in grado di sferrare questo tipo di attacco.

Tale eventualità rappresenta una minaccia alla stabilità di Bitcoin, in quanto tale nodo, per tutto il tempo in cui possedesse più della metà della potenza, avrebbe il potere di:

- Riuscire sempre in un double-spend attack, indipendentemente dal numero di conferme attese dal commerciante, in quanto sarà sempre in grado di costruire segretamente una catena alternativa più lunga di quella onesta;
- Esercitare il monopolio dell'attività di mining, non considerando mai i blocchi eventualmente prodotti dagli altri minatori, certo che nella distanza la sua catena sarebbe sempre più lunga di quella degli altri, facendo proprie tutte le ricompense;
- Decidere di non includere qualche transazione, o addirittura nessuna, all'interno dei suoi blocchi, forte del fatto che la "sua" catena vincerà sempre e comunque. Di fatto potrebbe produrre solo blocchi vuoti, relegando le tutte le transazioni processate dagli utenti a zero conferme.

Certamente un minatore in possesso di una tale potenza di calcolo potrebbe anche decidere di rimanere onesto, avendo comunque una probabilità di risolvere ogni nuovo blocco superiore al 50% e dunque un guadagno atteso giornaliero molto alto. In caso contrario tutti gli altri minatori non avrebbero più motivo di continuare la loro attività e sprecare tempo ed energia elettrica senza più ottenere una remunerazione, mentre la fiducia in Bitcoin come sistema di pagamento svanirebbe molto velocemente. Inoltre far fallire il sistema comporterebbe gravi ripercussioni economiche anche nello stesso attaccante, a causa della svalutazione del proprio capitale di apparecchiature hardware designate apposta per tale attività, che difficilmente troverebbero un altro impiego altrettanto remunerativo.

Per fare un rapido calcolo esemplificativo, attualmente, con un hashrate di 339.672.669,123 GH/s (Fonte: blockchain.info, data ultima consultazione 18/05/'15), un 51% attack richiederebbe al singolo nodo di immettere una potenza almeno superiore all'hashrate totale, per giungere a detenere una quota superiore al 50% del totale. Cercando in rete il prezzo di un comune dispositivo per il mining si trovano prezzi nell'ordine dei 0,50€ per GH/s. Moltiplicando tale prezzo per la potenza richiesta (facciamo l'hashrate totale più 100 GH/s) ai fini dell'attacco si ottiene il totale di

169.836.384,56 € (si consideri che oltre ai dispositivi per il mining si richiede un elevato consumo di energia elettrica); una somma di denaro certamente impegnativa e inarrivabile per i più, che probabilmente non verrebbe mai ripagata se il nodo rimanesse onesto, ma che qualche potente della Terra potrebbe comunque disporre e arrecare gravi danni se solo lo volesse.

3 L'ECONOMIA DI BITCOIN

3.1 L'ecosistema Bitcoin

L'innovazione tecnologica introdotta da Bitcoin ha portato alla nascita di un vero e proprio ecosistema attorno a questo nuovo sistema di pagamento. Un ecosistema in continua evoluzione, formato da attori diversi rispetto al mondo dei pagamenti tradizionali e da nuovi modelli di business incentrati generalmente sull'ottenimento e su servizi riguardanti l'utilizzo, lo scambio e l'investimento di bitcoin o di altre criptovalute alternative.

L'economia di Bitcoin è ancora molto giovane e in continuo fermento, tuttavia i principale attori che gravitano al momento attorno alla criptovaluta sono:

- **Gli sviluppatori:** contribuiscono allo sviluppo e al miglioramento del sistema dal punto di vista tecnico e alla risoluzione delle vulnerabilità che vengono scoperte.
- **I minatori:** permettono il funzionamento del sistema validando e registrando le transazioni nella blockchain, creando ed ottenendo come ricompensa nuove unità di valuta secondo le modalità descritte nel precedente capitolo. L'opportunità di profitto offerta dal mining ha attratto molti soggetti e molte risorse, specialmente a partire dalla seconda metà del 2013, tale da diventare ormai una vera e propria attività imprenditoriale, grazie anche all'introduzione nel mercato di apparecchiature studiate appositamente per questo scopo.
- **Gli utilizzatori:** tutti i soggetti che per diversi scopi e necessità diverse utilizzano i bitcoin, dai commercianti che li accettano in cambio di beni e servizi, alle persone che li conservano per fini speculativi.
- **I fornitori dei servizi di wallet:** forniscono diverse tipologie di portafogli elettronici, ideate per diverse esigenze, affinché l'utente possa ricevere, inviare o conservare dei bitcoin.

- **Le piattaforme di exchange:** servizio di compravendita di bitcoin in cambio di diverse valute legali, altre criptovalute o metalli preziosi. Si tratta generalmente di società non-finanziarie.
- **I fornitori di servizi finanziari:** piattaforme online che offrono opportunità di investimento sulla criptovaluta. Questi soggetti facilitano l'accesso al mondo bitcoin, facilitando l'investimento nelle start-up o in specifici prodotti finanziari, dagli ETFs ai prodotti derivati che scommettono sull'andamento del prezzo dei bitcoin.
- **Processori di pagamento:** servizi che facilitano l'accettazione di bitcoin come mezzo di pagamento sia per i negozi fisici che online, offrendo inoltre servizi come il cambio immediato in valuta legale dei bitcoin incassati, allo scopo di non far gravare nel bilancio dell'esercente il rischio derivante dalla volatilità del prezzo della criptovaluta.
- **Altri soggetti:** categoria di soggetti coinvolti indirettamente nell'ambiente Bitcoin, ma importanti per identificarne il giro d'affari complessivo. Tra questi troviamo le aziende produttrici di hardware specifici per il mining, per i wallet e per gli ATMs, quelle che sviluppano software con diverse applicazioni nell'ambito dell'utilizzo della valuta, e infine tutte le start-up che sfruttano la tecnologia di Bitcoin e in particolare quella della blockchain come base per nuove applicazioni, diverse da quelle dei pagamenti.

3.2 I numeri di Bitcoin

Uno degli aspetti più affascinanti di Bitcoin è la possibilità di sapere in ogni momento il numero di unità di valuta totali in circolazione, grazie al noto meccanismo che ne regola l'emissione, e di sapere inoltre il numero delle transazioni e gli importi scambiati in tempo reale, grazie alla pubblicità della blockchain. Una tale disponibilità di informazioni su base giornaliera è infatti impossibile da ottenere per le altre valute legali, perché è impossibile tenere traccia di tutti gli scambi effettuati col denaro contante. La tabella seguente fornisce un primo quadro riassuntivo sulla situazione di Bitcoin in questo momento, lunedì 18 maggio 2015.

Unità di bitcoin in circolazione	**BTC 14.175.525,00**
Prezzo di mercato del bitcoin (USD)	**$236,45**
Capitalizzazione di mercato (USD)	**$3.351.802.886,25**

Tabella 3.1: unità di bitcoin in circolazione, capitalizzazione e prezzo di mercato allo stato attuale (Fonte: blockchain.info, data ultima consultazione 18/05/'15).

3.2.1 Il prezzo del bitcoin

Il prezzo per un bitcoin oggi, lunedì 18 maggio 2015, è di **236,45$**, equivalenti a circa **206,60€**[24]. Dal 2009 a oggi il prezzo di mercato per un'unità della criptovaluta non è sempre stato lo stesso: dopo circa due anni di iniziale anonimità, nel febbraio 2011 il bitcoin raggiunge per la prima volta la parità con il dollaro, arrivando addirittura ad un massimo di **1.151,00$** il 4 dicembre 2013, in un percorso tutt'altro che omogeneo, come si evince dal *grafico 3.1*, caratterizzato da vertiginose salite e altrettanto repentine correzioni verso il basso.

[24] Il tasso di cambio euro/dollaro (S€/$) al 18/05 è di 1,1445 (Fonte: finance.yahoo).

Grafico 3.1: storico del prezzo per un bitcoin (in USD) da settembre 2010 a oggi (Fonte: blockchain.info, data ultima consultazione 18/05/'15).

Il prezzo del bitcoin è determinato dal mercato, ovvero dalla domanda e dall'offerta: un aumento o una riduzione della domanda causano rispettivamente un aumento o una diminuzione del prezzo della criptovaluta; le unità in circolazione di bitcoin aumentano nel corso del tempo di una quantità che decresce progressivamente fino ad annullarsi, secondo quanto stabilito dal protocollo, per cui l'offerta è rigida e dunque insensibile alle variazioni della domanda.

L'assenza di un'autorità centrale che controlli la stabilità del prezzo del bitcoin agendo sulla sua offerta, come accade invece per le valute legali, unitamente al fatto che il mercato della criptovaluta è ancora molto sottile se paragonato ai volumi di denaro scambiati attraverso gli altri sistemi per i pagamenti tradizionali, fa sì che anche piccole variazioni della domanda si traducano in un aumento o in una diminuzione del prezzo, rendendo il bitcoin molto volatile.

Le repentine salite e le successive discese del prezzo sono riconducibili al fatto che il mercato non ha ancora scoperto il reale valore del bitcoin, perché il fenomeno delle criptovalute è giovane, ed è ancora presto per dire se in futuro troveranno ampio uso come strumento per i pagamenti. In questa situazione molti individui, sulla base delle informazioni disponibili e la formulazione di aspettative personali, possono essere più o meno ottimisti in merito al futuro della criptovaluta, per cui possono essere spinti ad acquistare dei bitcoin per scopi speculativi, sperando che il suo prezzo crescerà nel

tempo. Le informazioni negative che coinvolgono Bitcoin di tanto in tanto, come ad esempio gli episodi di furti dagli exchange, possono altresì creare una perdita di fiducia nel sistema da parte degli stessi individui, inducendoli a vendere in fretta i bitcoin posseduti. Questi comportamenti speculativi alimentano la volatilià del prezzo: nelle fasi di aumento del prezzo l'azione speculativa può condurre ad un eccessivo entusiasmo nei confronti della criptovaluta; tale entusiasmo attrae nuovi investitori e gli effetti si traducono in un aumento eccessivo del prezzo, salvo poi subire una brusca correzione verso il basso frutto della volontà di sbarazzarsi in fretta dei bitcoin posseduti, in un meccanismo molto simile a quello dello scoppio di una bolla finanziaria.

Le frequenti variazioni del prezzo del bitcoin espongono gli utilizzatori e coloro che possiedono delle unità di criptovaluta all'incertezza del suo valore futuro. Una misura della rischiosità del detenere dei bitcoin può essere espressa dalla sua volatilità storica[25], che esprime l'entità delle oscillazioni del prezzo subite in passato. Il *grafico 3.2* mette a confronto la volatilità storica del bitcoin con quelle del prezzo (in USD) dell'euro e dell'oro, calcolate sullo storico dei prezzi giornalieri del periodo che va da ottobre 2010 fino al 31 maggio 2015.

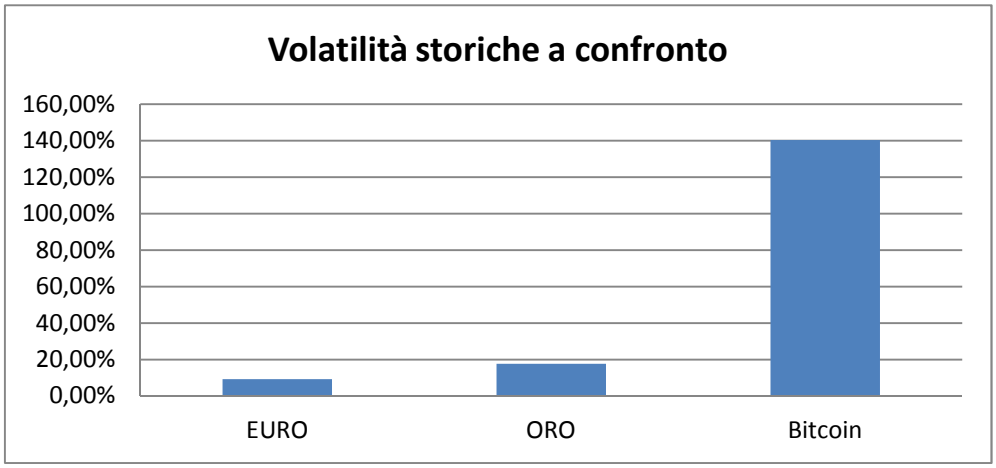

Grafico 3.2: Volatilità storica di euro, oro e bitcoin sulla base dei prezzi storici (in USD) del periodo 01/10/'10 – 31/05/'15. I prezzi storici dell'euro sono stati ricavati da federalreserve.gov, mentre quelli dell'oro da quandl.com/data/BUNDESBANK (data ultima consultazione 31/05/'15).

[25] Volatilità storica: misura della volatilità di uno strumento finanziario registrata in un determinato periodo di tempo. La volatilità storica è generalmente espressa attraverso la deviazione standard delle variazioni di rendimento dello strumento (giornaliere o mensili) verificatesi in un determinato periodo, moltiplicata per un coefficiente di annualizzazione.

