Bitcoin, Blockchain, Crypto

Carlomaria Occhipinti

5F

Liceo Scientifico Arturo Tosi

Busto Arsizio (VA)

Introduzione

Fin da quando ne son venuto a conoscenza nell'estate del 2017 sono sempre stato affascinato dal Bitcoin e dalle altre criptovalute.

Il funzionamento tecnico, il ruolo nei mercati finanziari, l'impatto sulla società... trovo tutto talmente interessante che passo una buona parte del mio tempo libero a leggere notizie, articoli, opinioni e dibattiti sull'argomento.

Mi rendo conto del fatto che questa delle criptovalute sia una materia nuova, l'inizio di un nuovo capitolo nell'ambito dell'informatica e forse anche in quello economico-sociale.

La novità dell'argomento mi ha fatto pensare che questo potesse essere un tema interessante da approfondire per la tesina di maturità.

L'ho scelto innanzitutto per passione, ma anche per avere l'opportunità di scrivere in un singolo testo tutti i concetti relativi alle criptovalute spiegandoli in modo dettagliato ma allo stesso tempo non eccessivamente complesso, cosa che non sono ancora riuscito a trovare da nessuna parte.

Spero che i lettori trovino la tesina di proprio gradimento, e chiedo scusa se certe parti risultano poco chiare.

Indice

1 Le origini del Bitcoin

2009. Il mondo è sconvolto dalla catastrofica crisi dell'anno precedente. L'economia era in distruzione. Banche, borse e stati sull'orlo del crollo. C'era il bisogno di una soluzione a tutto questo. Un sistema monetario che fosse immune a tutto ciò che colpì le valute crollate. Il Bitcoin[1], la prima criptovaluta del mondo creata a cavallo tra il 2008 e il 2009 fu la risposta a tutti questi problemi economici legati alla crisi.

Satoshi Satoshi Nakamoto è conosciuto come l'ideatore e l'iniziale sviluppatore del Bitcoin. L'identità di Satoshi è una questione discussa da sempre, e certi individui sono sospettati di essere il creatore del Bitcoin. In realtà nessuno sa veramente chi sia, dove abiti, se è un singolo o un gruppo di persone. Sappiamo solo che nei primi anni del Bitcoin era attivo sul forum bitcointalk.org fino al 13 dicembre 2010. e che il 31 ottobre 2008 Satoshi scrisse il *whitepaper*[2] del Bitcoin contenente la sua ideologia di moneta virtuale. Il documento è altamente tecnico e richiede un'elevata conoscenza di informatica e matematica, perciò ritengo superfluo citarne delle parti. [1]

Confronto con i soldi "tradizionali" Il Bitcoin si differenzia radicalmente dalla moneta legale[3]. Esso è:

- Decentralizzato: è una valuta internazionale, non legata particolarmente ad alcun paese (come lo Yen col Giappone, il Franco con la Svizzera). Le transazioni sono *peer-to-peer*, da pari a pari, senza la necessità di passare da un ente centrale come una banca.
- Deflazionario: la quantità totale limitata di bitcoin impedisce la perdita di valore della valuta, cosa che avviene frequentemente con le monete legali artificialmente inflazionate.
- Anonimo: non sono richieste informazioni personali per inviare e ricevere Bitcoin, per questo si ha una maggior tutela della privacy.
- Veloce: la natura *peer-to-peer* della valuta rimuove tutti gli eventuali ritardi e complicazioni che si possono avere con un gestore di carta di credito.

[1] Nella tesina scriverò "Bitcoin" con la 'B' maiuscola per riferirmi alla valuta in generale, mentre con "bitcoin" con la 'b' minuscola mi riferisco ai bitcoin in sé, la moneta usata per fare acquisti, per esempio "5 bitcoin"

[2] "Libro bianco", un documento redatto da un professionista esperto di una materia che offre informazioni di qualità e di interesse ad un pubblico selezionato di utenti.

[3] Chiamata anche "fiat" (da non confondersi con la casa di automobili)

2 Blockchain: cos'è e come funziona

La tecnologia rivoluzionaria utilizzata dal Bitcoin e da tutte le altre criptovalute è chiamata Blockchain. Come suggerisce il nome, "blockchain" indica una catena di blocchi. L'aspetto decentralizzato del Bitcoin gira intorno al fatto che chiunque può scaricare la blockchain e far sì che si aggiorni in tempo reale: ciò significa che finché esiste in tutto il mondo *almeno* un computer con la blockchain salvata, che prende il nome di *full node*, l'intera rete del Bitcoin e il registro delle transazioni rimangono autentiche e inviolate.

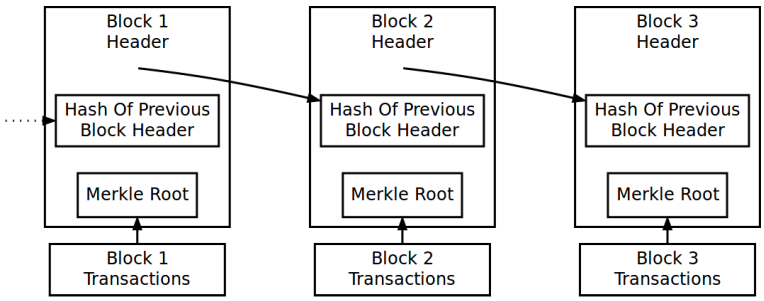

Figura 1: Schema della blockchain
fonte: bitcoin.org

2.1 Cosa sono i blocchi e che compito svolgono

Ciascun blocco contiene informazioni sulle transazioni di bitcoin che sono state effettuate di recente. Il blocco può essere visto come un contenitore, un hard disk grande 1MB che contiene un determinato numero di transazioni, che hanno un determinato peso espresso per comodità in kilobyte Tutte le transazioni di Bitcoin sono permanentemente, irreversibilmente[4] memorizzate nella Blockchain. Su un qualunque sito avente la funzione di "block explorer" posso cercare informazioni su ciascun indirizzo Bitcoin (per ora pensiamolo come se fosse un codice IBAN): posso vedere quanti bitcoin quell'indirizzo possiede, da quali indirizzi ha ricevuto quanti bitcoin, e a chi ne ha mandati. Sotto un punto di vista pratico, la blockchain del Bitcoin è un file di dimensioni oggi pari a circa 170 Gigabyte. La dimensione è così elevata perché in quel file sono contenute le informazioni di oltre 520.000 blocchi scoperti a partire dal primo, chiamato *genesis block*, trovato il 3 gennaio 2009. "Scoperti"? "Trovati"? In che senso? Da dove vengono questi blocchi? Mi tocca introdurre il concetto di *mining*.

[4]Nella maggior parte dei casi, vedi punto 3.3.1

2.2 Mining

Sebbene non sia tecnicamente corretto, il modo più semplice per spiegare il concetto di *mining* è quello di paragonare i bitcoin a una montagna nella cui roccia sono contenuti minerali preziosi. I bitcoin sono, per esempio, l'oro nella roccia. Per trovare l'oro bisogna scavare nella roccia della montagna utilizzando speciali apparecchiature quali ruspe, trapani, trivelle. I blocchi, per poter essere "scoperti" vengono "minati" dai cosiddetti *miner* ASIC [5], dei computer specializzati a risolvere un certo tipo di algoritmo che nel *whitepaper* Satoshi definisce come *proof of work*[6]: la PoW è l'algoritmo usato dal Bitcoin per confermare le transazioni e avanzare al blocco successivo della blockchain. Esso si basa sulla risoluzione di un problema matematico difficile (descritto nei paragrafi successivi) compiuta dai *miners* per poter ottenere una soluzione facilmente verificabile dai *full nodes* in tutto il mondo. Lo scopo della *proof of work* e il motivo per cui è presente un difficile problema matematico da risolvere è quello di impedire la generazione illimitata di blocchi e di conseguenza di abusare della blockchain .

Le hash L'obiettivo del *mining* è quello di indovinare una "parola chiave", chiamata *hash*, una serie di numeri e lettere che serve per trovare un blocco. Il Bitcoin usa l'algoritmo SHA-256, quindi le *hash* indovinate dai *miner* sono lunghe 64 caratteri. Questo perché come suggerisce il nome, 256 indica il numero di *bits* che costituiscono la stringa. Il *bit* è la più piccola unità di misura per quanto riguarda la dimensione di file nel campo dell'informatica, e 8 bit corrispondono a 1 byte. Nel sistema numerico esadecimale un carattere "pesa" 8 bit, quindi $256 : 8 = 64$. Una *hash* facente parte dell'algoritmo SHA-256 non può essere una qualunque combinazione di 64 numeri e lettere, ma deve rispettare determinati parametri per essere considerata tale, di cui non scriverò per evitare di complicare ulteriormente la situazione. In succinto, per trovare il numero di *hash* totali che si possono ottenere bisogna effettuare il calcolo 2^{256}, che corrisponde a circa $1,158 \times 10^{77}$ possibili *hash* da indovinare. Le *hash* che portano alla scoperta di uno specifico blocco, però, possono essere più di una.

2.2.1 Target e difficoltà di mining

Per trovare un blocco è necessario che i *miners* trovino un'*hash* che sia inferiore al cosiddetto *target*. Il *target* è un'*hash* che fa da "confine" sotto al quale tutte le *hash* sono accettabili. Tutte le *hash* trovate dai *miners* che hanno valore minore del *target* sono valide, e portano alla scoperta di un nuovo blocco. Con "difficoltà" si intende, ovviamente, quanto è difficile trovare un blocco, e il suo valore è collegato a quello del *target*. Più si abbassa il *target*, più si alza la difficoltà, perché abbassandosi il *target* le *hash* valide diventano meno, quindi la probabilità che i *miners* ne trovino una valida si riduce. Ma perché dovrebbe abbassarsi il *target*?

[5] *Application specific integrated circuit*, "circuito integrato con una specifica applicazione"
[6] Abbreviato "PoW", tradotto "prova di lavoro" o "prova di funzionamento"

Man mano che sempre più *miners* cominciano a lavorare, elevando l'*hashing power* complessivo del network del Bitcoin, se non ci fossero cambi di *target* i blocchi verrebbero trovati con frequenza sempre più elevata.