La volatilità storica del prezzo del bitcoin è stata del 140,29%, di gran lunga superiore a quelle fatte registrare nello stesso periodo rispettivamente da euro (9,17%) e oro (17,64%). I risultati di questa analisi sottolineano la rischiosità del possedere delle unità di bitcoin, soprattutto se paragonata a valute legali come l'euro, che aspira a sostituire nei pagamenti, e all'oro, principale alternativa alla detenzione di valuta legale come riserva di valore.

Nella *tabella 3.2* la volatilità del prezzo giornaliero del bitcoin è calcolata per ogni trimestre del periodo analizzato (l'ultima riga della tabella si riferisce soltanto al bimestre aprile-maggio '15), allo scopo di fornire una visione maggiormente informativa tenendo sempre presente l'andamento del prezzo illustrato dal *grafico 3.1*.

I trimestri caratterizzati da una più forte volatilità storica sono i primi tre del periodo considerato, in cui il prezzo arriva a toccare il massimo storico (fino a quel momento) di 35,00$ per un bitcoin; anche le variazioni giornaliere registrate, sia negative che positive, sono ampie se confrontate con tutti gli altri trimestri seguenti, ma il basso livello del prezzo per un bitcoin di quel periodo fa sì che la volatilità dei periodi successivi abbiano un impatto maggiore sulle tasche dei possessori di bitcoin.

L'anno 2013 è quello caratterizzato da un più ampio campo di variazione[26] del prezzo del bitcoin, che tocca la soglia minima di 13,40$ nel primo trimestre per poi arrivare a 1151,00$ a dicembre, in quello che è il più alto valore mai registrato.

La volatilità storica calcolata nei trimestri dell'ultimo anno e mezzo è mediamente più bassa rispetto a quella che ha caratterizzato i precedenti tre anni della criptovaluta; il trimestre più volatile è stato il gennaio-marzo 2015, con una volatilità del 5,19%. I due mesi appena conclusi hanno registrato una volatilià del 2,10%, una delle più basse finora, con oscillazioni giornaliere negative mai al di sotto del 5%.

Sempre nella tabella seguente sono indicate la variazioni percentuali medie del prezzo giornaliero per ogni trimestre considerato, e sono calcolate inoltre le variazioni percentuali giornaliere minime e massime per gli stessi periodi.

[26] Campo di variazione (range): dato statistico che indica la variabilità di una serie di dati storici, misurata attravero la seguente equazione: x_{max}-x_{min}.

Periodo	Prezzo medio (USD) (Min ; Max)	Variazione media (%) (Min ; Max)	Deviazione Standard Annualizzata(%)
2010			
ott - dic	$0,22 ($0,06 ; $0,50)	2,65% (-26,00% ; 74,30%)	14,96%
2011			
gen - mar	$0,74 ($0,30 ; $1,10)	1,53% (-12,07% ; 90,00%)	10,97%
apr – giu	$9,16 ($0,71 ; $35,00)	4,23% (-16,70% ; 67,42%)	13,73%
lug – set	$10,78 ($4,81 ; $17,00)	-1,05% (-12,31% ; 36,11%)	7,04%
ott – dic	$3,45 ($2,29 ; $5,30)	0,15% (-22,87% ; 21,61%)	6,82%
2012			
gen - mar	$5,59 ($4,33 ; $7,22)	0,07% (-12,86% ; 14,14%)	4,01%
apr – giu	$5,42 ($4,80 ; $6,80)	0,35% (-3,61% ; 7,04%)	1,71%
lug – set	$10,41 ($6,55 ; $15,40)	0,79% (-21,36% ; 14,48%)	4,62%
ott – dic	$12,37 ($10,60 ; $13,90)	0,11% (-5,43% , 6,17%)	1,72%
2013			
gen - mar	$33,46 ($13,40 ; $93,57)	2,28% (-11,89% ; 21,22%)	5,19%
apr – giu	$119,70 ($76,49 ; $237,99)	0,65% (-38,02% ; 43,16%)	10,77%
lug – set	$107,44 ($67,86 ; $132,75)	0,35% (-14,96% ; 12,22%)	3,58%
ott – dic	$493,43 ($104,47 ; $1.151,00)	2,25% (-18,65% ; 25,95%)	7,97%
2014			
gen - mar	$695,03 ($449,02 ; $934,21)	-0,42% (-13,05% ; 19,04%)	4,47%
apr – giu	$520,19 ($401,00 ; $674,98)	0,40% (-9,50% ; 11,89%)	3,73%
lug – set	$534,96 ($380,00 ; $654,45)	-0,49% (-6,84% ; 5,56%)	2,37%
ott – dic	$357,53 ($293,67 ; $430,07)	-0,13% (-12,60% ; 17,81%)	3,91%
2015			
gen - mar	$250,94 ($176,50 ; $316,15)	-0,16% (-23,56% ; 23,58%)	5,19%
apr – giu	$235,89 ($216,00 ; $257,03)	-0,05% (-4,55% ; 5,54%)	2,10%

Tabella 3.2: prezzo di mercato medio, variazione media (%) e la deviazione standard annualizzata (%) trimestrali del prezzo di mercato del bitcoin in USD dall' 01/10/'10 al 31/05/'15.

3.2.2 Fattori che determinano il prezzo del bitcoin

Come affermato in precedenza, il prezzo del bitcoin in dollari statunitensi (o tasso di cambio BTC/$) è determinato dal mercato, ovvero dal meccanismo della domanda e dell'offerta. Secondo lo schema proposto dalla *figura 3.1* la curva di offerta di bitcoin è rappresentata da una retta verticale; in questa configurazione l'offerta è inelastica ovvero insensibile alle variazioni della domanda, a conferma del fatto che le unità di bitcoin in circolazione aumentano sì nel corso dal tempo, ma a prescindere dalle dinamiche che spostano la domanda. La domanda è invece rappresentata da una retta orizzontale, e quindi perfettamente elastica, perché l'aumento dell'offerta nel tempo è sempre nota ed incorporata nelle aspettative degli utenti. Ne consegue che le variazioni di prezzo del bitcoin siano esclusivamente originate dalle variazioni della domanda della criptovaluta.

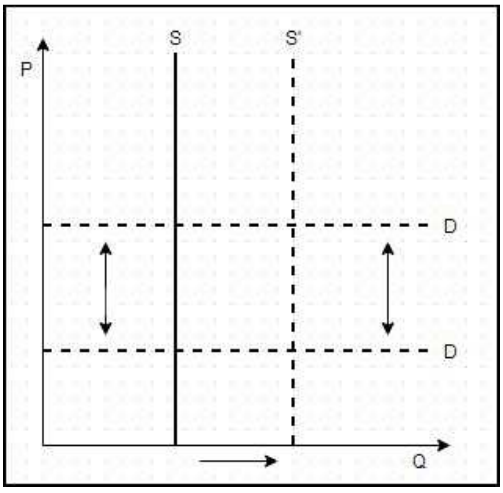

Figura 3.1: domanda e offerta di bitcoin (Fonte: "*Bits and Bets – Information, Price Volatility, and Demand for Bitcoin*", *Buchholz et al., 2012*).

Ma quali sono le dinamiche che muovono la domanda? O, detto in altri termini, quali sono i motivi per cui, in un determinato intervallo di tempo, un individuo desideri ottenere una certa somma di bitcoin piuttosto che tenersi i suoi dollari o euro?

Gli individui desiderano possedere dei bitcoin perché vi riconoscono un valore. Ogni individuo può riconoscervi diversi valori e di conseguenza avere diversi motivi per detenere delle unità di valuta. I principali valori individuabili sono:

- valori scientifico/tecnologici derivanti dall'innovazione apportata da Bitcoin, che configura un sistema senza precedenti; questa è stata la motivazione principale che ha condotto i primi utenti a entrare nel mondo dei bitcoin, quando ancora il suo prezzo era vicino allo zero;
- valori sociali derivanti dalle caratteristiche di decentralizzazione e pseudonimia del sistema Bitcoin, e quindi di indipendenza dalle banche e dai governi e di maggiore garanzia della privacy rispetto ai sistemi di pagamento tradizionali; inoltre i valori sociali derivanti dalla diffusione di Bitcoin tra gli individui: all'aumentare della diffusione cresce anche l'utilità del possedere dei bitcoin, poiché crescono le possibilità di un loro reale impiego;
- valori tecnico/funzionali derivanti dall'utilità e dall'efficacia di Bitcoin come sistema per i pagamenti, per la sua velocità, praticità e per tutti i vantaggi che possono derivare dall'utilizzo della criptovaluta, come ad esempio i bassi costi di transazione, o la possibilità di effettuare pagamenti in ogni parte del mondo comodamente da casa.

I principali fattori che conducono a variazioni della domanda di bitcoin, e quindi del suo prezzo sono:

- L'interesse: la diffusione dell'informazione in merito a bitcoin e al mondo delle criptovalute condiziona positivamente il prezzo; *Buchholz et al. (2012)* e *Kristoufek (2014)*, confrontando le statistiche del numero di digitazioni della parola bitcoin su *Google* e *Wikipedia* con l'andamento del prezzo dei bitcoin, affermano che aumento dell'interesse e aumento del prezzo sarebbero correlati. Kristoufek afferma che tale relazione è apprezzabile sia nel lungo periodo che in occasione delle repentine salite di prezzo, in cui l'interesse attrae maggiormente gli speculatori e spinge ulteriormente il prezzo verso l'alto; similmente nel corso delle correzioni del prezzo verso il basso, l'interesse è già sceso più velocemente e trascina maggiormente il prezzo verso il basso.
- Le notizie: le notizie negative causano incertezza, e in un sistema non controllato da un'autorità centrale i loro effetti si fanno sentire maggiormente. Esempi di tali notizie sono stati i frequenti furti delle chiavi private dai server delle piattaforme di exchange; la diminuzione del prezzo in relazione a tali eventi è frutto della perdita di fiducia in generale. Al contrario le notizie positive possono creare effetti positivi nel

prezzo nel lungo periodo, aumentando la diffusione della valuta e quindi della domanda: ad esempio la decisione di un'importante azienda di accettare la criptovaluta ha l'effetto di allarga

- L'utilizzo dei bitcoin per le transazioni reali: riguardano l'entità della diffusione di Bitcoin, determinata dal suo effettivo utilizzo per le transazioni. Poiché è proprio Bitcoin stesso a proporsi come sistema per i pagamenti alternativo, per analizzare il livello del suo utilizzo non ci si può limitare al volume delle transazioni giornaliere che vengono registrate nella blockchain, perché questo dato comprende sia gli scambi "reali", ovvero derivanti da operazioni di acquisto e vendita di beni o servizi, sia la movimentazione di bitcoin tra un indirizzo e l'altro appartenenti ad uno stesso utente. Dal volume totale delle transazioni si devo

  Kristoufek afferma che gli effetti dell'aumento dell'utilizzo dei bitcoin per le transazioni reali conducono ad un aumento del loro prezzo nel lungo periodo.
- L'utilizzo dei bitcoin per scopi speculativi: l'utilizzo di Bitcoin come investimento invece che come sistema per i pagamenti determina anch'esso effetti sul prezzo della criptovaluta; secondo *Ciaian et al.* (2014) la presenza di investitori o speculatori può essere visto come benefico, perché si assumono il rischio di detenere delle unità di bitcoin al posto di altri utenti intimoriti dalla loro volatilità, ma il loro comportamento nel breve periodo sarebbe causa di maggiore instabilità.

Sulla base dei fattori determinanti il prezzo dei bitcoin appena illustrati, si evince la difficoltà di costruire un modello che ne spieghi accuratamente tutte le dinamiche. Le variabili che condizionano l'andamento del prezzo della criptovaluta sono difficili da stimare, e possono essere descritte soltanto mediante delle assunzioni.

Un semplice e frequente esempio di modello macroeconomico per l'analisi del prezzo del bitcoin è il seguente:

$$\begin{cases} (\mathbf{1}) \text{ offerta di bitcoin al tempo t: } MS = P_{BTC} \times B; \\ (\mathbf{2}) \text{ domanda di bitcoin al tempo t: } MD = \frac{TxVol}{Vel}; \end{cases}$$

(**1**) l'offerta di bitcoin (MS) al tempo t è data dal prodotto del prezzo della criptovaluta (P_{BTC}) al tempo t per le unità totali in circolazione (B) al tempo t, il cui ammontare è

sempre noto, ma occorre fare alcune ulteriori considerazioni che saranno spiegate a seguire;

(**2**)la domanda di bitcoin al tempo t è ottenuta dividendo il volume totale delle transazioni (TxVol) al tempo t, per la velocità[27] (Vel) della criptovaluta.

Dalla messa a sistema delle equazioni (**1**) e (**2**) deriva la seguente condizione di equilibrio:

(**3**) condizione di equilbrio (MS=MD): $P_{BTC} = \frac{TxVol}{Vel} * \frac{1}{B}$.

Il prezzo del bitcoin è risulta così determinato dal rapporto tra il volume delle transazioni e il prodotto tra le unità di criptovaluta in circolazione e la loro velocità.

- TxVol: all'aumentare del volume delle transazioni, gli individui aumentano la domanda di bitcoin allo scopo di utilizzarli come strumento di scambio, e questo si traduce in un aumento del prezzo della criptovaluta. È necessario tuttavia fare delle assunzioni in merito a quante di queste transazioni derivino da operazioni di acquisto di beni e servizi, e quante invece derivino da operazioni di compravendita di bitcoin in cambio di valute legali e quante infine non siano altro che semplici movimentazioni tra un indirizzo e l'altro appartenenti a un medesimi utenti.
- Vel: la velocità della criptovaluta, ovvero il numero di volte in cui è possibile utilizzare un bitcoin in un determinato periodo di tempo, è posta al denominatore di questo modello; a parità di volume delle transazioni, una maggiore velocità del bitcoin determina una riduzione dell'entità della domanda e quindi anche una riduzione del prezzo. Infatti una veloce circolazione dei bitcoin permette di gestire elevati volumi di transazioni senza il bisogno di maggiori quantità in circolazione.
- B: è vero che si sa in ogni istante il numero delle unità totali di bitcoin minate, e che tale numero non supererà mai la quota di 21 milioni, ma bisogna considerare la possibilità che più di qualcuna di queste unità siano andate perse; se infatti un utente perdesse le chiavi private del proprio wallet, per esempio in seguito alla distruzione del proprio pc dove tali codici erano memorizzati, questi non potrebbe in nessun

[27] Velocità della moneta: è la velocità di circolazione della moneta nell'economia, misurata dalla frequenza media con cui un'unità di moneta viene spesa in un determinato periodo di tempo.

modo recuperare i suoi bitcoin, e tale quantità andrebbe a diminuire il numero totale delle unità in circolazione.

Alla luce del contributo apportato dai diversi economisti sopracitati e del funzionamento del modello appena esposto, è evidente la difficoltà di effettuare una stima precisa del prezzo futuro del bitcoin. Sappiamo che entro il 2040 il numero dei bitcoin in circolazione sarà il 99% del totale previsto, ma è difficile stabilire quale sarà il loro prezzo, poiché dipenderà principalmente dall'utilizzo che ne verrà fatto, che al momento è difficile da prevedere. Si ritiene comunque che se in futuro il bitcoin trovasse ampia accettazione come strumento di pagamento, il suo prezzo sarebbe destinato a salire, poiché molti più individui sarebbero disposti ad utilizzarli per i loro acquisti. Tale eventualità deriverebbe comunque da un processo relativamente lungo, frutto della progressiva scoperta da parte del mercato del suo reale valore di utilizzo e di una progressiva comprensione degli individui dell'importanza ed utilità del fenomeno.

La volatilità attuale è sintomo che il mercato non ha ancora scoperto il valore del bitcoin, e le repentine oscillazioni del suo prezzo dipendo dall'alternarsi di periodi di eccessivo ottimismo e di profonda incertezza, sovralimentati anche da posizioni speculative, derivanti dalle aspettative degli individui sulla base di personali interpretazioni riguardanti le informazioni su Bitcoin o legati alla più generale situazione socio-economica, variabili difficilmente stimabili e inseribili in un modello del prezzo. La situazione attuale è comunque inevitabile se si considera che il fenomeno delle criptovalute non è che appena iniziato, ma non può nemmeno essere vista come totalmente negativa: i picchi di prezzo, anche se brevi, suscitano comunque un maggiore interesse verso la criptovaluta, contribuendo così ad aumentare la popolarità e le possibilità che nuovi individui entrino a fare parte della comunità, accettandoli come pagamento nei loro negozi o semplicemente utilizzandoli.

3.2.3 Il numero delle transazioni e il volume scambiato

Nei tre grafici seguenti sono illustrati rispettivamente il numero delle transazioni trimestrali di bitcoin e i volumi scambiati attraverso quest'ultime, espressi prima in bitcoin e poi in dollari statunitensi, riguardanti il periodo di osservazione che va dal 01/10/'10 al 31/03/'15. Il *grafico 3.3* evidenzia una crescita progressiva del numero di transazioni trimestrali, una tendenza positiva iniziata a partire dai primi mesi del 2011, periodo in cui il prezzo per un bitcoin comincia a salire, superando per la prima volta la parità col dollaro, cominciando a suscitare un certo interesse.

Nel *grafico 3.4* si nota un elevato picco del volume di bitcoin scambiati in corrispondenza del quarto trimestre del 2011; si tratta tuttavia di un fenomeno isolato, riconducibili soltanto a pochi giorni di elevate movimentazioni, non riferibili peraltro a particolari episodi o notizie verificatesi in quel periodo. Nel corso dei restanti trimestri il volume dei bitcoin scambiato sembra salire e scendere periodicamente; si può notare in particolare un calo nei trimestri centrali del 2014, denotando un possibile periodo di stallo immediatamente successivo al record del prezzo per un bitcoin di dicembre 2013 e della sua successiva discesa.

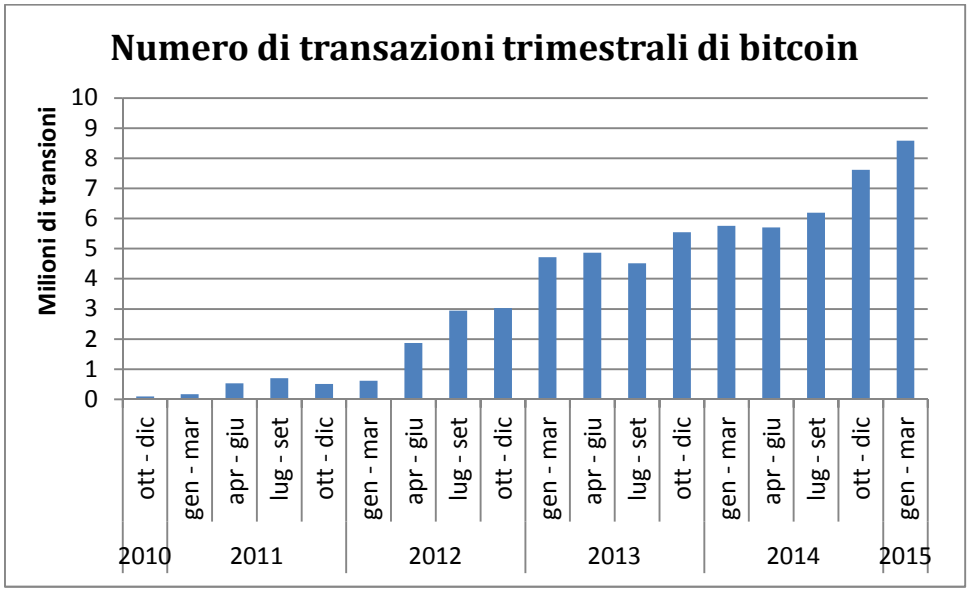

Grafico 3.3: numero di transazioni trimestrali di bitcoin dal 01/10/'10 al 31/03/'15 (Fonte: blockchain.info, data ultima consultazione 18/05/'15).

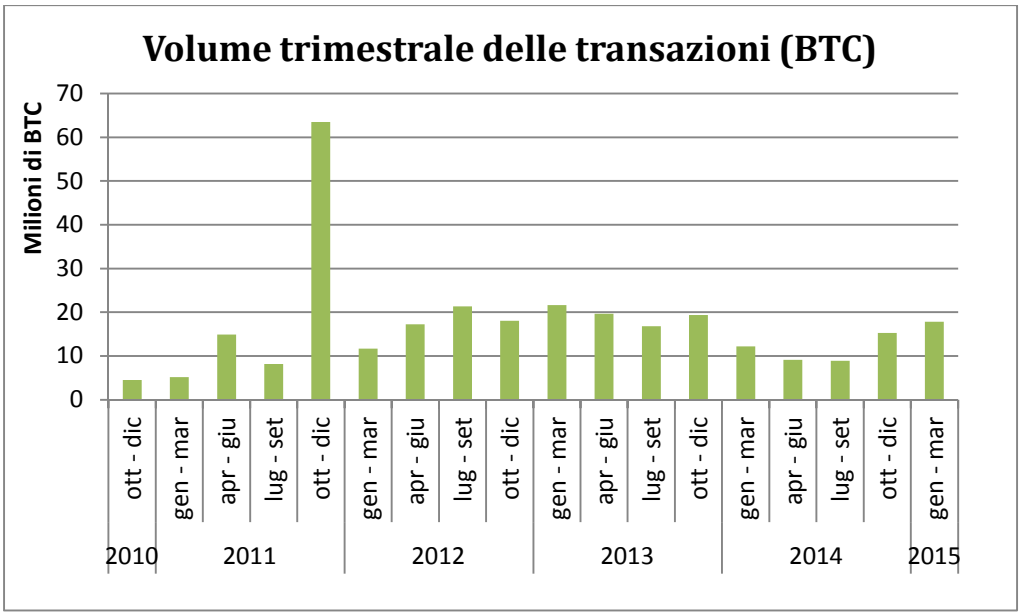

Grafico 3.4: volume delle transazioni trimestrali di bitcoin (in BTC) 01/10/'10 al 31/03/'15 (Fonte: blockchain.info, data ultima consultazione 18/05/'15).

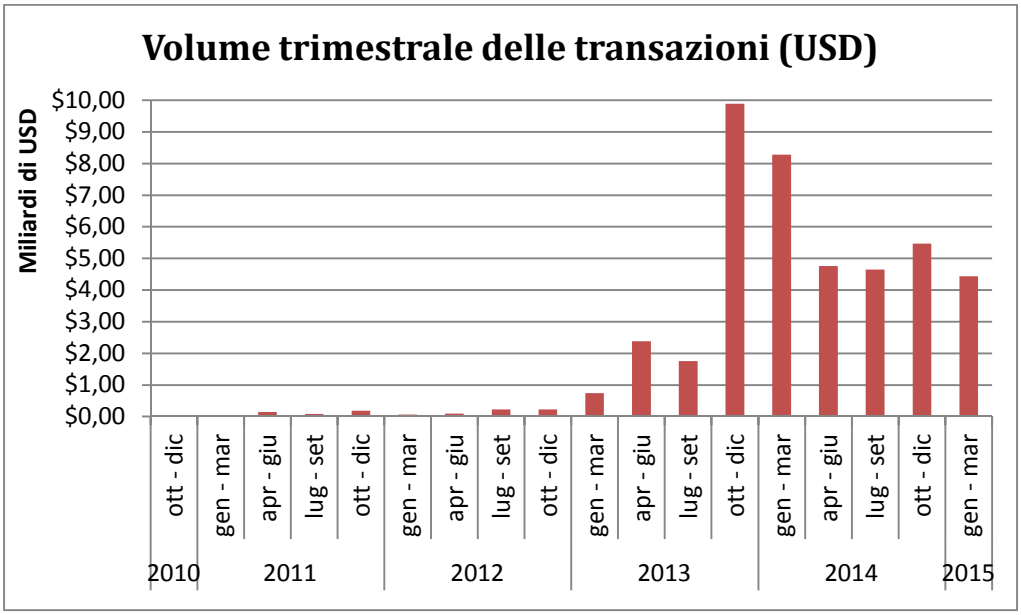

Grafico 3.5: volume delle transazioni trimestrali di bitcoin (in USD) 01/10/'10 al 31/03/'15 (Fonte: blockchain.info, data ultima consultazione 18/05/'15).

Gli effetti dell'andamento altalenante del prezzo del bitcoin sembra caratterizzare solamente il *grafico 3.5*, in cui il volume scambiato subisce un aumento del 463% dal terzo al quarto trimestre del 2013, proprio in concomitanza con il picco di prezzo.

Il fatto che i saliscendi del prezzo non determinino anche dei saliscendi del numero delle transazioni e dei BTC scambiati, può trovare spiegazione nel fatto le azioni speculative avvengono in via principale al di fuori della blockchain: infatti l'azione speculativa è svolta per la maggior parte all'interno delle piattaforme di exchange, a cui ogni utente registrato può inviare del denaro legale, tramite bonifico o carta di credito, oppure dei bitcoin, quest'ultimi inviati per mezzo di una transazione effettiva, che coinvolge solo successivamente la blockchain. A quel punto l'utente possiede un conto virtuale presso quel particolare exchange, e le operazioni di compravendita di bitcoin avvengono soltantanto tramite accrediti o addebiti virtuali di bitcoin o di denaro in tale conto, registrati dalla società che gestisce l'exchange. La blockchain viene coinvolta solo nel momento in cui l'utente desideri incassare i bitcoin disponibili nel proprio conto virtuale, o allo stesso modo l'exchange effettuerà un bonifico a favore dell'utente qualora desiderasse incassare il denaro legale depositatovi.