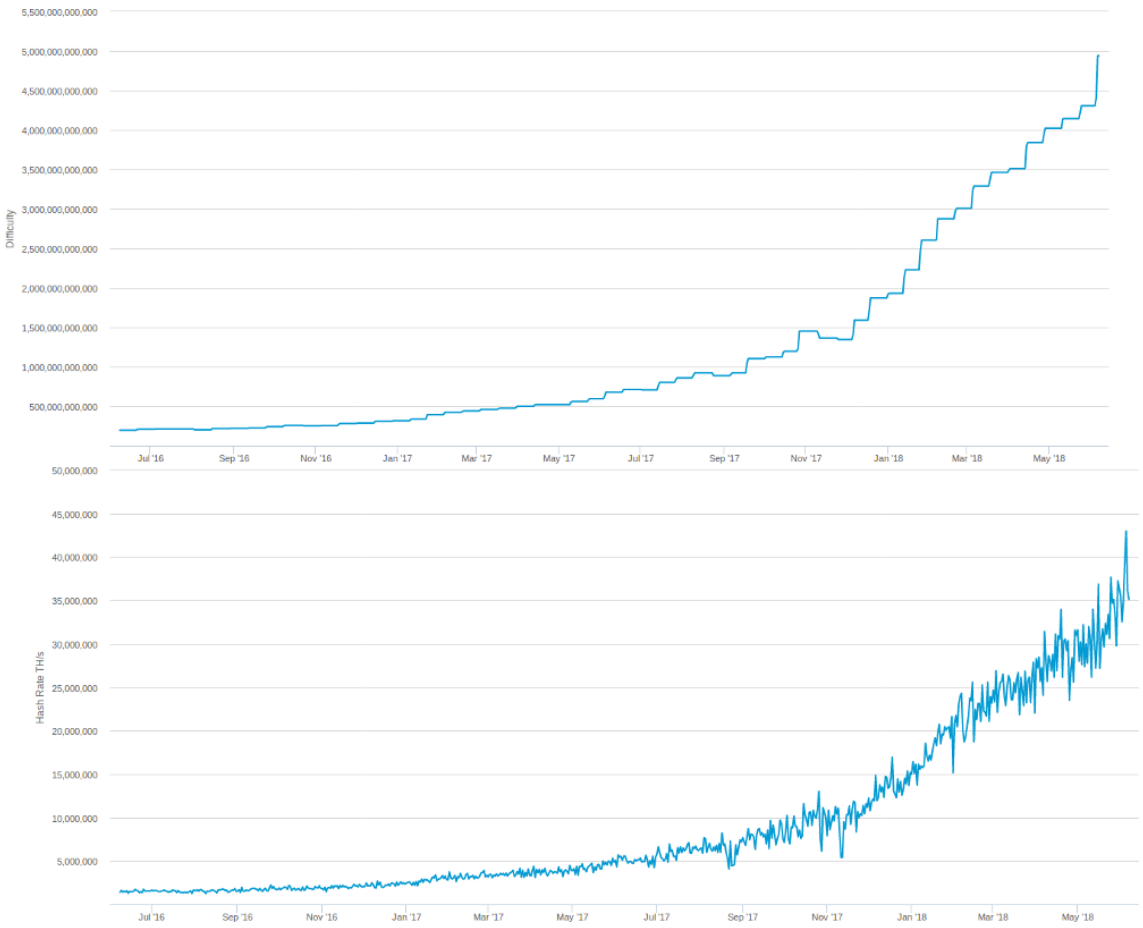

Figura 2: Confronto tra difficoltà (sopra) e *hashrate globale* (sotto)
fonte: blockchain.info

L'innalzamento o talvolta anche l'abbassamento della difficoltà avviene ogni 2016 blocchi (circa 2 settimane), quando il network controlla la frequenza con cui questi ultimi blocchi sono stati trovati. Modificando la difficoltà in modo proporzionale all'*hashing power* si fa in modo che in media i blocchi continuino ad essere trovati ogni ~10 minuti. Perché 10 minuti?

Tempo per blocco Satoshi ha deciso che ogni blocco deve impiegare un tempo di circa 10 minuti per essere scoperto. Il motivo della scelta è quello

di aver trovato un compromesso: sacrificare conferme e quindi transazioni più veloci per avere un processo di *mining* più efficiente. Nell'intervallo di 10 minuti tutti i *full nodes* hanno tempo sufficiente per accettare e validare l'ultimo blocco trovato e far sì che si propaghi in tutta la rete, impedendo eventuali conflitti su qual è la blockchain autentica. Quando non avviene ciò, può capitare che fra due blocchi che vengono trovati in istanti vicini solo uno dei due venga accettato dalla maggioranza dei *full nodes*. Il blocco che viene abbandonato è definito *stale block*[7], ovvero un blocco inizialmente considerato valido, ma poi abbandonato perché l'altro blocco trovato è stato accettato più velocemente, dando origine alla blockchain più lunga tra le due, quindi quella più reputabile. Per questo con i blocchi di 10 minuti si ha un *mining* più efficiente, perché si riduce la quantità di energia elettrica sprecata per far funzionare dei *miners* che trovano un blocco orfano. Quando viene trovato un blocco, tutti i *miners* devono interrompere la ricerca del blocco ormai trovato e cominciare a lavorare su quello successivo. Se questi non si fermano, troveranno eventualmente un blocco che è gia stato trovato, e che quindi non può essere "attaccato" alla blockchain. Un blocco orfano, *orphan block*, invece, è un blocco minato da un *miner* che non può essere accettato nella blockchain perché il *node* del *miner* non si è ancora aggiornato alla blockchain più recente che include il blocco precedente a quello appena trovato. Non avendo un "genitore" (*parent*), il blocco trovato dal *miner* non viene propagato agli altri *full nodes* perché non è "collegato" ad altri blocchi. A partire dalla versione 0.10 del software del Bitcoin, però, non possono più esistere blocchi orfani a seguito di una modifica radicale del sistema con cui i *nodes* scaricano i nuovi blocchi [2].

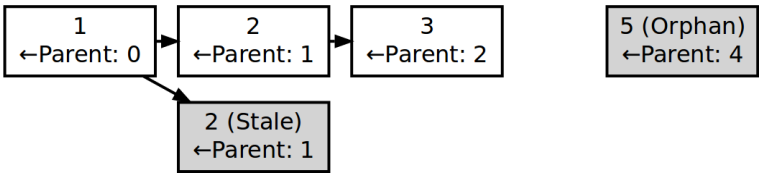

Figura 3: Rappresentazione di blocchi in stallo e orfani

Il tempo di 10 minuti di certo riduce la probabilità che vengano creati blocchi in stallo; tuttavia è sempre possibile che nascano.

2.2.2 Costi del mining

I *miner* di Bitcoin che si usano oggi lavorano a velocità comprese tra i 10 e i 14 TH/s[8] in base al loro consumo energetico, ovvero a oltre dieci trilioni di *hash* trovate in un secondo. Questi apparecchi sono molto costosi (quelli di ultima generazione superano i €700 per unità) e utilizzano un'elevata quantità

[7] Blocco in stallo
[8] Tera-hash al secondo

di energia elettrica per funzionare. Perchè, allora, c'è gente che spende tutti questi soldi per fare il lavoro di *mining*? Ebbene, quando si trova un blocco, oggi il *miner* riceve una quantità pari a 12.5 BTC, pari a circa €90.000 secondo il prezzo attuale. Quasi mai, però, la *block reward*[9] finisce a una singola persona: indovinare l'*hash* che trova il blocco è estremamente difficile! Per questo esistono le *pool* di *mining*.

L'uso di elettricità del mining I *miner* ASIC usano una notevole quantità di energia. Prendendo in considerazione quelli di ultima generazione, il più potente, il Bitmain Antminer S9 (14 TH/s) consuma circa 1300 W [3]; il più debole, l'Antminer V9 (4 TH/s) 1000 W [4]. In media, un S9 che lavora in una *pool* di *mining* fa guadagnare circa 0,00082 BTC al giorno, ovvero circa €5,5 [5]. Considerando che le *farm* sono locate in paesi come la Cina in cui l'elettricità costa poco, intorno ai €0.04/kWh[10], un S9 costa circa €1 al giorno in elettricità. Un *miner*, quindi, fa guadagnare almeno €4 al giorno considerando il costo dell'elettricità. Ho già scritto che i *miner* hanno un prezzo notevole, infatti un Antminer S9 costa attualmente ~€717. Prima di cominciare a guadagnare un profitto nel *mining*, bisogna calcolare il tempo impiegato per coprire il costo dell'attrezzatura di *mining*. Questo tempo si chiama ROI[11], e nel caso della situazione presa come esempio, ovvero quella di guadagnare €4 al giorno con un S9, il ROI è pari a 179 giorni, infatti

$$€717 : \frac{€4}{1giorno} = 179,25giorni$$

Questo è quanto vale per *un* singolo ASIC che produce solo 0,00082 BTC al giorno, una quantità minuscola rispetto ai ~17.000.000 che sono stati minati fino ad oggi. L'*hashing power* dell'intero network del Bitcoin, la somma del lavoro dei *miners* in tutto il mondo espressa in H/s, è di oltre 30.000 TH/s, e consuma un a quantità di elettricità pari a 60 TWh all'anno, ovvero $2,16 \times 10^{77}$ Joule consumati in un anno. Questo consumo di elettricità è maggiore dell'utilizzo di elettricità annuale di Algeria (60 TWh/anno), Colombia (52 TWh/anno), Portogallo (47 TWh/s) e Nuova Zelanda (39 TWh/anno) [8].

2.2.3 Profitti del mining

Perchè, allora, c'è gente che spende tutti questi soldi per fare il lavoro di *mining*? (lo metto prima o dopo inizio sezione?) Ebbene, quando si trova un blocco, oggi il *miner* riceve una quantità pari a 12.5 BTC, pari a circa €90.000 secondo il prezzo attuale. Quasi mai, però, la *block reward* finisce a una singola persona: indovinare l'*hash* che trova il blocco è estremamente difficile! Per questo esistono le *pool* di *mining*.

[9] Ricompensa del blocco

[10] Il costo medio per kWh in Cina è di €0,07 [6], ma l'energia pulita generata dai pannelli solari e dalle turbine costa molto meno [7]

[11] *Return on investment*

Mining pools Le *pool* sono dei siti in cui più *miners*[12] uniscono gli sforzi per trovare un blocco. Nella configurazione del software che fa compiere il *mining* agli ASIC bisogna inserire l'indirizzo web della *pool* per la quale si vuole lavorare, e il *miner* comincierà ad inviare le *hash* che calcola alla *pool*. Una volta trovato il blocco, la ricompensa di bitcoin si spartisce fra tutti i *miner*, in base a quanto ciascuno si è impegnato per trovarla. È possibile controllare il lavoro dei *miners* tramite un'interfaccia remota. Su tutti i siti delle *pool* è possibile inserire in un campo di ricerca l'indirizzo Bitcoin verso cui i bitcoin ricavati saranno inviati.

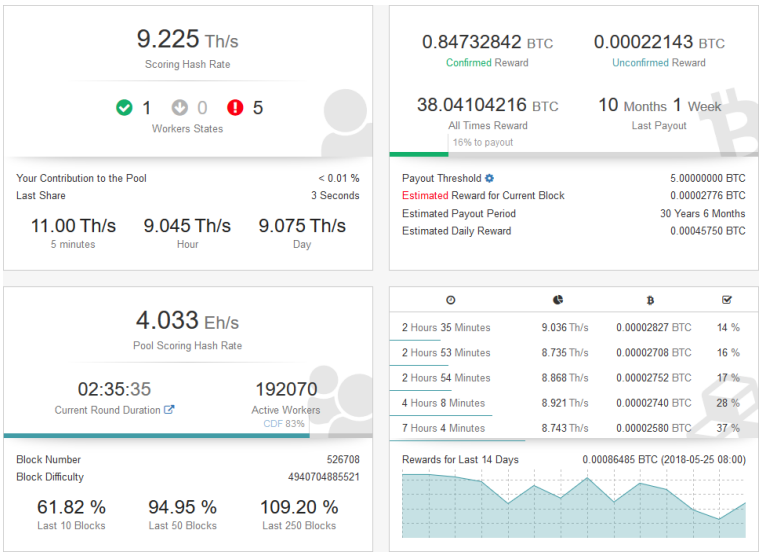

Figura 4: Interfaccia di una *mining pool*: si possono scorgere *hashrate*, bitcoin guadagnati, le stime sui guadagni giornalieri e il tempo rimanente per ricevere il pagamento *(fonte: slushpool.com/dashboard)*

Tassa di transazione La scoperta dei blocchi non è l'unico metodo con cui coloro che praticano *mining* guadagnano Bitcoin. Ogni transazione di Bitcoin prevede il pagamento di una piccola quota, solitamente compresa tra €0.01 e €1. Questa quota, chiamata *miner fee* serve per incoraggiare i *miner* a selezionare la nostra transazione da includere nel blocco in fase di ricerca. Questa tassa è espressa in sat/b, satoshi[13] per byte. Una tassa più elevata riduce il tempo di conferma della transazione, perché preferita dai *miner*. Al contrario, una transazione effettuata con una tassa inferiore alla media impiega più tempo ad essere inclusa in un blocco e quindi ad essere processata, perché i *miner*

[12] Con "*miner*" ci si può riferire sia ai computer che compiono il lavoro, sia alle persone che li operano e che guadagnano bitcoin

[13] Un satoshi è l'unità di misura più piccola del bitcoin, e corrisponde a 1×10^{-8} BTC

guadagnano più BTC dalle transazioni più costose. Come ho spiegato ciascuna transazione pesa tot kilobyte, quindi, conoscendo il peso in kb della transazione e avendo stabilito il valore della tassa in sat/b[14] per scoprire quanto paghiamo effettivamente possiamo ricavare la quantità di BTC dalla proporzione.

$$nSatoshi : 1byte = tassa : pesoTransazione$$

o semplicemente utilizzando la formula $tassa = \frac{nSatoshi \times pesoTransazione}{1byte}$.