Per una visione più ampia dell'entità del fenomeno Bitcoin, il *grafico 3.6* espone i volumi di acquisto in miliardi di dollari registrati nell'anno 2014 delle principali carte di credito e prepagate utilizzate negli Stati Uniti, confrontate con il volume delle transazioni di bitcoin dello stesso anno.

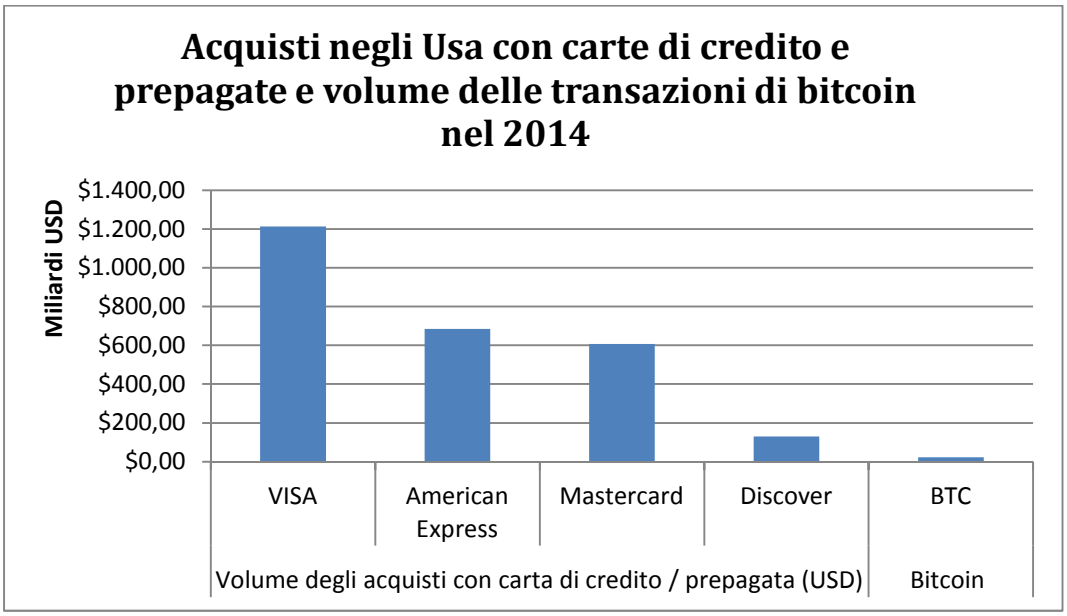

Grafico 3.6: Volume degli acquisti con carte di credito o prepagate (in USD) negli USA nel 2014, confrontati con il volume delle transazioni di bitcoin (in USD) dello stesso anno (Fonte: *The Nilson Report: General Purpose U.S. Cards 2014*).

Dal grafico appena illustrato si può notare come i pagamenti con la criptovaluta siano ancora un fenomeno di modeste dimensioni. Inoltre i volumi esposti riguardano solamente gli acquisti mediante carte di credito o prepagate, e non tengono dunque conto per esempio dei pagamenti mediante le carte di debito o i bonifici bancari. Inoltre tali dati sono riferiti al solo mercato statunitense, mentre i volumi delle transazioni di bitcoin sono su scala mondiale.

Attenendoci ai dati offerti dal *"The Nilson Report: General Purpose U.S. Cards 2014"*, il volume degli acquisti complessivi mediante carte di credito, prepagate e carte di debito dei brand Visa, American Express e Discover, registrati negli Stati Uniti nel 2014, ammonterebbero a 4,442 trilioni di dollari, contro i modesti 23,16 miliardi di dollari scambiati in bitcoin.

3.2.4 I numeri del mining

L'attività di mining, fondamentale per il funzionamento di Bitcoin, ha conosciuto una crescita esponenziale a partire dalla seconda metà del 2013. Come accennato anche in precedenza, l'attività dei minatori è remunerata da un preciso sistema di ricompense sottoforma di bitcoin di nuova emissione, unitamente alla somma delle commissioni di transazione. Prima di considerare l'aspetto economico, soffermiamoci sulle dimensioni del mining.

Per valutare le dimensioni di tale attività si deve considerare l'entità della potenza computazionale di tutti i dispositivi hardware utilizzati nella validazione e registrazione delle transazioni nella blockchain. La somma totale (o hashrate) è di poco inferiore ai 340 milioni di giga-hashes per secondo (GH/s). Di pari passo con l'aumento dell'hashrate totale è aumentata la difficoltà, il parametro che esprime complessità di minare un blocco. Tale parametro cambia infatti in relazione alla potenza computazionale del network, allo scopo che la produzione di ogni blocco avvenga mediamente ogni 10 minuti. I *grafici 3.7* e *3.8* mostrano le progressioni storiche di hashrate e difficoltà; è facile notare che l'andamento qualitativo del secondo grafico è identico a quello del primo, ma mentre l'hashrate può cambiare anche da un minuto all'altro, a seconda che un nodo spenga temporaneamente i propri dispositivi, la

difficoltà è rivista ogni circa 14 giorni (cioè ogni circa 2016 blocchi) e viene aumentata o diminuita a seconda che i tempi medi di produzione di tali blocchi abbiano rispettato o meno la soglia prestabilita dei 10 minuti.

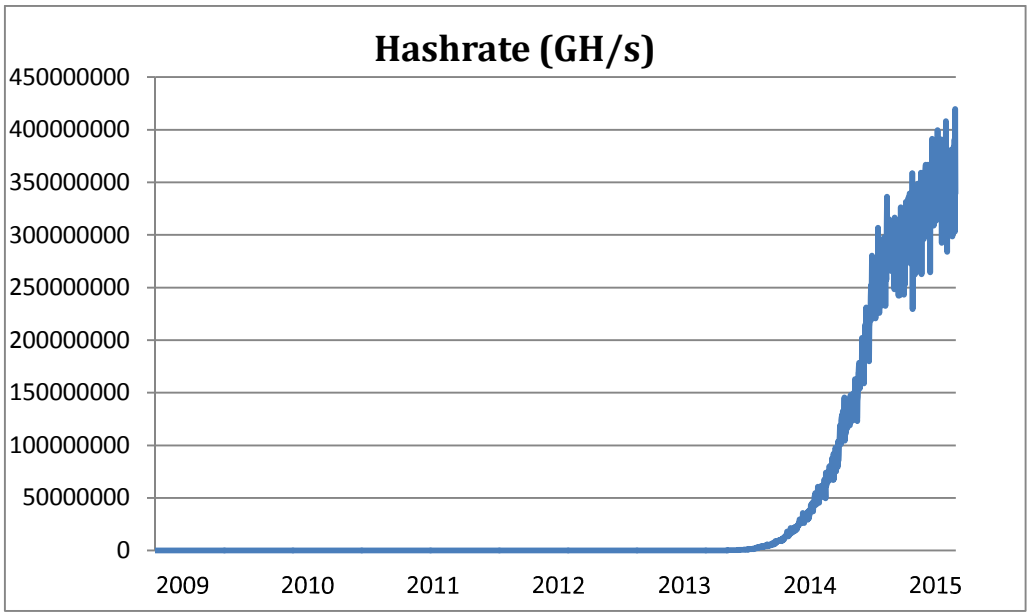

Grafico 3.7: potenza di calcolo totale immessa nel network misurata in GH/s (Fonte: blockchain.info, data ultima consultazione 18/05/'15).

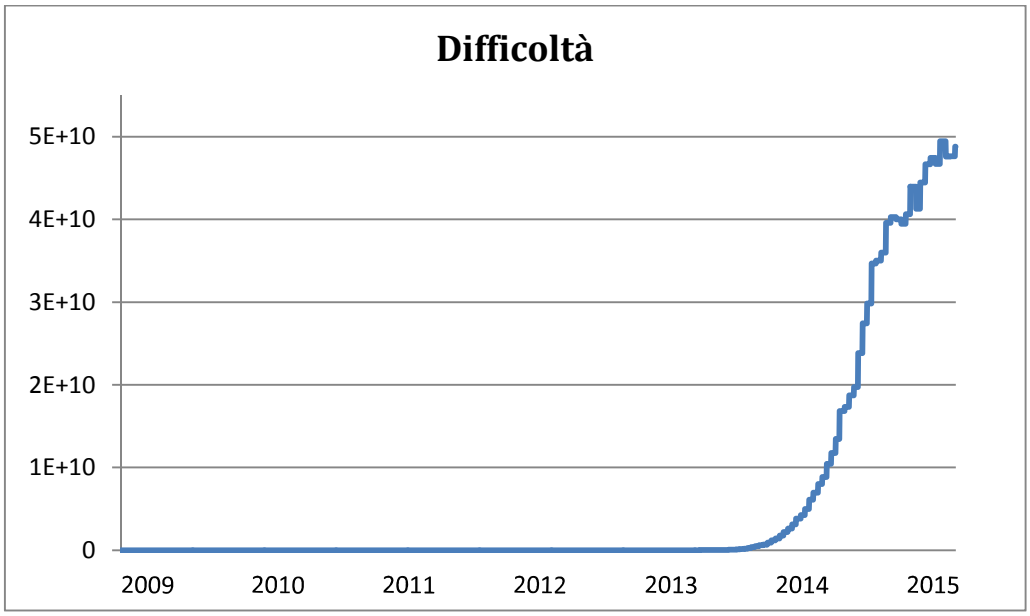

Grafico 3.8: difficoltà del mining (Fonte: blockchain.info, data ultima consultazione 18/05/'15).

L'aumento esponenziale della potenza di calcolo del network Bitcoin è stata guidata principalmente da due fattori:

- La diffusione di Bitcoin, assieme all'aumento del suo prezzo, che hanno indotto molti individui a investire nell'attività di mining; l'aumento del prezzo dei bitcoin aumenta le opportunità di profitto dei minatori, per cui molti individui decidono di investirvi;
- Il progresso tecnologico: inizialmente per il mining si potevano impiegare dei comuni computer di casa; al crescere dell'interesse per l'attività si sono impiegati dispositivi sempre più potenti, sino all'adozione di circuiti integrati disegnati apposta per svolgere gli algoritmi del mining.

Ritornando al *grafico 3.7* si può notare come la fase di crescita esponenziale iniziata dalla seconda metà del 2013 vada via via rallentando verso gli ultimi mesi del 2014. Il tasso di crescita dell'hashrate ha avuto un tale rallentamento in seguito alla riduzione del prezzo dei bitcoin nello stesso periodo (*grafico 3.1*).

I ricavi dei minatori sono costituti dalle ricompense attribuite al minatore che per primo risolve il blocco più la somma di tutte le commissioni delle transazioni incluse in quel blocco. Attualmente l'èntità della ricompensa è di 25 BTC per blocco mentre fino a novembre 2012 era di 50 BTC; l'importo della ricompensa si dimezza ogni quattro anni (ogni circa 210.000 blocchi), fino ad annullarsi, e a quel punto il lavoro dei minatori sarà remunerato soltanto dalle commissioni di transazione. Facendo un calcolo rapido, 25 BTC per blocco ogni 10 minuti fanno circa 3.600 BTC al giorno (al prezzo attuale di 236,45$ fanno 851.220$ dollari al giorno di ricavi, da distribuire tra i minatori risolvono uno dei 144 blocchi giornalieri), a cui vanno sommate le commissioni, che sono mediamente di 0,0001 BTC a transazione.

Convertendo i ricavi in valuta legale, i due grafici seguenti espongono i volumi (in USD) delle entrate giornaliere medie dei minatori calcolate per trimestre (si sono presi tutti i ricavi giornalieri del trimestre derivanti dal mining ricavandone la media aritmetica; si consideri che a causa delle variazioni del prezzo del bitcoin, il volume dei ricavi cambia di giorno in giorno). In particolare il *grafico 3.8* mostra le entrate giornaliere medie derivanti dalle ricompense per la risoluzione dei blocchi, mentre il *grafico 3.9* riguarda le entrate giornaliere medie derivanti dalle commissioni di transazione. Entrambi i grafici

rispecchiano l'andamento altalenante del prezzo del bitcoin, che rappresenta senza dubbio la componente più rischiosa nelle decisioni di investimento sul mining.

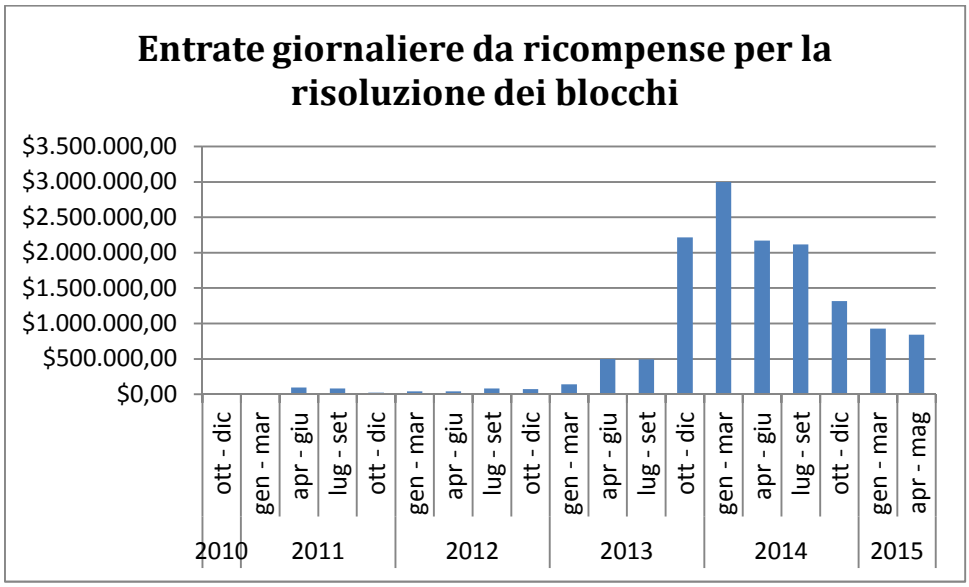

Grafico 3.8: volume delle entrate medie giornaliere per trimestre (in USD) derivanti dalle ricompense per la risoluzione dei blocchi; si noti che l'ultimo periodo considerato è di soli due mesi (Fonte: blockchain.info, data ultima consultazione 31/05/'15).

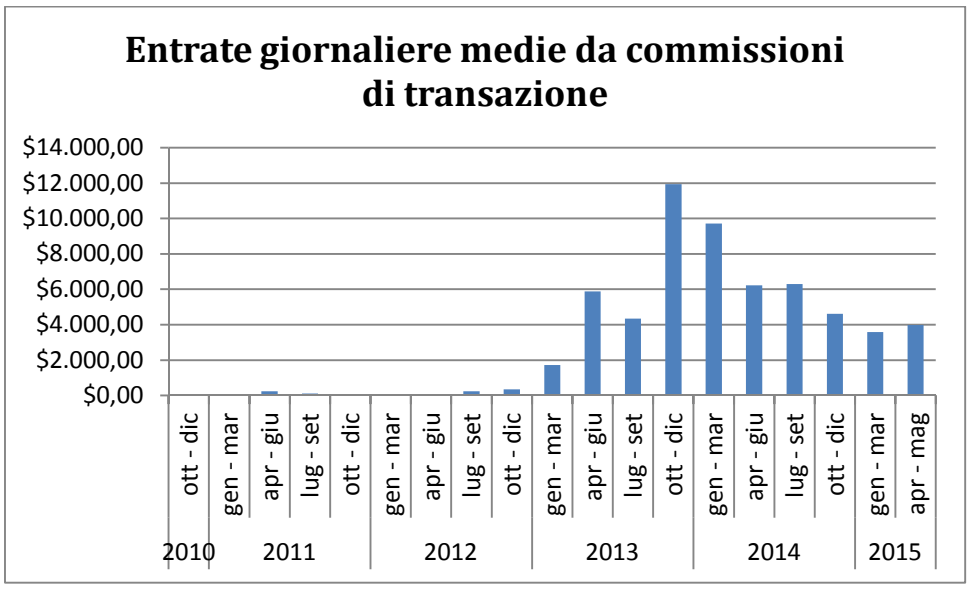

Grafico 3.9: volume delle entrate medie giornaliere per trimestre (in USD) derivanti dalle commissioni di transazione; si noti che l'ultimo periodo considerato è di soli due mesi (Fonte: blockchain.info, data ultima consultazione 31/05/'15).

Valutazione teorica di un progetto di investimento nell'attività di mining

Come valutare un progetto di investimento nell'attività di mining? Sulla base di quanto esposto finora si propone la valutazione di un investimento mediante il metodo del valore attuale netto (VAN[28]), pur introducendo alcune semplificazioni, necessarie per poter inquadrare meglio le dinamiche di un investimento nel mining.

Le variabili da considerare per assumere delle corrette decisioni se investire o meno in tale attività sono:

- Il prezzo del bitcoin: i flussi in entrata sono in bitcoin, e dunque il tasso di cambio BTC/$ gioca un ruolo fondamentale nella determinazione dei ricavi realizzabili attraverso l'attività di mining; poiché il prezzo fluttua nel tempo, è particolarmente difficile stabilire con certezza quali saranno i ricavi giornalieri attesi, e questo rende l'attività particolarmente rischiosa.
- Il tasso di crescita dell'hashrate: come visto nel *grafico 3.6*, la potenza di calcolo complessiva del network ha avuto una crescita esponenziale a partire dalla seconda metà del 2013, per incontrare poi un rallentamento negli ultimi sei mesi. Nel momento in cui un individuo acquista dei dispositivi hardware per intraprendere l'attività del mining, immette nel network una determinata potenza di calcolo che va ad aumentare l'hashrate totale di una determinata percentuale; tale percentuale applicata ai ricavi medi giornalieri dei minatori, determina l'entità dei ricavi medi giornalieri attesi dall'individuo. Per questo motivo è necessario fare una previsione sul tasso di crescita della potenza di calcolo totale; infatti al crescere dell'hashrate totale, la percentuale di potenza detenuta dall'investitore si riduce, e di conseguenza i ricavi medi giornalieri attesi dall'individuo decrescono progressivamente fino ad annullarsi, a meno che non alimenti l'investimento acquistando nuovi dispositivi hardware. Il tasso di crescita dell'hashrate totale dipende fondamentalmente dal progresso tecnologico, ma soprattutto dal prezzo del bitcoin, che salendo incentiva l'ingresso di nuovi minatori.
- I costi fissi di energia elettrica e di manutenzione: i dispositivi hardware impiegati nel mining lavorano ininterrottamente, consumando notevoli quantità di energia elettrica e necessitando di tanto in tanto di manutenzione; se i flussi di cassa medi

[28] VAN (valore attuale netto): metodo di valutazione di un investimento attraverso l'attualizzazione dei flussi di cassa previsti mediante un tasso di rendimento.

giornalieri attesi sono inferiori alla somma dei costi di energia e di manutenzione giornalieri, l'attività di mining genererebbe dei flussi di cassa negativi, e a quel punto il minatore si troverebbe di fronte a un bivio: interrompere l'attività di mining per intraprenderla qualora il prezzo del bitcoin salisse, poiché i ricavi attesi tornerebbero a quel punto ad essere superiori ai costi di energia e manutenzione, oppure acquistare nuovi dispositivi hardware, alimentando l'investimento iniziale. Per l'importanza che assumono i costi dell'energia elettrica in questo particolare tipo di attività, le opportunità di profitto offerte dal mining cambiano da Stato a Stato, in relazione alle tariffe applicate**.**

- I tempi previsti per la consegna dei dispositivi: bisogna valutare quando il mining sarà effettivamente iniziato, ovvero quando l'investitore potrà definitivamente accendere tutti i dispositivi e iniziare l'attività. A seconda delle stime che si sono effettuate sul tasso di crescita dell'hashrate, un ritardo nelle consegne dei dispositivi da parte della società produttrice potrebbe causare dei ricavi giornalieri attesi inferiori a quelli previsti già dall'inizio.

Al fine di calcolare il valore attuale netto di un progetto di investimento nell'attività di mining, si proceda secondo le seguenti fasi(per semplicità si consideri ogni dato su base settimanale):

1. Stima dei ricavi attesi dall'investimento: i ricavi attesi dall'investimento dipendono dalla percentuale dell'hashrate totale immessa nel sistema (h)[29]. Ipotizziamo che il l'hashrate totale cresca settimanalmente secondo il tasso di crescita z_h[30]; i ricavi di bitcoin attesi dall'investitore sono dunque decrescenti nel tempo. Tali ricavi vanno comunque convertiti in valuta legale, in quanto le bollette dell'energia elettrica o i costi di manutenzione vengono pagati in valuta legale, come pure le rate dell'eventuale finanziamento stipulato. I ricavi attesi dall'investimento al tempo t si calcolano dunque tramite la seguente equazione:

$$S_t = P_{BTC} * [R_t * h * (1 - z_h)^t]$$

[29] Una semplificazione introdotta riguarda i ricavi: si consideri che un minatore con una potenza h(%) ha ad ogni blocco una probabilità di h di risolvere per primo il blocco; quindi avrà un ricavo atteso di h ad ogni blocco. I ricavi del mining non sarebbero dunque continui; in questo modello si considera per semplicità che settimanalmente i ricavi del minatore siano in linea con i ricavi attesi.

[30] Il tasso z_h può essere determinato analizzando il trend della crescita dell'hashrate settimanale per esempio dal 2013 a oggi.

dove R_t sono i ricavi totali settimanali dei minatori, dati dalla somma delle ricompense per i nuovi blocchi più il totale delle commissioni di transazione; h è la percentuale di hashrate posseduta, che diminuisce settimanalmente del fattore $(1 - z_h)$. Moltiplicando i ricavi di bitcoin attesi dall'investitore per il loro prezzo (P_{BTC}) si ottengono i ricavi settimanali in USD.

2. Determinazione dei flussi di cassa attesi: i flussi di cassa attesi sono dati dai ricavi attesi dall'investitore meno i costi dell'energia elettrica sommati a quelli di manutenzione:

$$FC_t = S_t - EM$$

dove *EM* sono i costi di energia elettrica e di manutenzione settimanali; nel momento in cui i flussi di cassa diventassero negativi, il mining non sarebbe più profittevole, e si dovrebbe interrompere l'attività.

3. Determinazione del valore attuale netto: il valore attuale netto si ottiene attualizzando all'epoca 0 tutti i flussi di cassa futuri al tasso *i*, sommandoli all'esborso iniziale C_0 con cui si sono acquistati i dispositivi hardware, che è un flusso negativo (per semplicità si consideri l'assenza di imposte sui redditi ottenuti dall'investimento):

$$VAN = -C_0 + \frac{FC_1}{(1+i)} + \frac{FC_2}{(1+i)^2} + \cdots + \frac{FC_{n-1}}{(1+i)^{n-1}}$$

si noti che l'ultimo flusso da attualizzare nella formula del VAN è quello dell'epoca $(n-1)$; si ipotizzi infatti che a partire dall'epoca n i ricavi attesi dall'investimento (S_n) siano inferiori ai costi sostenuti per l'energia e per la manutenzione (*EM*); a quel punto l'attività dovrebbe essere interrotta, poiché genererebbe soltanto flussi di cassa negativi. Un calo inatteso del prezzo del bitcoin potrebbe causare flussi di cassa negativi anche in epoche molto vicine all'epoca iniziale; in tale situazione non solo il nostro investitore, ma anche altri come lui potrebbero decidere di interrompere l'attività, in attesa di momenti di prezzo più favorevoli. Affinché l'investimento possa essere profittevole, la somma di tutti i flussi di cassa attualizzati deve essere superiore all'esborso iniziale. Fondamentali risultano quindi le previsioni riguardanti il prezzo del bitcoin e il tasso di crescita dell'hashrate totale, tuttavia

l'incertezza che avvolgono queste due variabili, la prima in particolare, rende il mining particolarmente rischioso.

3.3 I vantaggi

1. I costi di transazione

Le transazioni di bitcoin possono prevedere una piccola commissione a carico del mittente, che in media è di circa 0,02€ (0,0001 BTC), indipendentemente dall'importo inviato, ma può essere maggiore o addirittura nulla secondo le modalità descritte nel precedente capitolo.

L'utilizzo di strumenti per i pagamenti elettronici tradizionali nell'ambito dell'acquisto di beni e servizi, sia online che presso i negozi fisici, non imputano dei costi di transazione all'utente, bensì all'esercente in una percentuale sul totale transato.

La tabe lla seguente propone un confronto tra i costi delle transazioni derivanti dall'utilizzo di Bitcoin e quelli derivanti dall'utilizzo di PayPal e degli altri strumenti più frequenti per i pagamenti elettronici, ricavati dall'analisi dei fogli informativi di alcune delle principali banche italiane.

Strumento di pagamento	Commissione a carico del consumatore/mittente	Commissione a carico dell'esercente/ricevente
Bitcoin	da 1mBTC (0,02€)	Nessuna
Carte di credito / prepagate	Nessuna	da 3,5% a 4% sul transato
PayPal	Nessuna	da 1,8% a 3.4% + 0,35€ sul transato
Carte di debito	Nessuna	da 2% a 2,25% sul transato
Bonifici SEPA	da 0 a 10€	Nessuna
Bonifici Extra SEPA	fino a 50€	fino a 15€

Tabella 3.1: confronto delle commissioni di transazione derivanti dall'utilizzo di Bitcoin e degli altri sistemi per i pagamenti elettronici più utilizzati. I dati sono ricavati dai fogli informativi di alcune delle principali banche italiane, consultati a maggio '15.