Il futuro del mining In precendenza ho detto che la scoperta di un blocco porta al guadagno dei *miners* di 12.5 BTC. Questa ricompensa, però, non è un valore costante: ogni 210.000 blocchi trovati la quantità di bitcoin che i *miners* ricevono si dimezza, infatti la ricompensa iniziale era di ben 50 BTC. Questo processo di dimezzamento è chiamato *halving*. Oggi abbiamo superato il blocco numero 526000, infatti essendo $526.000 : 210.000 = \sim 2.5$, fin ora ci sono stati due *halving*. $50 : 2 = 25$, $25 : 2 = 12.5$, la ricompensa attuale. I bitcoin, però, esistono in quantità limitata, infatti il limite massimo è di 21.000.000 BTC. Fino ad oggi sono stati minati circa 17.000.000 BTC, ovvero l'81% della quantità totale. Eventualmente tutti i bitcoin verranno minati, e i profitti dei *miners* dipenderanno esclusivamente dalle tasse di transazione.

[14] Spiegherò come si viene a conoscenza di queste due nel punto X.Y

3 Aspetto tecnico del Bitcoin

3.1 Mempool: il primo passo delle transazioni

La *mempool* è il luogo in cui si trovano tutte le transazioni effettuate non ancora confermate dai *miners*. Si può dire che una volta effettuate, le transazioni si mettono in lista d'attesa nella *mempool*, aspettando che un *miner* la includa nel blocco che sta cercando. Ciascun *full node* ha una propria mempool, di dimensione massima variabile a seconda della quantità di RAM del computer.

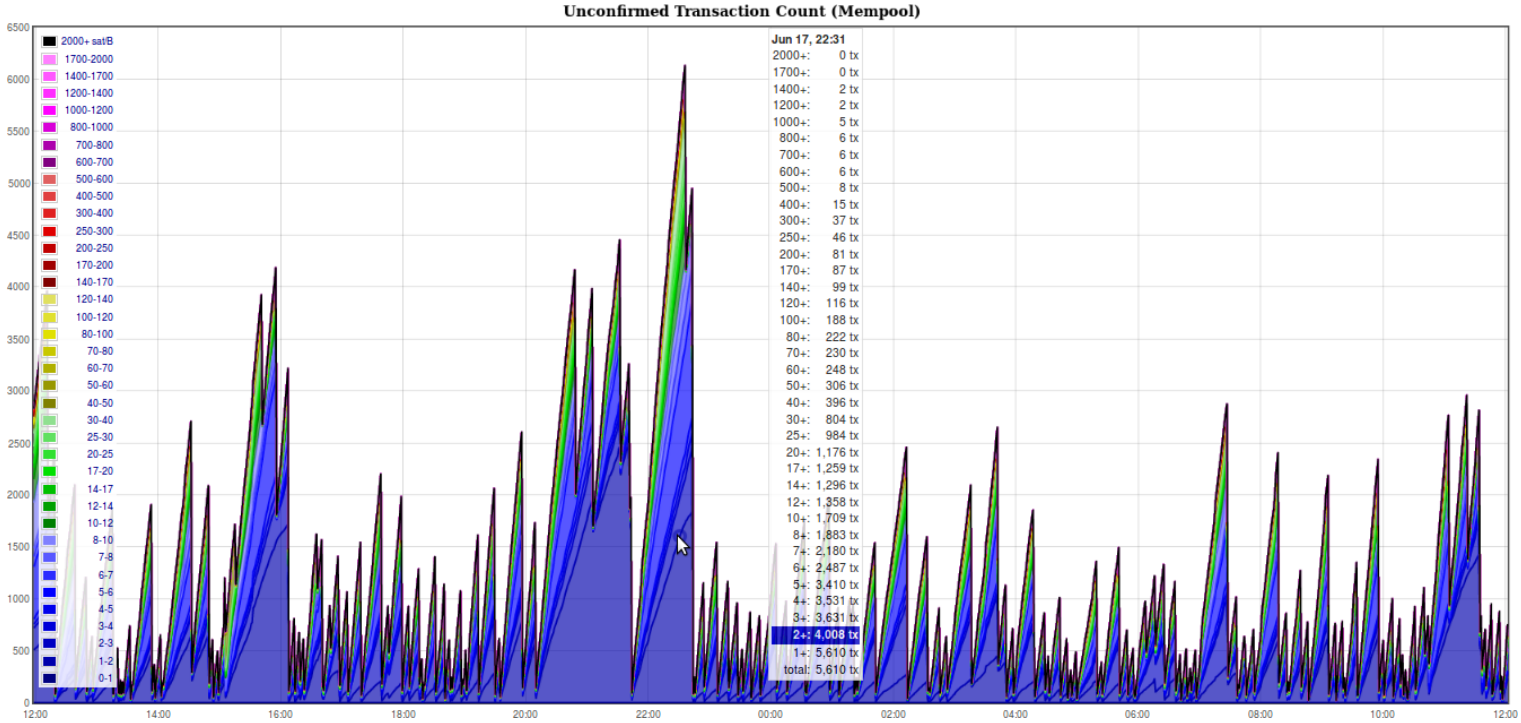

Figura 5: Grafico del numero di transazioni nella *mempool*
fonte: jochen-hoenicke.de/queue

I diversi colori indicano il valore della tassa in sat/b usato per effettuare le transazioni. Le tonalità di blu rappresentano quelle comprese tra 0 e 10 sat/b, quelle verdi tra 10 sat/b e 40 sat/b e così via. Il 17 giugno alle ore 22:21, per esempio, sono state effettuate 4008 transazioni con una tassa di 2 sat/b e 396 con una tassa compresa tra 40 e 50 sat/b, per un totale di 5610 transazioni.

In questa figura è raffigurata (suona male) la somma di tutte le tasse delle transazioni effettuate in un determinato istante. Per esempio, alle 22:25 del 17

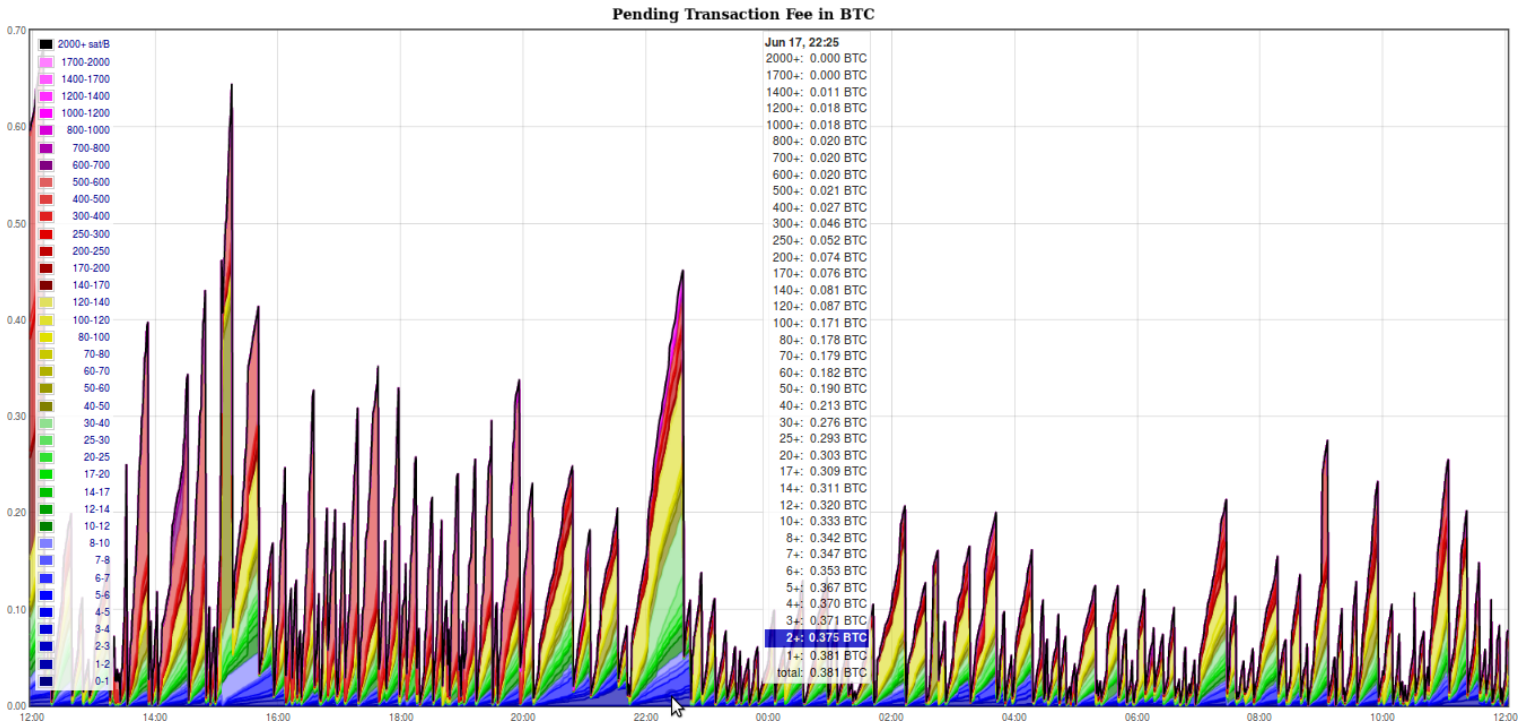

Figura 6: Grafico della tassa complessiva in bitcoin
fonte: jochen-hoenicke.de/queue

giugno la somma delle tasse di tutte le transazioni che pagano 2 sat/b (circa 4000 secondo il grafico precedente) è pari a 0,375 BTC.

3.2 Come e dove si conserva

3.2.1 Indirizzi

Poiché i bitcoin non sono oggetti materiali, si dice che nella blockchain sono associati x BTC a ciascun indirizzo. Esistono 2^{160} diversi indirizzi (non sto a dire xk xk trpp cmplct) Gli indirizzi sono delle stringhe di 34[15] caratteri che possono essere visti come codici IBAN se si vuole rimanere in un contesto finanziario, o anche come indirizzi email. Esistono diversi tipi di indirizzo.