Con riferimento alla *tabella 3.1*, le transazioni di bitcoin risultano essere le più vantaggiose dal punto di vista dell'esercente o ricevente del pagamento, mentre l'utilizzo

dei bitcoin è di gran lunga più economico rispetto ai bonifici bancari, soprattutto per l'invio di denaro al di fuori dell'area SEPA[31].

Alle commissioni sul transato indicate a carico dell'esercente vanno a sommarsi i costi di installazione e di locazione dei terminali POS situati nei negozi fisici. Tutti questi costi derivanti dall'accettazione di diversi strumenti per i pagamenti elettronici vanno a ridurre sensibilmente le marginalità sulle vendite degli esercenti. La conseguenza è un possibile costo indiretto a carico del consumatore, poiché gli esercenti potrebbero tenere una soglia dei prezzi più elevata per sopperire all'incidenza di tali costi. Peraltro è presumibile che una maggiore diffusione di Bitcoin come sistema di pagamento potrebbe portare a una generale riduzione dei prezzi.

Per quanto riguarda l'utilizzo di Bitcoin, non sono da dimenticare le commissioni imputate agli utenti quando "passano attraverso" un exchange o un ATM per comprarli o venderli in cambio di euro o altra valuta legale. Tali commissioni variano generalmente dallo 0,1% allo 0,5% sull'importo scambiato.

2. Tempi di attesa per le transazioni

Una transazione di bitcoin impiega mediamente 10 minuti per essere registrata nella blockchain, ottenendo una prima conferma, mentre il numero di conferme che è consigliato attendere per ritenere un pagamento pervenuto a tutti gli effetti sono almeno sei, ovvero circa un'ora di tempo. Le sei conferme sono appunto consigliate, perché a quel punto la probabilità di un double-spending attack è veramente bassa (minore dello 0,1%). Tuttavia c'è da tenere presente che non tutti i clienti sono degli esperti informatici che ci vogliono truffare, e soprattutto è difficile che la loro abitazione sia una mining farm pronta a costruire una diversa versione della blockchain. Per questo motivo un esercente, anche in relazione al prezzo del bene o del servizio venduto, potrebbe accettare transazioni con zero conferme, semplicemente verificando che sono state processate perché appaiono in tempo reale sia all'interno del client Bitcoin che in un qualsiasi block explorer, lasciando uscire il cliente con il nuovo prodotto senza annoiarlo eccessivamente. Per transazioni di importi più sostenuti trattenere il cliente per qualche conferma non dovrebbe risultare un gravoso problema.

[31] SEPA (Single Euro Payments Area): l'area in cui si possono effettuare e ricevere pagamenti in euro, sia all'interno dei confini nazionali che fra i paesi che ne fanno parte, secondo condizioni di base, diritti e obblighi uniformi, indipendentemente dalla loro ubicazione all'interno della SEPA.

Infine dai 10 minuti ad un'ora di tempo per uno scambio di denaro tra due persone distanti tra loro, in qualunque parte del mondo uno si trovi, è comunque molto più vantaggiosa dell'attesa a cui ci costringe il circuito bancario, che richiede mediamente un giorno per processare un bonifico entro l'area SEPA, e dai tre o quattro giorni per l'invio di denaro al di fuori di tale area.

3. Facilità e accessibilità

Utilizzare Bitcoin è facile e alla portata di tutti. Chiunque può creare un indirizzo e ricevere dei pagamenti in qualunque momento e da qualunque parte del mondo, senza dover possedere un conto corrente bancario. Inoltre ognuno ha il totale controllo del proprio denaro non essendoci un'autorità che possa congelare i propri fondi o imporre ogni altro tipo di limitazione nell'utilizzo dei propri bitcoin.

4. Trasparenza e pseudonimia

Le transazioni di bitcoin sono perfettamente tracciabili e verificabili da chiunque, grazie alla pubblicità della blockchain. Tuttavia agli occhi del pubblico il registro non è interpretabile o associabile alle persone fisiche o giuridiche che stanno dietro a tutti quei codici; è possibile riconoscere solo il proprio indirizzo, e al limite quello di qualche commerciante dove si è fatto un acquisto o al limite quello di un amico che ce l'ha comunicato, per questo Bitcoin è un sistema pseudonimo.
Per quanto riguarda la lotta alla criminalità e al riciclaggio di denaro, Bitcoin può essere uno strumento potente per poter eludere i controlli sul traffico di denaro "sporco" e la compravendita anche online di prodotti illegali. D'altronde l'introduzione di tecnologie innovative apre sempre a nuove opportunità, anche illegali, ed è compito del governo trovare delle nuove soluzioni normative per contrastarle (la polizia postale per esempio non è sempre esistita).
Ricollegare gli indirizzi Bitcoin agli utilizzatori e quindi contrastare il riciclaggio non è comunque impossibile. Poiché i punti di accesso ed uscita dal sistema, cioè le diverse modalità di compravendita di bitcoin in cambio di valuta legale, sono controllati da società terze, attraverso le procedure di registrazione di ciascun utente ormai divenute obbligatorie, è possibile risalire alle identità fisiche e a tutte le operazioni effettuate e ricevute.

5. Rigidità del protocollo

Poiché Bitcoin è decentralizzato, nessuno ha l'autorità di modificare il protocollo o di costringere gli utenti e i minatori ad accettare tali modifiche. La comunità di esperti e sviluppatori informatici svolge un ruolo fondamentale nello scoprire e proporre la risoluzione di eventuali vulnerabilità del sistema che si presentano o vengono scoperte con il passare del tempo. Le modifiche sono apportate attraverso il rilascio di nuove versioni del client Bitcoin, ma queste si considerano accettate solo se la maggioranza di utenti e minatori passa a tale versione. Se un minatore non lavora con l'ultima versione in cui è stata introdotta una modifica nelle regole del protocollo, i blocchi da lui creati (validi se le regole non fossero cambiate) vengono rigettati dal network. Anche se la caratteristica di open source del sistema dà la possibilità di apportarvi modifiche, finora Bitcoin ha mantenuto le caratteristiche originali attribuitegli da Nakamoto, anche perché è difficile ottenere il consenso sulla proposta di modifiche rilevanti protocollo. Questa rigidità può essere vista come una vantaggio perché garantisce alti livelli di democrazia.

3.4 Gli svantaggi

1. Volatilità

La forte volatilità che caratterizza il prezzo dei bitcoin è la principale attrattiva per coloro che li detengono a scopi speculativi, ma anche un problema per tutte le altre categorie di utilizzatori. Le fluttuazioni del prezzo rendono rischioso detenere delle unità di bitcoin, e scoraggiano l'abbandono degli strumenti di pagamento tradizionali a favore della criptovaluta. I commercianti che li accettano in cambio di beni e servizi non possono fissare i prezzi di tali beni in bitcoin, ma devono controllare e aggiornare il tasso di cambio con le altre valute legali almeno giornalmente, col rischio che alla fine della giornata lavorativa tale cambio abbia subito ulteriori variazioni. I consumatori a loro volta non possono detenere importi elevati di bitcoin, e ciò si riflette negativamente sul loro impiego per gli acquisti. Una maggiore stabilità dei prezzi favorirebbe la diffusione su più ampia scala della criptovaluta, come pure l'aumento degli esercenti disposti ad accettarli, facilitando le loro decisioni in merito al consumo o al risparmio.

2. Irreversibilità delle transazioni

Bitcoin è un sistema per i pagamenti irreversibile. Quando un utente invia dei bitcoin ad un determinato indirizzo e la transazione è processata e registrata nella blockchain, non è possibile annullarla. L'unico modo per riavere il denaro indietro è conoscere l'identità del destinatario e chiederne la restituzione, cosa che può risultare assai ardua in caso di errore nella digitazione dell'indirizzo[32] considerata la pseudonimia del sistema.
Questa caratteristica può essere vantaggiosa ma anche svantaggiosa, a seconda dei punti di vista. Dal punto di vista degli esercenti un sistema di pagamento irreversibile è senza dubbio un vantaggio, specialmente per quanto riguarda il commercio online.
La procedura di *chargeback* prevista per gli strumenti di pagamento tradizionali consente infatti al consumatore di poter richiedere l'annullamento della transazione e la restituzione del denaro. Tale procedura è prevista a tutela del consumatore contro il furto di carte di pagamento, o dei dati relativi, e il loro utilizzo indebito da parte di

[32] Se si sbaglia a digitare l'indirizzo, perché la transazione sia processata tale indirizzo deve essere comunque esistente; se l'indirizzo sottoforma di qr-code viene scannerizzato dal proprio smartphone si risolve anche il problema di errata digitazione.

malintenzionati, ma anche contro i commercianti disonesti che tentano di frodare la clientela inviando merce difettosa o addirittura non inviando nulla a seguito di un acquisto online. Tali annullamenti dei pagamenti , oltre che causare un mancato ricavo per l'esercente, comportano anche dei costi amministrativi di invio della documentazione relativa all'acquisto indebito, e dunque perdita di tempo e risorse. Capita inoltre che il consumatore disonesto utilizzi il chargeback per frodare egli stesso l'esercente, simulando falsi furti degli strumenti di pagamento, o dichiarando ingiustamente che la merce acquistata sia difettosa; spesso capita che di fronte a queste spiacevoli eventualità, considerando anche il prezzo del bene in questione, il commerciante lasci perdere, perdendo anche l'incasso.
Bitcoin è dunque un sistema per i pagamenti elettronici più affidabile dal punto di vista dell'esercente, perché lo tutela maggiormente contro i consumatori disonesti, tuttavia i consumatori onesti non sono tutelati alla pari dei sistemi tradizionali.

3. Vulnerabilità dei servizi connessi

Se la solidità della struttura della blockchain e delle transazioni offrono importanti livelli di sicurezza a chiunque possieda delle unità della criptovaluta, la stessa cosa non può dirsi dei servizi connessi, in particolar modo i wallet e le piattaforme di exchange, a cui l'utente deve necessariamente rivolgersi per entrare nel mondo di Bitcoin.
Il meccanismo crittografico delle firme digitali impone che per rubare dei bitcoin ad un utente si debbano necessariamente rubare le chiavi private dei relativi indirizzi, poiché solo le chiavi private permettono di spendere i bitcoin di un indirizzo. L'utente generalmente custodisce le chiavi private o all'interno del proprio hard disk, oppure si affida ai servizi di web-wallet che le custodiscono in appositi server controllati dagli stessi fornitori del servizio. Tutti gli episodi negativi sin qui accaduti nella storia di Bitcoin sono stati degli attacchi hacker apportati proprio a questi ultimi livelli del sistema, in modo particolare ai server delle piattaforme di exchange, che hanno provocato ingenti perdite agli utenti e gravi ripercussioni sulla fiducia nella criptovaluta. Gli hardware wallet di cui si è spiegato nel primo capitolo possono rappresentare una risposta forte a questa necessità di maggiore sicurezza dei servizi connessi.

4. Regolamentazione

La situazione legale e fiscale di Bitcoin non è omogenea e varia da Stato a Stato.

Gli stati attualmente più avversi alla criptovaluta sono **Equador** e **Bolivia**, dove è illegale comprare o effettuare transazioni in bitcoin; in **Islanda** è illegale acquistare unità di criptovaluta, ma non è illegale la vendita o l'attività di mining; infine in **Russia** è prevista l'emanazione di un provvedimento legislativo entro la fine del 2015 che proibirà l'utilizzo delle criptovalute da parte di cittadini ed entità legali, e che sottoporrà a sanzioni le attività di mining o di emissione di Bitcoin o di altre valute digitali.

Dal dicembre 2013 la People Bank of **China** (PBOC) mediante l'avviso "*Precautions against the risks of Bitcoin*" proibisce alle banche e alle altre istituzioni finanziarie di comprare o vendere bitcoin, di accettarli come pagamento per beni e servizi e di offrire al pubblico ogni altro servizio correlato alla criptovaluta. Tuttavia non è illegale il possesso o la compravendita di bitcoin tra individui.

Nelle altre parti del mondo l'utilizzo di bitcoin non è illegale, ma gli Stati non sembrano essere d'accordo per quanto riguarda il loro inquadramento giuridico. Secondo gli esperti Bitcoin sarebbe qualificabile come "prodotto ibrido", in quanto ricalcherebbe sia le caratteristiche di una valuta che quelle di una *commodity*[33], e tale ambiguità si caraterizza anche la diversa presa di posizione dei vari Stati nei confronti delle criptovalute.