P2PKH Gli indirizzi P2PKH "*Pay To PubKey Hash*", comunemente chiamati indirizzi "legacy", sono il primo formato di indirizzo, utilizzato esclusivamente fino all'agosto del 2017. Questi indirizzi si riconoscono dal fatto che iniziano col carattere '1', per esempio `12dmWhp2dyog8GQRX3GMFqmFmV3duWUMmN`.

[15] Nella stragrande maggioranza dei casi

P2SH SegWit P2SH significa "Pay To Script Hash". Gli indirizzi P2SH sono stati ideati il 18 ottobre del 2011 con il BIP[16]-13 e lanciati l'1 Aprile del 2012 [**bip13**]. CITE METTERE 1 APRILE 2012 Il lancio di questi indirizzi non avvenne affatto in modo liscio e "indolore": il problema principale è che tutti i *miners* che non hanno aggiornato il proprio *full node* stavano includendo nei blocchi transazioni ritenute invalide dai loro software. La differenza sostanziale con gli indirizzi "normali" è che tramite cose tecniche utilizzano la tecnologia SegWit[17] per ridurre potenzialmente la tassa di transazione. Il sistema/protocollo P2SH richiede però la presenza di uno script che aumenta lievemente il peso della transazione, che non è presente nell'ultimo tipo di indirizzo.

bech32 Gli indirizzi Bitcoin *bech32* sono stati introdotti il 20 marzo 2017 con il BIP-173 [**bip173**]. Gli indirizzi bech32 implementano SegWit nativamente, e di conseguenza sono quelli con le dimensioni di transazione più inferiori. Questo tipo di indirizzo, essendo sotto un punto di vista tecnico molto diverso dagli indirizzi tradizionali (che cominciano con 1 e 3), non è supportato da una moltitudine di siti di compravendita e da portafogli che non riconoscono il `bc1q` presente all'inizio di tutti questi indirizzi, ma sempre più piattaforme e app si stanno aggiornando per permettere di inviare e ricevere dagli indirizzi bech32.

3.2.2 Keys

Ogni indirizzo Bitcoin è composto due chiavi: una *public key* e una *private key*.

Public key Da non confondere con l'indirizzo in sé, la chiave pubblica è una forma diversa dell'indirizzo. L'indirizzo è la chiave pubblica *hashata*, per questo è di dimensioni più corte. (impreciso, sistemo).

Private key La *private key* è un codice che consente a chiunque di avere accesso ai Bitcoin conservati nell'indirizzo. Come le *hash* viste in precendenza, le private keys sono numeri di 256 *bit*, che nel sistema numerico esadecimale sono codici di 64 caratteri tra numeri e lettere. Come le *hash*, esistono poco meno[18] di 2^{256} *private keys*. È paragonabile ad una password che dà accesso ad account di qualunque tipo, l'unica differenza è che non è modificabile.

Seeds Un *seed* è un codice che svolge una funzione simile a quella della *private key*: se inserito in un software di wallet, ripristina tutti i bitcoin associati ad esso. I *seeds* sono stati introdotti nel 2 febbraio 2012 con il BIP 32 [9]. Questi primi *seed* hanno un aspetto simile a quello delle *private keys*, con lunghezza variabile. La differenza con le *private keys* è che un seed "genera" una o più private keys, dalle quali si possono ricavare le public keys e quindi gli indirizzi

[16] *Bitcoin Improvement Proposal*, una proposta di un miglioramento al software del Bitcoin
[17] Vedi punto 3.3.3
[18] "Poco meno" perché esse devono rispettare i parametri dell'algoritmo ECDSA, di cui non parlerò per non andare fuori tema

stessi. Di conseguenza, ad un seed possono corrispondere un numero indefinito di indirizzi, ovvero di coppie di public e private keys. Realisticamente, quasi tutti i seed usati nei portafogli software comprendono da 1 a 20 indirizzi. Esistono diversi tipi di seed, ma il formato più famoso è quello della cosiddetta *mnemonic phrase*, una frase di 12 - 20 parole scelte a caso da un elenco di 2048 parole in lingua inglese, introdotta nel 10 settembre 2013 con il BIP-39 [10]. Il vantaggio dei *seeds* rispetto alle singole private keys è il fatto che sono facili da ricordare. Un seed ha un aspetto simile al seguente:

witch color pride feed shame open despair creek road again ice least

Il secondo vantaggio è che la presenza di molteplici indirizzi Bitcoin aiuta a tutelare la propria privacy. Come abbiamo visto nella blockchain tutte le transazioni sono visibili da chiunque, così per rendere i fondi meno tracciabili si possono usare diversi indirizzi per diverse operazioni.

3.2.3 Portafogli

Un portafoglio è il metodo usato per conservare e interagire con i Bitcoin che si possiede. I portafogli contengono le chiavi pubbliche e private e di conseguenza l'indirizzo stesso. I portafogli si dividono in *hot* e *cold* storage. I *cold wallets* sono paragonabili a un salvadanaio o a una cassaforte, mentre i *hot wallets* sono simili ai portafogli che portiamo in giro.

Cold storage Con il *cold storage*[19], *public* e *private* keys sono conservate offline, ovvero in un ambiente non collegato a internet. Sebbene sia necessaria una connessione ad internet per effettuare transazioni, riceverle non la richiede (suona male). (metto sopra?) quando creiamo un indirizzo a partire da una *private key* ricavata casualmente, questo è in realtà già esistente nella blockchain. Tutti gli indirizzi, *public* e *private* keys sono già esistenti nella blockchain a prescindere, e creando un indirizzo non stiamo facendo altro che appropriarcene di uno a caso. È naturale porsi la domanda: "Ma se qualcuno "ottenesse" la mia private key mi ruberebbe tutti i soldi! Non è rischioso?". Ebbene, come ho scritto prima, esistono X keys, un numero simile a 1/3 degli atomi in tutto l'universo. La probabilità è praticamente nulla. (riguardare, forse sbagliato e confondendo). I principali tipi di *cold storage* sono:

- Digitale: le keys sono salvate sottoforma di file su un computer, un CD, una chiavetta USB...
- Carta: si possono scrivere le keys su un pezzo di carta o stampare un *paper wallet*, metodo poco sicuro per la fragilità del materiale.
- Metallo: le keys possono essere incise su una lamina di metallo, preferibilmente oro, argento, bronzo, nickel, ottone o cobalto per la resistenza alle alte temperature.

[19] Archiviazione a freddo

- *Hardware wallet*: I portafogli hardware sono dei piccoli dispositivi simili a chiavette USB, in cui la *private key* è contenuta.

(a) Un Ledger Nano S, portafoglio hardware

(b) Un *paper wallet*

Figura 7: Due forme di *cold storage*

Esistono anche dei veri e propri "Bitcoin" fisici, ovvero delle monete materiali con incise le keys.

Hot wallets Gli *hot wallets* sono invece dei portafogli che utilizzano un collegamento a internet per permettere di effettuare pagamenti *dall'*indirizzo in uso. Esistono come software, tra cui app per smartphone, programmi per computer o servizi online. Certi *hot wallets* permettono di stabilire manualmente la tassa in sat/b

3.3 I problemi del Bitcoin

3.3.1 Gli attacchi al network

La rete del Bitcoin può essere abusata da malintenzionati per compiere *double spending*, ovvero l'atto di spendere una stessa quantità di Bitcoin due volte, effettivamente annullando il primo pagamento. Il *double spending* è solitamente usato per truffare: dopo aver inviato x BTC al ricevente, il truffatore fa subito un attacco di *double spending* inviando a sé stesso la stessa quantità di bitcoin. Il ricevente si troverà con 0 BTC, che sono rimasti al truffatore. Esistono tre principali modi per fare *double spending* [11]:

- *Race attack*: questo tipo di attacco avviene alle transazioni non ancora confermate (quindi ancora nella *mempool*). Il truffatore fa un pagamento a sé stesso con una tassa di transazione inferiore a 1 sat/b in modo da propagare la transazione ai *nodes* che accettano transazioni con una tassa molto bassa. Questi sono una minoranza, perché la maggior parte dei *full nodes* ha un limite di 1 sat/b come tassa minima. Subito dopo, il truffatore ripete la transazione al mercante, questa volta con una tassa

più elevata: i *nodes* con una maggiore tassa minima accettano la seconda transazione considerandola come l'unica avvenuta di recente, ma quelli che avevano accettato la prima la rifiutano, perché è uguale a quella accettata in precendenza. Di conseguenza, la prima transazione passa alla *mempool* senza problemi, mentre la seconda, quella fatta al mercante, non viene processata [12].

- *Finney attack*: un altro metodo di attacco che colpisce le transazioni con 0 conferme. L'attacco Finney richiede che il truffatore abbia la possibilità di fare *mining* e quindi di generare nuovi blocchi. Quando questo trova un blocco, non lo diffonde ai *full nodes* per poi includerlo nella blockchain, ma se lo tiene per sé. In questo blocco il truffatore compie una transazione a sé stesso. Subito dopo aver pagato il mercante, prima che la transazione legittima venga confermata, il truffatore "rilascia" il blocco che ha tenuto fermo, facendolo confermare prima di quello in cui è avvenuto il pagamento al mercante.

- *Majority attack*: più comumemente conosciuto come "*51%*" o "*>50% attack*", è il tipo di attacco più temuto perché può essere applicato a qualunque transazione, indipendentemente dal numero di conferme ricevute[20]. Un attacco 51% si può effettuare solo se un singolo possiede più della metà dell'*hashrate* di tutta la rete del Bitcoin. Dopo aver pagato il mercante, questo attende x conferme e poi invia la sua merce. Il truffatore sdoppia la blockchain e su questa ripete il pagamento a un indirizzo in suo controllo; in seguito impiega il 51% dell'*hashrate* per minare blocchi sul suo clone privato della blockchain, e dopo aver trovato un numero di blocchi maggiore al numero di conferme attese manda "live" la sua blockchain ai *full nodes* in tutto il mondo per sostituire quella più corta, nella quale il mercante aveva ricevuto bitcoin.

3.3.2 La parziale centralizzazione

L'intenzione di Satoshi, con la creazione della blockchain e di un sistema di *mining* universale, fu quella di creare una valuta decentralizzata, e in parte ci riuscì. Purtroppo, il lavoro dei *miners* è concentrato in un piccolo gruppo di *pools* che possiedono quasi tutta l'*hashrate* globale [13].

Non ci sono *pools* con una percentuale di *hashrate* maggiore al 50%, ma è sufficiente dirottarne 3 per compiere un attacco 51%, essendo la maggior parte situate in Cina.

[20] Ricordo che una conferma corrisponde a un blocco trovato dopo aver effettuato il pagamento. Più conferme rendono una transazione più sicura perché questa viene "superata" da un maggior numero di blocchi

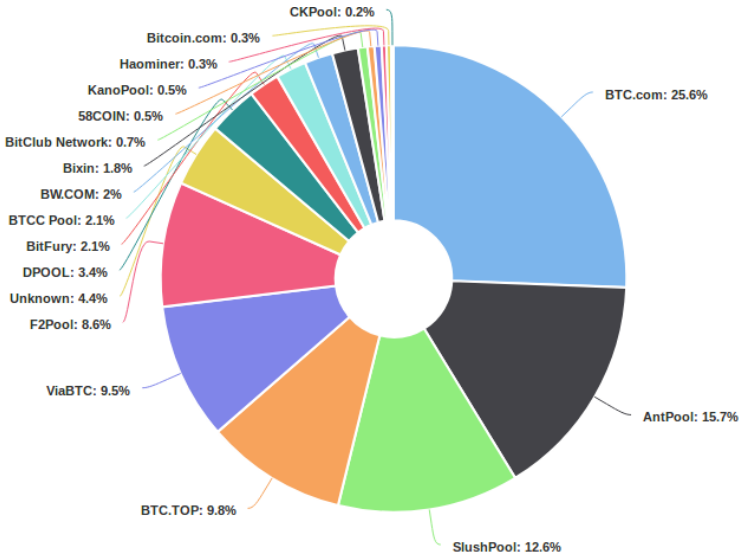

Figura 8: pie-chart della percentuale di *hashrate* controllata dalle più grandi *pools*
fonte: blockchain.info

3.3.3 Il limite dei blocchi da 1 Megabyte

Nell'inverno del 2017 l'improvviso incremento del numero di transazioni ha avuto un impatto decisamente negativo sulla tassa di transazione media. Un qualunque pagamento in Bitcoin poteva costare fino ai €25 [**highfees**]. La causa di tutto questo è il fatto che la dimensione di 1MB dei blocchi non era sufficiente per farci stare tutte le transazioni nella *mempool*. I software dei portafogli, per poter far confermare le transazioni degli utenti, hanno automaticamente aumentato il valore della tassa in sat/b per rendere la transazione effettuata preferibile ai *miners*, che la includono nel blocco in fase di ricerca. Fortunatamente, gli sviluppatori hanno elaborato due principali soluzioni per ridurre, se non eliminare, il problema delle tasse elevate.

Segregated Witness Segregated Witness (comunemente abbreviato in SegWit) è una *soft fork* del Bitcoin introdotta il 21 dicembre 2015 col BIP-141 [**bip141**]. Una *soft fork* è un aggiornamento che viene effettuato alla blockchain già esistente[21], e per far sì che si possa usufruire di questi aggiornamenti è necessario che gli utenti scarichino la versione più recente del software dell'*hot wallet* o di Bitcoin Core (nel caso si voglia operare un *full node*). Il funzionamento tecnico è altamente complesso e non ritengo indispensabile includerlo nella tesina. SegWit è una grande invenzione perché riduce il peso effettivo delle transazioni in modo da poterne includere un numero maggiore nei blocchi. Di conseguenza, SegWit aiuta indirettamente a pagare una tassa di transazione inferiore, perché

[21] A differenza delle *hard forks*, descritte al punto 5.6

essendo le transazioni più "leggere", è meno probabile che un blocco si riempia e inizi l'"asta" delle tasse per decidere le transazioni da processare.

Lightning Network Il Lightning Network è un'infrastruttura esterna alla blockchain che rende cose veloci

4 Utilizzare Bitcoin

Ho notato che nonostante se ne parli sempre di più in televisione e su internet, il Bitcoin è sempre visto come un concetto astratto, un'entità misteriosa di cui non si sa esattamente come si usa, dove si prende, e in cosa si spende. In questa sezione spiegherò come entrare in contatto con l'ecosistema delle criptovalute, partendo dalla creazione di un portafoglio (*hot* e non *cold* per avere la possibilità di effettuare pagamenti).

4.1 Creazione del portafoglio

Per comodità è consigliabile usare un app per smartphone: sull'App Store dei dispositivi Apple e sul Play Store di quelli Android sono disponibili numerosi portafogli di Bitcoin, ma il funzionamento è lo stesso per tutti. Una volta scaricato il portafoglio incomincia la creazione di un nuovo indirizzo che verrà usato per inviare e ricevere bitcoin. L'app ci mostrerà il *seed* al quale sono associati i nostri indirizzi (ma talvolta solo uno). Il seed dovrà essere copiato e conservato in un luogo sicuro (su carta e/o chiavetta USB), perché nello sfortunato caso in cui perdiamo il nostro smartphone sarà possibile importarlo in un altro dispositivo. Una volta confermato il seed saremo in grado di inviare e ricevere Bitcoin al nostro indirizzo.

4.2 Come ottenere Bitcoin

Exchange Il metodo più veloce e utilizzato è quello di acquistarlo su un sito di *exchange*[22]. Esistono moltissimi siti che permettono di acquistare Bitcoin con bonifico bancario o semplicemente con una carta di credito. Coinbase è di gran lunga l'exchange più famosa del mondo, ma ne esistono una moltitudine. Basta aprire un account, collegare il proprio conto o la carta di credito, verificare la propria identità con passaporto o carta d'identità e compare bitcoin è questione di secondi. Una volta acquistato, è consigliabile spostare i propri bitcoin su un portafoglio indipendente da quello dell'exchange. Quasi tutte le exchange più reputabili sono dotate di sistemi di sicurezza ad elevatissimo livello che riducono la possibilità di una violazione della sicurezza al minimo, ma ci sono stati tragici episodi di exchange colpite da attacchi hacker, derubate di quantità di bitcoin che oggi valgono milioni di Euro. Ritengo che non valga la pena di rischiare di perdere tutti i propri bitcoin per la pigrizia di non volerli mettere al sicuro.

ATMs Esistono dei veri e propri "Bancomat" in cui anzichè prelevare soldi dal proprio conto bancario è possibile acquistare e vendere criptovalute. Sono comodi, veloci ed anonimi, ma c'è sempre il rischio di venire derubati tramite forza fisica; si paga un bonus per la comodità e al giorno d'oggi sono ancora molto poco diffuse. Si può trovare una mappa online con la posizione di questi ATM in tutto il mondo su coinatmradar.com.

[22] "Scambio", siti di compravendita di valute

Mining Come spiegato in precedenza, il processo di *mining* porta i *miners* a guadagnare Bitcoin, che possono essere venduti sulle exchange per soldi veri e propri. Ovvio che per una persona inesperta il *mining* è fuori portata, ma è certamente un modo valido per ottenere Bitcoin.

Forma di pagamento Al posto di soldi in contanti o carta di credito è possibile accettare Bitcoin come forma di pagamento per merce o servizi offerti in vita reale e online. Esistono infatti diversi sistemi automatizzati che consentono ai mercanti di accettare criptovalute velocemente e in sicurezza. Coinbase Commerce, per esempio, si integra con i siti web mostrando un'interfaccia di pagamento che permette di scegliere la criptovaluta con cui pagare e l'indirizzo verso cui pagare. Il pagamento è concluso solo quando Coinbase riceve il pagamento della quota, che reindirizza al portafoglio del mercante

4.3 Trasferire Bitcoin

Un tipico trasferimento da persona a persona avviene con gli smartphone. Il ricevente va nella sezione "ricevi" della propria app, che gli mostrerà un codice QR che decifrato corrisponde all'indirizzo di pagamento. Il pagatore va nella sezione "paga", e tramite la fotocamera del proprio telefono scansiona il codice QR del ricevente. Una volta scansionato, l'app del pagatore chiederà la quantità di bitcoin da inviare. Una volta stabilito, il pagamento avverrà e il ricevente rieceve si dai. Per i pagamenti online è possibile anche utilizzare un computer. Il processo è lo stesso, l'unica differenza è che anziché scansionare un codice QR, colui o colei che effettua il pagamento dovrà semplicemente copiare e incollare l'indirizzo nel campo di pagamento del portafoglio.

5 Non solo Bitcoin

Esistono numerosissime criptovalute. Il sito coinmarketcap.com ne lista ben 1640. Ritengo indispensabile spendere almeno qualche pagina per parlare delle valute più rilevanti, perchè una diffusa convinzione, per quanto falsa, è che il Bitcoin è l'unica criptovaluta. Tutte le criptovalute che non sono Bitcoin prendono il nome di "altcoin" (*alternative coin*).

5.1 Ethereum

Ethereum (ETH) è una valuta ideata nel 2013 da Vitalik Buterin e lanciata nel 2014. Il *whitepaper* stabilisce un tempo di blocco pari a 12 secondi, che per motivi tecnici è effettivamente intorno ai 15-17 secondi. È stato scelto un tempo così inferiore rispetto ai 10 minuti del Bitcoin perché oggi la maggioranza del mondo utilizza una connessione a internet abbastanza veloce da poter diffondere i blocchi ai *full nodes* con rapidità. Inoltre, a seguito di un miglioramento del software della blockchain, con l'utilizzo di nuove tecnologie si riducono al minimo i blocchi orfani trovati, nonostante un tempo di blocco così breve. Non esiste un limite massimo di ETH che possono esistere, tuttavia Vitalik ha proposto di mettere un limite a 120.204.432 ETH per evitare un'inflazione della valuta.

Smart contracts L'idea di *smart contract*[23] è nata nel 1996 dallo scienziato Nick Szabo quando questi fece l'esempio più semplice di *smart contract*: il distributore di merendine [14]. Inserendo dei soldi nella macchina, questa compie dei calcoli per stabilire se abbiamo inserito abbastanza denaro, se deve dare del resto e quanto, e infine ci dà il prodotto richiesto. Nel caso di Ethereum, gli *smart contracts* sono programmi che svolgono determinate funzioni in base a quanto Ethereum viene dato loro. Questo permette la creazione delle cosiddette "dapps", *decentralized applications*, siti web che offrono automaticamente servizi in cambio di Ethereum.

Mining In precedenza mi sono concentrato sul processo di *mining* del Bitcoin, ma come quasi tutte le criptovalute anche Ethereum funziona grazie al *mining*. La principale differenza tra il *mining* di Bitcoin e di Ethereum è che Ethereum non richiede gli ASIC, ma si può effettuare con l'uso di schede grafiche per computer. Questo perché il *mining* di Ethereum non utilizza l'algoritmo SHA-256 come il Bitcoin, bensì l'algoritmo Ethash[24]. La più grande differenza tra i due algoritmi è che Ethash richiede una quantità di RAM[25] ben maggiore di quella dei *miner* ASIC. Le schede grafiche dei computer desktop, comunemente chiamate GPU[26], grazie alla maggior quantità di RAM (superiore a 4GB nella maggior parte delle schede moderne), sono effettivamente l'unico mezzo

[23] Contratti intelligenti

[24] Chiamato in passato Dagger-Hashimoto perché include delle caratteristiche presenti in questi due algoritmi

[25] *Random Access Memory, memoria ad accesso casuale*

[26] *Graphics Processing Unit*

in grado di cercare e trovare i blocchi di Ethereum. In questo modo Vitalik ha impedito agli ASIC di minare Ethereum, rendendo il lavoro possibile esclusivamente alle GPU. Ma perché? I *miner* ASIC sono apparecchiature costose ed estremamente potenti, presenti in quantità limitata perché concentrate in enormi *farm* e sottomesse al monopolio delle *pools* cinesi. Questi due fattori sono grandi minacce per la decentralizzazione della valuta. Le schede grafiche sono presenti in quasi tutti i computer di fascia medio-alta, e il prezzo di una GPU è normalmente intorno ai €200 - €400. Questo rende Ethereum potenzialmente "minabile" da una grandissima quantità di persone, e ciò impedisce la centralizzazione dell'*hashing power*, riducendo la possibilità di attacchi 51%.

La deflazione del mercato di schede grafiche Il boom del *mining* di Ethereum, come quello del prezzo di tutte le criptovalute, avvenne nell'estate del 2017. Sempre più persone si resero conto della possibilità di poter guadagnare soldi veri facendo lavorare delle schede grafiche (come?), così gli interessati cominciarono ad acquistarne. Certi *miners* di Ethereum, però, acquistarono schede grafiche in quantità colossali per creare delle *farm*, con centinaia, se non migliaia di GPU ciascuna.