Negli **Stati Uniti** i bitcoin ricadono sotto la categoria delle valute virtuali, che a differenza di quelle reali non hanno corso legale ma possono comunque comportarsi come sostitute. Nel marzo 2013 il FinCEN (*Financial Crimes Enforcement Network*) stabilisce quali categorie di soggetti appartenenti al mondo di Bitcoin e di altre valute virtuali (in particolar modo exhange e gestori di ATMs) siano da ricomprendere nel gruppo degli MSBs (*Money Service Businesses*). Questo primo provvedimento normativo ha lo scopo di assoggettare questi nuovi tipi di business alle norme antiriciclaggio (AML) e alle procedure di *Know Your Client*[34] (KYC), che impongono precise misure di profilazione della clientela. Dal punto di vista fiscale i bitcoin sono considerati come una *property* (IRS Notice 14-21); i bitcoin ricevuti nell'ambito di vendite di beni o servizi devono andare a sommarsi al reddito lordo mediante loro valutazione al *fair market value*, cioè convertendoli in dollari statunitensi al tasso di cambio del giorno in cui sono stati ricevuti. I redditi percepiti dall'attività di mining vanno anch'essi a sommarsi al

[33] Commodity: bene indifferenziato, offerto sul mercato da differenti produttori ma senza differenze qualitative. Esempi di commodities sono i metalli o il petrolio.

[34] Know Your Client (KYC): processo da parte dell'azienda fornitrice del servizio di exchange della verifica dell'identità dei propri clienti.

reddito lordo del contribuente, mentre se i bitcoin sono detenuti a scopo di investimento, i guadagni ottenuti dalla loro vendita rientrano nella fattispecie di *capital gain*[35] e tassati come tali.

L'**Unione Europea** non ha finora adottato un regolamento specifico in merito al fenomeno delle criptovalute, limitandosi ad analizzarne il funzionamento ed evidenziando i rischi che possono derivare dal loro utilizzo. Negli Stati membri la compravendita di bitcoin e l'attività di mining sono comunque legali. La nazione in cui Bitcoin gode di maggiore chiarezza dal punto di vista normativo è certamente la **Germania**; a dicembre 2013 la BaFin (*Autorità Federale della Supervisione Finanziaria*) ha definito i bitcoin come "moneta privata" attribuendone la valenza come unità conto, ma ovviamente non considerandola a corso legale, implicando che i profitti derivanti dall'utilizzo dei bitcoin sono sottoposti a tassazione, così come l'applicazione delle norme antiriciclaggio alle società finanziarie che hanno a che fare con la criptovaluta.

L'"Avvertenza sull'utilizzo delle cosiddette valute virtuali" redatta dalla Banca d'Italia a inizio 2015, 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*", e mette in guardia i cittadini dai rischi che possono derivare dall'utilizzo dei bitcoin e delle altre criptovalute. L'Italia dunque, alla pari dell'UE non ha finora provveduto a fornire una chiara regolamentazione per Bitcoin.

Il quadro legale riguardante Bitcoin e gli altri tipi di criptovaluta appena delineato è certamente nella sua fase iniziale, e ci sono da aspettarsi numerosi cambiamenti in futuro. Affinché Bitcoin possa esplicare il proprio potenziale e possa diffondersi definitivamente come sistema di pagamento alternativo, è necessaria una normativa che faccia chiarezza sullo status legale di Bitcoin e sull'attività delle società che trattano direttamente i bitcoin, come ad esempio gli exchange; la stessa chiarezza è inoltre richiesta da un punto di vista fiscale per consapevolizzare gli utilizzatori e le aziende che li accetteranno come mezzo pagamento.

5. Vulnerabilità del protocollo

Le principali vulnerabilità di Bitcoin sono ricollegabili alla possibilità che un singolo nodo, o un gruppo di nodi organizzato, dotato di una grande potenza computazionale

[35] Capital Gain: differenza positiva tra il prezzo di acquisto e vendita di uno strumento finanziario.

possa avere la possibilità di mettere a repentaglio la stabilità dell'intero sistema. Il fatto che attaccare Bitcoin con un double-spending attack o con un 51% attack non sia economicamente vantaggioso, indipendentemente dal potenziale finanziario di ciascun individuo, non esclude che al mondo ci possano essere delle persone tanto ricche e allo stesso tempo irrazionali da voler arrecare dei danni alla società. Inoltre non si può sapere se in futuro le aziende produttrici dei dispositivi hardware impiegati per il mining ne manterranno costante il prezzo; in caso contrario il prezzo di un 51% attack potrebbe non essere più così proibitivo.

3.5 Il futuro di Bitcoin

Come già affermato in precedenza la parola Bitcoin indica sia il sistema per i pagamenti elettronici nella criptovaluta bitcoin, sia la tecnologia che rende possibile il suo funzionamento come sistema decentralizzato. Per questo motivo è opportuno compiere sia delle riflessioni in merito al futuro di Bitcoin come criptovaluta, sia un accenno alle possibili applicazioni alternative che può e potrebbe trovare la sua tecnologia.

3.5.1 Il bitcoin potrà sostituire le valute legali?

Secondo la tradizione economica la moneta deve essere in grado di soddisfare tre principali funzioni:

1. Riserva di valore: la moneta deve essere in grado di conservare il proprio valore nel tempo affinché gli individui possano decidere se utilizzarla subito oppure accumularla per spenderla in futuro;
2. Mezzo di scambio: la moneta deve svolgere la funzione di strumento di pagamento in cambio di beni e servizi, e deve essere comunemente accettata;
3. Unità di conto: la moneta deve svolgere la funzione di unità di misura comune, attraverso la quale determinare il prezzo dei beni e facilitare la misurazione delle transazioni economiche.

Vediamo ora come si comporta il bitcoin rispetto alle funzioni appena delineate, e come potrebbe comportarsi in futuro.

Con riferimento alla prima funzione, ovvero quella di riserva di valore, non si è in grado in questo momento di stabilire se il bitcoin conserverà o meno il proprio valore in futuro. Nonostante sia previsto un limite nel totale delle unità di criptovaluta in circolazione, e tale limite assieme a tutte le altre regole stabilite dal protocollo risultino difficili da stravolgere attraverso delle sostanziali modifiche, non si può prevedere con certezza la futura domanda di bitcoin da parte degli individui, vera determinante del prezzo della criptovaluta. La domanda futura di bitcoin dipenderà dal suo utilizzo futuro come strumento di pagamento. Il valore del bitcoin attualmente è troppo volatile da

poter essere considerato uno strumento di riserva di valore, e risulta assai arduo prevedere se questa volatilità persisterà anche in futuro o se il bitcoin raggiungerà un livello di prezzo stabile.

La funzione di mezzo di scambio è quella che il bitcoin sembra attualmente poter soddisfare più di tutte le altre, quella per cui del resto è stata ideata dallo stesso Satoshi Nakamoto. Con Bitcoin si possono effettuare pagamenti in modo semplice, veloce, con elevati livelli di privacy e a costi bassi se confrontati con tutti gli altri sistemi di pagamento tradizionali. Tuttavia la criptovaluta non è universalmente accettata come strumento di pagamento per beni e servizi, perciò è ancora difficile spenderli, ma sono in costante aumento gli esercizi commerciali, sia fisici che online, disposti ad accettarli, e di conseguenza sono in crescita gli individui desiderosi di utilizzarli. Come visto in precedenza, i volumi di denaro scambiati attraverso Bitcoin non sono che una modestissima frazione dei volumi totali scambiati tramite i sistemi per i pagamenti elettronici tradizionali, e tale frazione risulta ancora più infinitesimale se si considera che molte transazioni di bitcoin non riguardano l'acquisto di beni o servizi, ma sono processate solamente per fini speculativi.
Tuttavia, anche nell'ambito di questa seconda funzione non ci si può esimere da considerazioni riguardanti il futuro di Bitcoin. Considerando l'attività di mining e le modalità con cui viene remunerata, è necessario delineare gli scenari che potrebbero presentarsi in futuro quando le ricompense previste per la risoluzione di ogni blocco saranno quasi nulle, e l'unica fonte remunerativa sarà rappresentata dalle commissioni di transazione: la diffusione dei bitcoin come mezzo di pagamento potrebbe condurre ad un aumento del numero di transazioni giornaliere e quindi del totale dei ricavi derivanti dalle commissioni, compensando l'annullamento delle ricompense per i blocchi risolti; un altro possibile scenario potrebbe prevedere l'aumento del costo delle commissioni, annullando uno dei principali vantaggi derivanti dall'utilizzo della criptovaluta; il terzo scenario possibile prevedrebbe invece l'abbandono del mining da parte di numerosi individui o società poiché non più profittevole, con il rischio che tale attività e si concentri nelle mani di pochi soggetti o, nella peggiore delle ipotesi, che degeneri in un monopolio, cancellando la più innovativa caratteristica del sistema, ovvero la decentralizzazione. Dunque nemmeno il futuro utilizzo di bitcoin come mezzo di scambio è così certo, ed è difficile da prevedere in questo momento.

L'ultima funzione, ovvero quella di unità di conto, è difficilmente soddisfabile dal bitcoin nello stato attuale. L'elevata volatilità che caratterizza il prezzo della criptovaluta non ne consente un agevole utilizzo come unità di misura per determinare il valore dei beni. I commercianti dovrebbero aggiornare i prezzi dei beni in bitcoin anche più volte nell'arco della giornata, poiché il tasso di cambio con il dollaro o con altre valute legali cambia anche più volte nello stesso giorno. Per questo motivo i prezzi dei beni rimangono comunque nominati in valuta legale e convertiti in bitcoin al momento della vendita secondo il tasso di cambio corrente.

Da quanto emerso finora si può comprendere la difficoltà del bitcoin nel soddisfare in maniera esaustiva le tre funzioni che comunemente ci si aspetta da una moneta legale, sia attualmente che in previsione futura. Non essendoci un'autorità centrale che imponga l'utilizzo o l'accettazione del bitcoin come strumento di pagamento, il suo futuro non può che dipendere dalla volontà degli individui di utilizzarlo ed accettarlo, tuttavia permangono troppi dubbi che tale sistema possa raggiungere una definitiva diffusione.

Il primo dubbio è legato al persistere della forte volatilità del prezzo del bitcoin anche in futuro. Il tetto massimo prestabilito di unità di bitcoin in circolazione rende la sua curva di offerta inelastica, ovvero insensibile alle variazioni della domanda di criptovaluta degli individui, variazioni che vanno a riflettersi totalmente nel suo prezzo. Anche nell'ipotesi che il mercato scoprisse il reale valore del bitcoin come mezzo di scambio, comunque le variazioni della domanda di bitcoin determinerebbero delle fluttuazioni più o meno consistenti del prezzo, considerando che la domanda può variare in ragione di moltissimi fattori, dovuti per esempio alla stagionalità delle vendite o ai cicli economici. Se si rendesse l'offerta di bitcoin più elastica, per esempio aumentando o diminuendo le ricompense previste per la risoluzione dei blocchi in relazione al numero di transazioni processate in un determinato periodo di tempo antecedente, gli effetti delle variazioni della domanda si rifletterebbero lo stesso nel prezzo ma in maniera meno accentuata, garantendo maggiore stabilità, tuttavia questo richiederebbe una sostanziale modifica del protocollo e del disegno originale di Bitcoin.

Il secondo dubbio è legato alla possibilità che Bitcoin possa un giorno perdere le caratteristiche originarie. Come accennato prima, in futuro le commissioni di transazione potrebbero non bastare da sole a remunerare il lavoro dei minatori,

L'aumento delle commissioni di transazione sarebbe certamente negativo, ma la competitività di bitcoin potrebbe lo stesso perdurare nei confronti di alcuni dei sistemi per i pagamenti tradizionali. Invece il progressivo abbandono del mining da parte dei minatori con minori potenze di calcolo, che non riuscirebbero più a far fronte ai costi di energia elettrica e manutenzione, delineerebbe un'attività di mining concentrata nelle mani di pochi individui, o alla peggio di un solo minatore, che diventerebbe una sorta di autorità centrale; in questa situazione si manifesterebbe un vero e proprio fallimento di Bitcoin come sistema decentralizzato, la fiducia nella correttezza della blockchain potrebbe venire meno visto gli enormi poteri di frode nelle mani del monopolista, con gravi ripercussioni nell'utilizzo della criptovaluta e infine nel suo valore.

Alla luce di quanto analizzato all'interno di questo paragrafo, ricordando inoltre i vantaggi e gli svantaggi di Bitcoin illustrati nei paragrafi precedenti, si può concludere che è veramente improbabile che il bitcoin riesca in futuro a sostituire le valute legali, non sembrando in grado di poter soddisfare le funzioni di riserva di valore e di unità di conto. Il bitcoin come mezzo di scambio potrebbe invece trovare ampia diffusione in futuro, tuttavia è ancora troppo presto per dirlo, considerando che il fenomeno delle criptovalute è ancora giovane. Fondamentale per tale diffusione sarà lo sviluppo dei servizi connessi al mondo della criptovaluta, che dovranno offrire maggiori garanzie di sicurezza e rendere, se possibile, ancora più facile ed accessibile tale mondo. Fondamentali saranno inoltre le decisioni dei Governi in merito alla qualifica normativa e fiscale entro cui ricomprendere Bitcoin e le altre criptovalute.