Figura 9: Una *farm* di Ethereum con 1440 schede grafiche

Si verificò una vera e propria crisi nel mercato delle schede grafiche: i negozi erano quasi sempre vuoti, e appena arrivava un nuovo carico di GPU queste venivano istantaneamente acquistate. Ovviamente i mercanti videro questa come un'opportunità per aumentare i profitti sulla loro merce, e così aumentarono

esponenzialmente i prezzi di tutti i modelli di schede grafiche. Per esempio le AMD RX 580 8GB con MSRP[27] pari a €159 raggiunsero prezzi ben oltre €300 [15]. Questa inflazione è in corso tutt'oggi.

5.2 Litecoin

Litecoin (LTC) è una criptovaluta creata nell'ottobre del 2011 dallo sviluppatore Charles Lee, comunemente chiamato Charlie Lee. L'obiettivo di questa valuta è quello di relazionarsi al Bitcoin come l'argento fa con l'oro. Come per questi metalli, infatti, l'oro è usato come uno *store of value*[28], essendo un metallo prezioso con elevato valore (oggi circa €42 per grammo [16]). L'argento è un metallo più comune con valore ben inferiore all'oro (oggi circa €16 per grammo [17]), usato anche dalle industrie. Lo stesso vale per Bitcoin e Litecoin. Come abbiamo visto in precedenza la quantità totale di bitcoin è limitata a 21.000.000 BTC, e il valore attuale per bitcoin è di circa €7000. Di litecoin invece ne possono esistere ben 84.000.000, e il prezzo per LTC è di €100. Il tempo stabilito per trovare un nuovo blocco è di 2.5 minuti anziché 10, rendendo le transazioni notevolmente più veloci. Per bilanciare la maggior quantità di litecoin che possono esistere, l'*halving* avviene ogni 840.000 blocchi anziché ogni 210.000 [18].

5.3 Monero

Monero (XMR) è un altcoin creato in aprile 2014 che ha come prima preoccupazione quella della privacy. Monero è l'unica criptovaluta che è completamente intracciabile. Come abbiamo visto con il Bitcoin, nella blockchain possiamo trovare informazioni su tutto quello che avviene: il bilancio di qualunque indirizzo, chi manda quanto a chi. Con Monero tutto questo non è possibile. Mentre ha una blockchain come tutte le altre criptovalute, non è possibile vedere le transazioni che avvengono dall'uno all'altro indirizzo, e non è nemmeno possibile visualizzare il saldo.

Questo rende Monero una valuta estremamente utile a chiunque voglia nascondere i propri fondi. Purtroppo, come tutte le tecnologie a favore della privacy, Monero può essere utilizzato anche da evasori delle tasse, truffatori e da venditori di merce illegale. Monero ha un tempo stabilito di scoperta blocchi di 2 minuti, rendendo le transazioni relativamente veloci. Inizialmente il tempo per trovare il blocco successivo era di 1 minuto, ma poi è stato aumentato a 2 minuti per ridurre la quantità di blocchi orfani e perché i blocchi non venivano sufficientemente "riempiti" di transazioni. Le transazioni di Monero, per essere anonime, hanno un peso in kb notevole, per questo le tasse di transazione sono più elevate di quelle della maggior parte delle altre criptovalute.

[27] *Manufacturer's Suggested Retail Price*, il prezzo di un oggetto consigliato dal manufattore
[28] Riserva di valore

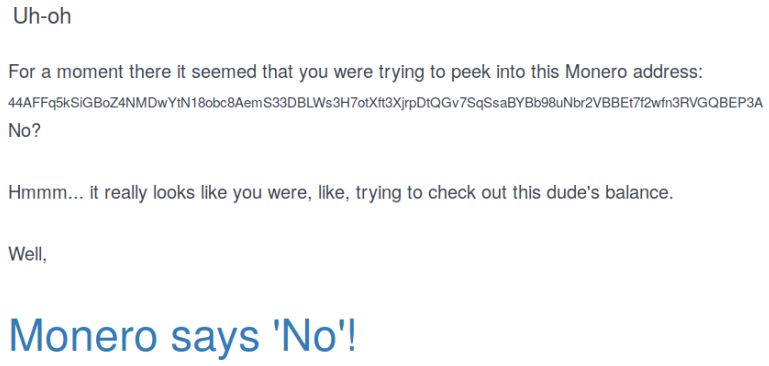

Figura 10: Sul sito moneroblocks.info viene mostrato il seguente messaggio se si cercano informazioni legate a un indirizzo

5.4 Nano

Inizialmente chiamata RaiBlocks[29], Nano è una criptovaluta creata nel 2015 da Colin LeMahieu. Nano non prevede l'impiego di *miners* per validare le proprie transazioni [**nanofaq**]. Esistono in totale 133.248.290 NANO, distribuiti gratuitamente fino all'ottobre 2017 tramite un sito che inviava una piccola quantità di Nano a chiunque completasse un *captcha*, una parola da trascrivere in una casella di testo per confermare di non essere un robot programmato per abusare del sistema di distribuzione gratuita. È veramente interessante sotto il punto di vista tecnico perché è la prima che usa la tecnologia *Block Lattice*[30] in sostanza, anziché dipendere da una singola blockchain come fanno tutte le altre valute, ogni singolo indirizzo *è* una blockchain a sé stante. Questa tecnologia permette di effettuare transazioni estremamente veloci rispetto a quelle del Bitcoin (che impiegano un'ora per essere ritenute pienamente concluse), con una durata inferiore ai 2 secondi, talvolta letteralmente istantanee. Non è l'unico vantaggio. A differenzaaa La *Block Lattice* rende tutte le transazioni di Nano completamente gratuite.

5.5 Ripple

Ripple (XRP) è un altcoin creato nel 2012 dalla Ripple Foundation. La sua particolarità sta nel fatto che Ripple mira ad essere una valuta fortemente legata all'ambito bancario, utilizzata come un bene digitale per compiere scambi di valore tra banche [**whatsripple**]. La principale critica a Ripple è quella di non essere decentralizzato come la stragrande maggioranza delle criptovalute, bensì la Ripple Foundation ha una forte influenza sull'andamento della valuta. Ripple è un coin *premined*, che non è generato tramite *mining*, infatti per entrarne in possesso è solamente possibile acquistarne direttamente dalla Foundation.

[29] il passaggio da RaiBlocks a Nano è avvenuto il 31 gennaio 2018
[30] Da non confondere con la parola italiana, *lattice [/'let.is/]* significa reticolo, intreccio

Per questo, la Ripple Foundation possiede oltre il 50% di tutti i ripple, circa 50.000.000.000 XRP [19]. Questo le permette di modificare artificialmente il prezzo.

5.6 Bitcoin "hard forks"

La blockchain del Bitcoin "originale" può essere clonata indefinitamente. Chiunque può prendere il codice sorgente del Bitcoin, applicarci qualche modifica e mandarlo "live", rendendo disponibili dei wallet al download e impiegando qualche *miner* per processare le transazioni del "nuovo" bitcoin.

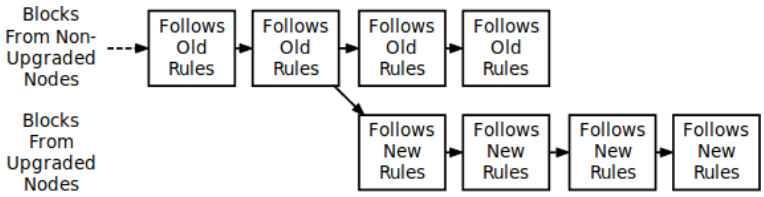

Figura 11: Schema di un'*hard fork*: I *full nodes* non aggiornati ignorano le nuove regole, dividendo in due la blockchain *(fonte: investopedia.com)*

Tecnicamente Litecoin è una *hard fork* del Bitcoin, ma ho deciso di dedicarle un paragrafo a sé stante perché, a differenza delle altre di cui parlerò in seguito, Litecoin introduce numerose differenze e il nome non include la parola "Bitcoin". Oggi esistono più di 30 *fork* del Bitcoin: Bitcoin Gold, Bitcoin Candy, Bitcoin Private, Bitcoin Unlimited, Bitcoin Super... Persino Bitcoin Pizza e Bitcoin God. Quasi tutti i fork vengono visti come delle truffe, come valute che non possiedono nulla di nuovo rispetto all'originale Bitcoin, ma viene sempre data attenzione perché chiunque possiede Bitcoin il momento in cui la blockchain è stata clonata, entra automaticamente in possesso del coin della fork. Se un indirizzo ha il bilancio di x BTC *prima* che venga lanciata la *hard fork*, per esempio Bitcoin Top (BTT) a quell'indirizzo sarà anche associato x BTT. Per poter ottenere effettivamente tutti i coin che l'indirizzo "possiede", è necessario scaricare il software di wallet del coin di fork e inserire la private key dell'indirizzo con su il coin di fork. Verrà generato un nuovo indirizzo completamente diverso, però con il bilancio di x BTT. Abbiamo visto prima che la private key dà accesso a tutti i fondi presenti sull'indirizzo a chiunque ne entri in possesso, eppure per ottenere i Fork siamo costretti ad inserirla in un software sconosciuto (perchè quasi tutti i fork non hanno alcuna reputazione: saltano fuori con siti web senza preavviso). Per evitare che un qualche malintenzionato sfrutti la sbadataggine dell'utente e rubi tutti i suoi bitcoin, è bene che I fondi vengano mossi a un altro indirizzo. Infatti, sarà comunque possibile prelevare i BTT dal vecchio indirizzo BTC ora svuotato, e non si ha nulla da perdere nel caso qualcuno riuscisse a rubare la private key: all'indirizzo sono associati 0 BTC.

6 Crypto oggi

In questa sezione andrò a parlare dell'impatto del Bitcoin nella società di oggi.

6.1 Adozione

Il Bitcoin è una valuta relativamente nuova nata neanche 10 anni fa, e il fatto che utilizza una tecnologia sconosiuta prima d'ora, limita l'adozione da parte di mercanti e imprese. Nonostante ciò, sempre più servizi stanno cominciando ad accettare criptovalute come forma di pagamento, tra cui:

- Immobiliare: in varie parti del mondo si stanno vendendo ville e appartamenti. A Dubai, per esempio, sono stati venduti 50 appartamenti di lusso per Bitcoin[20].
- Microsoft: è possibile acquistare software e giochi sul Microsoft Store con Bitcoin [21].
- Gyft e eGifter: è possibile comprare codici regalo per una moltitudine di siti che non accettano Bitcoin tra cui Amazon, iTunes, Nike, eBay e Starbucks [21].
- KFC Canada e Subway: due catene fast-food famose in tutto il mondo stanno incominciando ad accettare Bitcoin [21].

Questi sono i

Rovereto: quasi tutti accettano Bitcoin Rovereto è una cittadina nelle Dolomiti di 40.000 abitanti in cui l'uso del Bitcoin come forma di pagamento è estremamente diffusa. Tutto ebbe inizio quando ... ... [22]

Elizavetovka: il villaggio in Ucraina in cui tutti utilizzano criptovalute è bellus [23]

6.2 La bolla del 2017: cause e conseguenze

A partire dal settembre 2017 il prezzo del Bitcoin ha subito un'esponenziale crescita, passando dai €3000 del 16 settembre fino a raggiungere un picco di €17.230 il 12 dicembre. Le cose(?) che hanno causato questo boom non sono certe, ma Il prezzo del Bitcoin, ma anche della stragrande maggioranza delle altre criptovalute è precipitato nel dicembre del 2017, andando dall'ATH (*all time high*) del 12 dicembre di €17.230 ai €6000 del 5 Febbraio 2018. Un calo di più del 65%! futures?