3.5.2 Oltre la decentralizzazione dei pagamenti

Se i bitcoin entreranno o meno nelle "tasche" di tutti noi e saranno in grado di cambiare il modo di intendere il denaro è ancora presto per dirlo. Tuttavia l'innovazione introdotta da Satoshi Nakamoto non si limita al mondo delle criptovalute e dei sistemi di pagamento, ma sembra destinata a sconvolgere molti altri sistemi tradizionalmente basati sulla fiducia in un'autorità centrale.

L'innovazione tecnologica apportata da Bitcoin si esplica nella struttura e nel funzionamento della blockchain, un registro elettronico le cui informazioni sono protette crittograficamente e risultano impossibili da manomettere, e la cui autenticità è

garantita non da un'autorità centrale bensì dagli utenti in maniera decentralizzata sulla base del consenso. Un organo potenzialmente in grado da solo di soppiantare le autorità centrali e gli intermediari di molti sistemi esistenti, la cui applicazione al sistema monetario rappresenta soltanto un primo e particolare tentativo di decentralizzazione possibile.

Se è possibile infatti trasferire del denaro in maniera decentralizzata, in maniera rapida e sicura, allora potrebbe essere possibile anche scambiare delle risorse digitali per esempio, come le azioni di una società, le obbligazioni ed altri strumenti di investimento, che potrebbero rivoluzionare il sistema finanziario tradizionale.

Non solo gli intermediari finanziari, ma anche le società che offrono servizi di archiviazione di risorse digitali nel cloud[36]: Storj è infatti un sistema di archiviazione cloud decentralizzato che si basa sulla tecnologia di Bitcoin per garantire elevati livelli di privacy e anonimità nell'archiviazione di tali risorse, che non verrebbero più archiviati in un unico server gestito centralmente. Ogni file che l'utente desidera archiviare nel cloud viene criptato e distribuito tra i nodi di Storj attraverso la rete p2p, mentre le chiavi per decriptare il file rimangono in possesso al proprietario, pertanto lui solo ha accesso a tali risorse; i nodi di tale network conservano i file degli utenti all'interno dei propri dispositivi, trasferiscono tali file all'utente quando ne richiede il download, e sono remunerati in base alla memoria messa a disposizione.

Poiché la blockchain può prestarsi all'archiviazione in modo sicuro di file criptati, questa potrebbe essere utile per depositarvi i brevetti industriali in maniera anonima, senza doverli depositare pubblicamente e allo stesso tempo poter dimostrare, qualora ce ne fosse bisogno, che quel particolare brevetto è stato depositato (a tale data e a tale ora nella blockchain) all'interno della blockchain.

Queste appena esposte sono solo alcune delle principali applicazioni alternative della blockchain, il cui futuro sembra avere in serbo molte novità. Secondo gli esperti informatici Bitcoin rappresenta infatti soltanto un punto di partenza, una *killer app* per utilizzare un gergo informatico, ovvero una particolare applicazione di una determinata tecnologia il cui successo nel mercato ha l'effetto di aprire la strada ad altre diverse applicazioni della tecnologia stessa.

[36] Cloud storage: sistema di conservazione di dati su server appartenenti e gestiti da società terze.

b. CONCLUSIONI

All'interno di questo elaborato si sono analizzate le caratteristiche tecniche che permettono il funzionamento di Bitcoin, in particolare della blockchain, un registro distribuito e aperto a chiunque, che tenendo traccia di tutte le transazioni risolve senza la necessità di un'autorità centrale il problema del double-spending. La blockchain e l'impossibilità di una sua manomissione è sicuramente l'elemento più innovativo del sistema, la cui applicazione alternativa a Bitcoin sembra in grado di rivoluzionare tutti i sistemi di gestione centralizzata a cui siamo abituati. L'analisi del funzionamento del sistema ha evidenziato alcune vulnerabilità del sistema, che potrebbero destare qualche preoccupazione sul futuro della criptovaluta, anche se per ora si trattano di possibilità piuttosto remote.

Molte più preoccupazioni sul futuro della criptovaluta sono emerse invece da una sua analisi dal punto di vista economico. Bitcoin non è attualmente adatto per essere utilizzato come una moneta: l'unica funzione che sembra in grado di soddisfare è quella di mezzo di scambio (funzione per cui è stato ideato) ma il numero di persone disposte ad accettarli è ancora troppo esiguo per permetterne la facilità di utilizzo; la volatilità del suo prezzo, che è determinato dal mercato, non ne consente l'utilizzo né come riserva di valore, né come unità di conto. Il volume scambiato dalle transazioni di bitcoin è di modestissime dimensioni, tale da non rappresentare una minaccia né per le Banche Centrali, né per la permanenza sul mercato di banche o intermediari che gestiscono i sistemi per i pagamenti tradizionali.

L'incertezza in merito al suo futuro, la mancanza di una chiara presa di posizione da parte di molti dei governi mondiali dal punto di vista normativo e fiscale, la vulnerabilità dei servizi connessi e la mancanza di tutela dei consumatori che li utilizzano, oltre che le motivazioni sopracitate, ostacolano la definitiva diffusione della criptovaluta, che attualmente si comporta più come strumento su cui speculare che come strumento per i pagamenti.

Tuttavia non si può escludere che sia il bitcoin, che altre criptovalute esistenti o che nasceranno in futuro, potrà un giorno trovare maggiore diffusione di quanto non ce l'abbia adesso. L'inelasticità dell'offerta di bitcoin, dovuta al tetto massimo di unità in circolazione previsto, è la principale responsabile delle forti oscillazioni di prezzo. Tale svantaggio sembrerebbe destinato a protrarsi anche in futuro, ma potrebbe anche nascere una nuova criptovaluta migliore di bitcoin, più stabile e più adatta ad essere utilizzata come moneta. Anche bitcoin inoltre potrebbe avere un futuro; il suo mercato è ancora giovane, il suo reale valore di utilizzo come mezzo di scambio deve ancora essere scoperto, e il suo prezzo potrebbe raggiungere buoni livelli di stabilità.

Tutto questo sarebbe comunque il frutto di una generale evoluzione di ogni particolare determinante della domanda di bitcoin e delle criptovalute in generale; gli Stati dovrebbero dare loro una qualificazione omogenea e i servizi connessi dovrebbero migliorare dal punto di vista della sicurezza e dei servizi offerti. Allora molti più commercianti sarebbero disposti ad accettare i bitcoin, e molte più persone li potrebbero utilizzare per gli acquisti, e la sua diffusione sarebbe tale da poter essere usato ovunque come moneta alternativa, ma questo è ancora troppo presto per dirlo.

c. BIBLIOGRAFIA

A BEGINNER'S GUIDE TO BITCOIN, coindesk.com, URL: http://www.coindesk.com/information/, data ultima consultazione 18/05/'15.

BANK OF ENGLAND, "*The economics of digital currencies*", Quaterly Bullettin 2014 Q3, URL: http://www.bankofengland.co.uk/publications/Documents/, data ultima consultazione 18/05/'15.

BLIND SIGNATURE, Wikipedia, L'enciclopedia libera, URL: https://en.wikipedia.org/wiki/Blind_signature, data ultima consultazione 18/05/'15.

BITCOIN WIKI, URL: https://it.bitcoin.it/wiki/Pagina_principale, data ultima consultazione 31/05/'15.

BITCOIN.ORG, URL: bitcoin.org/it, data ultima consultazione 31/05/'15.

BITCOIN.ORG, Developer Guide, URL: https://bitcoin.org/en/developer-guide, data ultima consultazione 31/05/'15.

BUCHHOLZ M., DELANEY J. e WARREN J., "*Bits and Bets. Information, Price Volatility, and Demand for Bitcoin",* URL: http://www.bitcointrading.com/pdf/bitsandbets.pdf, 2012.

CALCOLO DISTRIBUITO, Wikipedia, L'enciclopedia libera, URL: https://it.wikipedia.org/wiki/Calcolo_distribuito, data ultima consultazione 31/05/'15.

CIAIAN, RAJCANIOVA e KANKS1, "The economics of Bitcoin price formation", URL: http://arxiv.org/ftp/arxiv/papers/1405/1405.4498.pdf, 2014.

CHANG J.M., "*First Bitcoin ATM Installed in Vancouver Coffee Shop*", abcnews.go, 30/10/'13, URL: http://abcnews.go.com/Technology/bitcoin-atm-conducts-10000-worth-transactions-day/story?id=20730762, data ultima consultazione 31/05/'15.

CHAUM D., "*Blind signatures for untraceable payments*" URL: http://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF, 1982.

CRITTOGRAFIA ASIMMETRICA, Wikipedia, L'enciclopedia libera, URL: https://it.wikipedia.org/wiki/Crittografia_asimmetrica, data ultima consultazione 31/05/'15.

CRYPTOCURRENCY, oxforddictionary.com, http://www.oxforddictionaries.com/definition/english/cryptocurrency, data ultima consultazione 31/05/'15.

CRYPTOGRAPHY@METZDOWN.COM, mail-archive.com, URL: Cryptography@metzdowd.com/, data ultima consultazione 31/05/'15.

DAI Wei, "B-money", URL: http://www.weidai.com/bmoney.txt, 1998.

DeMARTINO I, "*The many types and functions of bitcoin wallets*", 20/06/2014, URL: http://cointelegraph.com/news/111891/the-many-types-and-functions-of-bitcoin-wallets

ECB, "*Virtual currency schemes",* URL: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, ottobre 2012.

ECB, "*Virtual currency schemes – a further analysis",* URL: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, febbraio 2015.

E-GOLD, Wikipedia, L'enciclopedia libera, URL: https://en.wikipedia.org/wiki/E-gold, data ultima consultazione 18/05/'15.

FINCEN, "*Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*", 18/03/'13, URL: http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

FUNZIONE CRITTOGRAFICA DI HASH, Wikipedia, L'enciclopedia libera, URL: https://it.wikipedia.org/wiki/Funzione_crittografica_di_hash, data ultima consultazione 18/05/'15.

GRIFFITH K., "A quick historyof criptocurrencies BBTC – Before Bitcoin", Bitcoin Magazine, 16/04/'14, URL: https://bitcoinmagazine.com/12241/quick-history-cryptocurrencies-bbtc-bitcoin/, data ultima consultazione 18/05/'15.

KRISTOUFEK L., *"What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis"*, URL: http://arxiv.org/pdf/1406.0268v1.pdf, 2014.

NAKAMOTO Satoshi, "*Bitcoin: a peer-to-peer electronic cash system*", URL: https://bitcoin.org/bitcoin.pdf, 2008.

NARAYANAN A., *"What Happened to the Crypto Dream?Part 1"*, IEEE Security & Privacy, vol. 11, no. 2, 2013, pp. 75–76, URL: http://randomwalker.info/publications/crypto-dream-part1.pdf.

PEER-TO-PEER, Wikipedia, L'enciclopedia libera, URL: https://it.wikipedia.org/wiki/Peer-to.peer, data ultima consultazione 31/05/'15.

PBOC, Bank Notice No. 239, 2013.

POLCI M., "*Cos'è il bitcoin –seconda parte*", rischiocalcolato.it, 16/12/'13 URL: http://www.rischiocalcolato.it/2013/12/cose-il-bitcoin-seconda-parte.html, data ultima consultazione 18/05/'15.

ROSENFELD M,"*Analysis of hashrate-based double-spending*", URL: https://bitcoil.co.il/Doublespend.pdf, 11/12/'12.

SZABO N., "*Bitgold*", http://unenumerated.blogspot.it/2005/12/bit-gold.html, 27/12/'08.

THE NILSON REPORT: GENERAL PURPOSE U.S. CARDS 2014, URL: http://www.nilsonreport.com/, data ultima consultazione 18/05/'15.

VOORHEES E., "*What is Bitcoin*?", Bitcoin Magazine, 15/05/'15, URL: https://bitcoinmagazine.com/19020/bitcoin/ , data ultima consultazione 18/05/'15.

WAGNER A., "*Digital currency vs virtual currency*", Bitcoin Magazine, 22/08/'14, URL: https://bitcoinmagazine.com/15862/digital-vs-virtual-currencies/ data ultima consultazione 18/05/'15.

WAGNER A., *"The role and future of altcoins"*, Bitcoin Magazine, 22/05/'14, URL: https://bitcoinmagazine.com/13150/role-future-altcoins/ data ultima consultazione 18/05/'15.

WAGNER K., "*World's first bitcoin ATM opnes in Vancouver, Canada*", 31/10/'13, meshable.com, URL: http://mashable.com/2013/10/30/bitcoin-atm-2/, data ultima consultazione 18/05/'15.

WILMOTH J, "*What is altocoin?*", cryptocoinsnews.com, 12/09/'14 ,URL: https://www.cryptocoinsnews.com/altcoin/, data ultima consultazione 18/05/'15.