6.2.1 L'analogia con la crisi del '29

Il 24 ottobre del 1929 è il giorno che marcò il crollo della Borsa di Wall Street, che ebbe come conseguenza il fallimento di molte imprese, una riduzione della domanda da parte di altri stati, e una forte crescita della disoccupazione, raggiungendo i 13 milioni di disoccupati nel 1932. Tra le principali cause di questa crisi ci sono la sovrapproduzione di merce. detto così sembra fatto da un bambino delle elementari Gli Stati Uniti erano grandi fornitori di merce e dané all'Europa, e il progressivo aumento della domanda ha portato gli USA ad incrementare la produzione industriale, grazie anche alla diffusione del Taylorismo e della generale innovazione tecnologica(). A partire dal 1926, però, l'Europa e poi il Giappone ridussero notevolmente la domanda agli Stati Uniti perché anche questi beneficiarono del progresso tecnologico che ha avuto inizio in America. Questo portò a un'eccessiva produzione di merce che non venne mai venduta all'Europa perché non richiesta. Un'altra enorme causa di questa crisi fu l'andamento dell'economia mondiale: era puramente un'economia di carta, basata su opinioni e speculazioni. Gli scambi di azioni e gli investimenti di imprenditori verso le diverse aziende era una scommessa su quale attività avrebbe fatto successo, facendo ricavare profitti a chi avesse investito. [24] Questo è estremamente simile a quello che è successo al Bitcoin perché sì.

La ricorrenza dei "crash" dei mercati

6.3 Controversie

Il Bitcoin e le criptovalute in generale sono frequentemente soggetto di controversie. La nuova tecnologia della blockchain è criticata da molti imprenditori, e numerosissime truffe girano intorno alla parziale anonimità della valuta [25].

6.3.1 Moneta per scambi illegali

Inizialmente il Bitcoin, ma oggi anche altre criptovalute (speciamente quelle centrate sulla privacy), sono usate per compiere scambi di merce proibita, principalmente droga e armi. Nel dark web, infatti, esistono numerosi siti dove è possibile acquistare merce illegale tramite criptovalute. Fino al 2013, nei primi anni del Bitcoin, infatti, la valuta era quasi esclusivamente utilizzata per fare acquisti sul *marketplace* chiamato Silk Road[31], chiuso dall'FBI nell'ottobre del 2013. L'accusa alle criptovalute di essere monete "da mercato nero" è secondo molti una forma di FUD, *fear, uncertainty, doubt*[32], per il semplice fatto che la moneta cartacea, il *cash* è anch'essa una forma di denaro da sempre usata per atti/motivi illeciti, anch'essa anonima, più del Bitcoin!

[31] Strada di seta

[32] Paura, incertezza, dubbio: tecnica per incutere timore nella gente inesperta riguardo a qualcosa

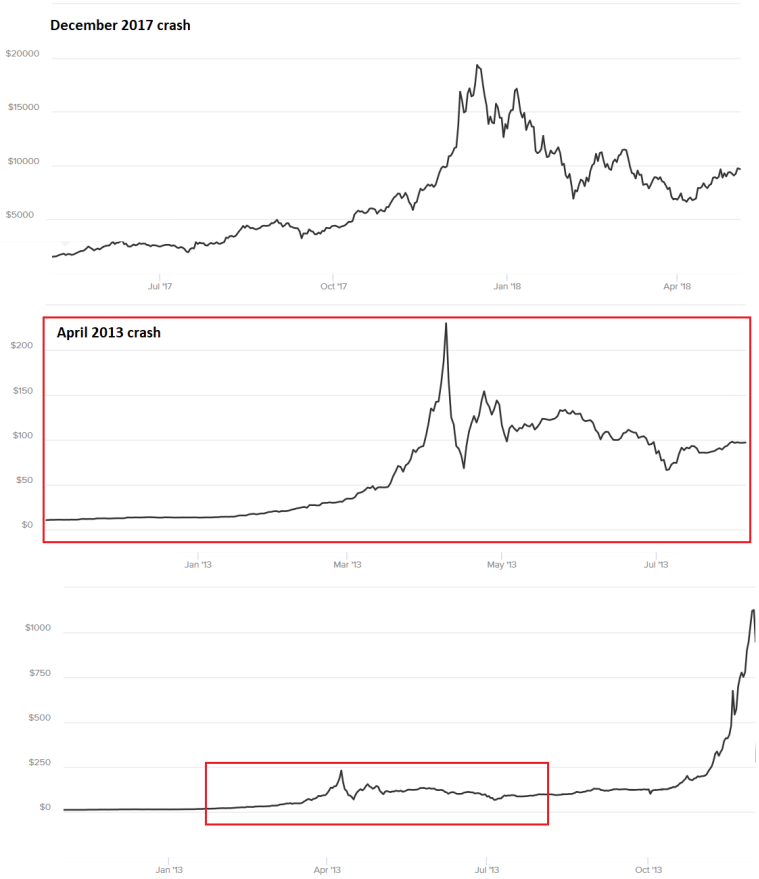

Figura 12: Confronto tra il crollo del prezzo del Bitcoin nel 2013 e nel 2017
fonte: coinmarketcap.com

6.3.2 Il ban del Bitcoin in certi stati

boh, faccio dopo.

6.3.3 Mt. Gox

Mt. Gox[33] è il primo grande sito di *exchange* di Bitcoin, creato da Jeb McCaleb nel 18 luglio 2010. Il dominio mtgox.com è stato poi venduto allo sviluppatore francese Mark Karpelès nel marzo del 2011; la sede è stata spostata dall'America al Giappone. Fin da subito l'*exchange* ha avuto gravi problemi di sicurezza, infatti il 19 giugno 2011 un hacker è riuscito a rubare una grande quantità di bitcoin. Nel settembre del 2011 un hacker entrò in possesso delle *private keys*

[33] "Mt." è *mount* in inglese, "monte"

del portafoglio dell'*exchange*, e rubò una quantità di circa 630.000 BTC[34] fino al 7 febbraio 2014, quando Mt. Gox annunciò una "temporanea sospensione" degli scambi a causa di un *bug* nel loro software. Gli amministratori di Mt. Gox non si accorsero del trasferimento dei bitcoin da parte dell'hacker. Questo causò un enorme divario tra la quantità di bitcoin effettiva e quella prevista da Mt. Gox:

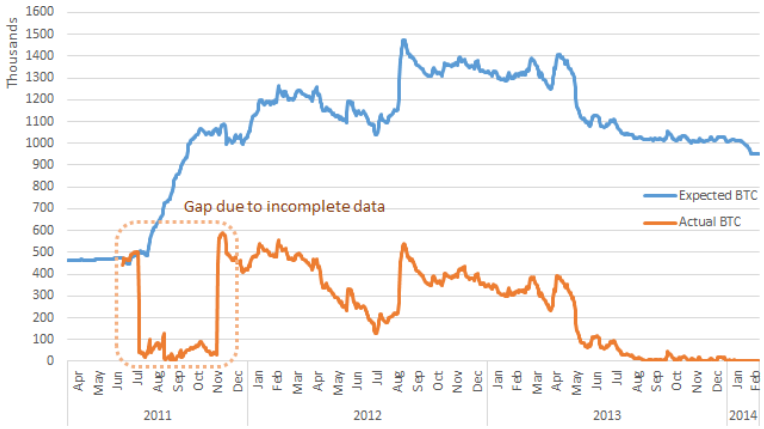

Figura 13: Confronto tra i bitcoin effettivamente posseduti da Mt. Gox e quelli creduti
fonte: wizsec.jp

Intorno alla fine del 2013 due utenti chiamati "Willy" e "Markus" effettuarono una grande quantità di acquisti di bitcoin su Mt. Gox, con una frequenza di 5-10 BTC ogni 5-10 minuti, per un totale di oltre 250.000 BTC in pochi mesi. Il fatto che l'utente facesse ordini di acquisto anche in periodi in cui il sito non era funzionante indicò che Willy e Markus non erano altro che *bot*, dei computer con il compito di incrementare artificialmente il prezzo del Bitcoin. Il 24 febbraio 2014 Mt. Gox annunciò la perdita di 850.000 BTC, di cui 750.000 posseduti dai loro utenti, anche se il 20 marzo sono stati poi trovati 200.000 BTC in un vecchio portafoglio, rendendo il numero effettivo di bitcoin persi ~650.000. L'1 agosto 2015 Mark Karpèles venne arrestato dalle autorità di Tokyo, accusato di aver falsificato i dati del prezzo del Bitcoin e del volume di liquidità di Mt. Gox. L'11 luglio 2017, il giorno del processo, venne scoperto che i due *bot* erano infatti operati dallo stesso CEO Mark Karpèles [26]. L'hacker responsabile del furto dei 630.000 BTC, Alexander Vinnik, è stato arrestato dalle autorità americane in Grecia il 26 luglio 2017, e BTC-e, un'*exchange* russa, è stata sequestrata (ma non chiusa) dall'FBI a partire dal 25 luglio 2017, accusata di aver assistito Vinnik nel nascondere 300.000 bitcoin rubati [27].

[34] Oggi valgono €4.410.000.000

6.3.4 Bitconnect

Bitconnect è un altcoin con un tasso di interesse variabile (dal 0.1% all'1%) che aumentava quotidianamente i profitti di chiunque ne possedesse. Non era ben chiaro chi fosse il creatore, e molti erano già dubiosi del claim di arricchire magicamente chiunque ne comprasse. Tra il 14 e il 17 Gennaio 2018 il prezzo di Bitconnect è crollato da €273 a €30, arrivando agli €0.55 di oggi. Si è scoperto che l'intero progetto Bitconnect non era altro che un' "exit scam", una truffa in cui i truffatori spariscono improvvisamente, lasciando gli investitori a mani vuote. In particolare Bitconenct è stato uno schema Ponzi, un tipo di truffa in cui il truffatore promette guadagni a chiunque si indebitasse con lui, per poi sparire. Il nome Ponzi deriva da Charles Ponzi, un italo-americano che si arricchì notevolmente tra il 1918 e il 1920 compiendo ripetutamente questo tipo di truffa. Oggi tutti coloro coinvolti nel pubblicizzare Bitconnect, soprattutto chi pubblicava video su YouTube che incitavano all'acquisto della valuta, sono sotto investigazione.

6.3.5 Roger Ver e la truffa di "Bitcoin Cash"

Bitcoin Cash è di gran lunga l'hard fork più popolare di tutte, al quarto posto (!) in capitalizzazione di mercato. Come mai è l'unica che ha raggiunto un prezzo così elevato? Roger K. Ver è un imprenditore americano che fin dai primi anni della nascita del Bitcoin è stato coinvolto nella scena delle criptovalute. Dall'agosto del 2017, però, quando è stato lanciato Bitcoin Cash, Roger è stato l'esponente principale per il marketing di questa valuta. BCH è nato in Cina, infatti i suoi CEO sono cinesi, e Roger dev'essere stato impiegato per fare propaganda a BCH. Tutto ciò non sembra alcunché di preoccupante: è normale se un imprenditore pubblicizza i propri investimenti sperando di ricavare più guadagni, (nel caso che...) ed è normale che sviluppatori paghnio uno abile a parlare e a pubblcizzare un prodotto. è così che funziona il marketing. Quella di Roger, però, è una spietata propaganda anti-Bitcoin (BTC) e pro-BCH (Bitcoin Cash), che spesso e volentieri arriva alla censura, alle bugie più false e alla corruzione di persone. La tesi base che accomuna Roger e tutti i fan di Bitcoin Cash è quella che BCH introduce delle modifiche al codice di Bitcoin che aumentano la dimensione dei blocchi, che anzichè limitarsi a 1MB arrivano fino a 12MB. Questo riduce esponenzialmente la probabilità che i blocchi vengano riempiti di transazioni, innalzando le tasse a livelli esorbitanti[35]. Il team di sviluppatori di Bitcoin si ostina a mantenere la dimensione del blocco a 1MB, perchè i blocchi di maggiore dimensioni sono *ancora* più difficili da minare. Una difficoltà così elevata di *mining* porta necessariamente a una centralizzazione dell'*hashing power*, che va contro il concetto di Bitcoin e di criptovalute in generale. inoltre, ... [28] Roger è entrato in possesso del sito bitcoin.com, che su numerose pagine (tra cui quella in fig. 5) ripete come BCH è una versione aggiornata di BTC. Una cosa che irrita la stragrande maggioranza delle persone è il fatto che su bitcoin.com il Bitcoin originale, BTC, è chiamato Bitcoin Core.

[35] Vedi punto 3.3.3

Il nome Bitcoin Core, paragonato a Bitcoin Cash, fa sembrare le due valute due alternative sullo stesso livello, invece uno (BCH) è un clone dell'originale (BTC). In Aprile del 2018 bitcoin.com penalizzò ulteriormente la situazione del "vero" Bitcoin definendo "BTC" "Bitcoin Core" e "BCH" (che sarebbe Bitcoin Cash) "Bitcoin". Questa mossa fu la goccia che fece traboccare il vaso, perché mentre il fatto di chiamare BTC Bitcoin Core era già una bugia di per sé, sostituire "Bitcoin Cash" con "Bitcoin" era semplicemente inaccettabile. A seguito di questa modifica dei termini, bitcoin.com venne denunciato da oltre 1000 persone e fu eventualmente costretto a tornare alle vecchie denominazioni delle valute che, purché volontariamente misleading, non facevano apparire BCH come il "vero" Bitcoin [29]. bitcoin.com, essendo il secondo risultato su Google per la ricerca "bitcoin", ha portato molte persone nuove nel mondo delle criptovalute che cercavano di acquistare dei Bitcoin ad acquistare BCH anziché BTC. Ver possiede anche l'account Twitter @bitcoin, che svolge le stesse opere di propaganda di bitcoin.com.

6.4 Il futuro delle criptovalute

Molti ritengono che quella del Bitcoin sia solo una moda passeggera, simile a quella dei film in 3D e Google Glass, che ha avuto il suo picco nell'inverno del 2017 e che è destinato a sparire. Personalmente sono ottimista nello sviluppo delle criptovalute. Osservando l'andamento dei grafici, pur avendo subito gravi crolli in brevi intervalli di tempo, il prezzo delle valute è in una regolare crescita. Il fatto che se ne parli sempre più nei media (i media parlino piu), sebbene spesso in negativo, rende la gente comune consapevole dell'esistenza di questa tecnologia, e fra tanti che la ignorano sono sicuro che qualcuno come me si interessi. La natura deflazionaria della valuta aiuta sicuramente il prezzo: abbiamo visto che non possono esistere più di 21 milioni di bitcoin, e ciò rende un'inflazione del prezzo tecnicamente impossibile. paragone all'inizio btcoro? Tutte le inflazioni sono dovute a un'eccessiva stampa di soldi cartacei, cosa che è impossibile nell'ambito delle criptovalute. Un altro fattore concreto che indica un futuro promettente per il Bitcoin è il numero di transazioni giornaliere:

Indipendentemente dal motivo per cui queste transazioni sono state effettuate, è logico pensare che un aumento così progressivo nell'uso del Bitcoin sia una cosa bella :D

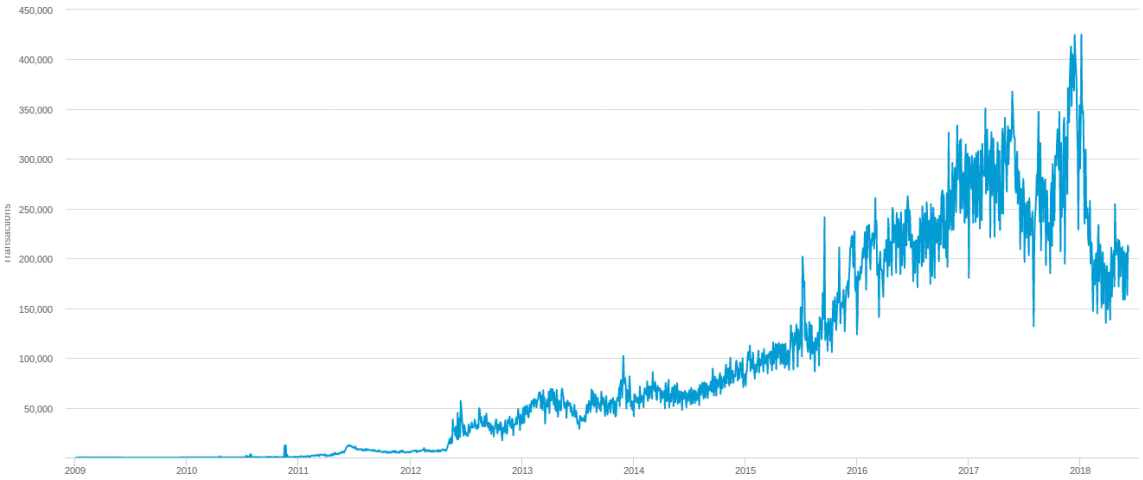

Figura 14: Transazioni giornaliere a partire dal 2009
fonte: blockchain.info

Riferimenti bibliografici

[1] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: *bitcoin.org* (31 ott. 2008). URL: https://bitcoin.org/bitcoin.pdf.

[2] Pieter Wuille. In: *Bitcoin StackExchange* (2015). URL: https://bitcoin.stackexchange.com/questions/5859/what-are-orphaned-and-stale-blocks.

[3] URL: https://shop.bitmain.com/antminer_s9_asic_bitcoin_miner.htm?flag=specifications.

[4] URL: https://shop.bitmain.com/product/detail?pid=00020180205101615915Og4OS2hk0661.

[5] URL: https://www.asicminervalue.com/miners/bitmain/antminer-s9-14th.

[6] "Average electricity prices around the world: $/kWh". In: *OVOEnergy.com* (). URL: https://www.ovoenergy.com/guides/energy-guides/average-electricity-prices-kwh.html.

[7] Shangfeng Han et al. "China's Energy Transition in the Power and Transport Sectors from a Substitution Perspective". In: *Energies* (29 apr. 2017). URL: mdpi.com/1996-1073/10/5/600/pdf.

[8] URL: https://yearbook.enerdata.net/electricity/electricity-domestic-consumption-data.html.

[9] Pieter Wuille. "Hierarchical Deterministic Wallets". In: *Bitcoin Improvement Proposals* (11 feb. 2017). URL: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki.

[10] Marek Palatinus et al. “Mnemonic code for generating deterministic keys”. In: *Bitcoin Improvement Proposals* (10 set. 2013). URL: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki.

[11] “Irreversible Transactions”. In: *Bitcoin Wiki* (2017). URL: https://en.bitcoin.it/wiki/Irreversible_Transactions.

[12] Jason Chayannes. “Double Spending a 0-Conf Bitcoin Transaction”. In: *Jason C. Blog* (2 apr. 2018). URL: https://jasonc.me/blog/bitcoin-double-spend#.

[13] Egor Homakov. “Stop. Calling. Bitcoin. Decentralized.” In: *Medium.com* (2017). URL: https://medium.com/@homakov/stop-calling-bitcoin-decentralized-cb703d69dc27.

[14] Nick Szabo. *Formalizing and Securing Relationships on Public Networks*. Rapp. tecn. 1997. Cap. The Idea of Smart Contracts. URL: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.

[15] CustardFilled. “Video card prices and Cryptocurrency mining - what’s going on?” In: *BuildAPC subreddit* (giu. 2017). URL: https://www.reddit.com/r/buildapc/comments/6jl60i/video_card_prices_and_cryptocurrency_mining_whats/.

[16] URL: https://silverprice.org.

[17] URL: https://goldprice.org.

[18] “What is the Difference Between Litecoin and Bitcoin?” In: (2014). URL: https://coindesk.com/information/comparing-litecoin-bitcoin/.

[19] URL: https://ripple.com/xrp/market-performance/.

[20] Oscar Williams-Grut. “50 luxury flats in Dubai have been sold for bitcoin — and one buyer bought 10”. In: *Business Insider UK* (10 feb. 2018). URL: http://uk.businessinsider.com/50-dubai-luxury-flats-sold-for-bitcoin-and-one-buyer-bought-10-2018-2?IR=T.

[21] Jonas Chokun. “Who Accepts Bitcoins As Payment? List of Companies, Stores, Shops”. In: *99Bitcoins.com* (15 mar. 2018). URL: https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/.

[22] Luca Pianesi. “A Rovereto nella Bitcoin Valley, dove puoi comprare tutto con la criptovaluta e dei dipendenti si fanno già pagare l’intero stipendio così”. In: *Il Dolomiti* (10 mar. 2017). URL: http://ildolomiti.it/societa/rovereto-nella-bitcoin-valley-dove-puoi-comprare-tutto-con-la-criptovaluta-e-dei-dipendenti.

[23] Sharat Chandra. “A Ukranian Village Where Everyone Owns Cryptocurrency”. In: *BCFocus* (5 mag. 2018). URL: https://bcfocus.com/news/latest-news-news/a-ukranian-village-where-everyone-owns-cryptocurrency/7977/.

[24] Alberto De Bernardi e Scipione Guarracino. “La Grande depressione”. In: *La realtà del passato 3: il novecento e il mondo attuale*. A cura di Bruno Mondadori. 2014. Cap. 7, p. 561.

[25] “Why is Bitcoin so controversial?” In: *Unocoin Blog* (17 ott. 2017). URL: https://blog.unocoin.com/why-is-bitcoin-so-controversial-527caf8ee4c7.

[26] William Suberg. “Mt. Gox Trial Update: Karpeles Admits ‘Willy Bot’ Existence”. In: *Cointelegraph* (11 lug. 2017). URL: https://cointelegraph.com/news/mt-gox-trial-update-karpeles-admits-willy-bot-existence.

[27] Liesl Eichholz. “MtGox, BTC-e, and the Missing Coins: A living timeline of the greatest cyber crime ever”. In: *Brave New Coin* (17 ago. 2017). URL: https://bravenewcoin.com/news/mtgox-btc-e-and-the-missing-coins-a-living-timeline-of-the-greatest-cyber-crime-ever/.

[28] Joseph Young. “The Centralization Issue of Scaling BTC Solely by Block Size Increase”. In: *News BTC* (12 nov. 2017). URL: https://newsbtc.com/2017/11/12/61408/.

[29] Marie Huillet. “Bitcoin Cash Opposers Scrap Lawsuit Against Bitcoin.com, Citing Lack Of Cash”. In: *Cointelegraph* (4 mag. 2018). URL: https://cointelegraph.com/news/pro-btc-movement-scraps-lawsuit-against-vers-bitcoincom-citing-lack-of-funds.

Giugno 2018