Liceo Scientifico Arturo Tosi

Tesina di Maturità

Bitcoin, Blockchain, Crypto

Carlomaria Occhipinti 5F

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. Panico. 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, 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 Nakamoto è conosciuto come l'ideatore e l'iniziale sviluppatore del Bitcoin. Nessuno sa 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. Satoshi scrisse il whitepaper[1] del Bitcoin contenente la sua ideologia di moneta virtuale. Il documento è altamente tecnico e richiede un'elevata conoscenza di informatica e matematica, ma mi sembra doveroso citare il primo paragrafo [2]:

> **Abstract**. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Tradotto in italiano:

> **Riassunto**. Una versione puramente *peer-to-peer*[3] di soldi elettronici permetterebbe ai pagamenti online di essere inviati direttamente da un party all'altro senza passare attraverso un'istituzione finanziaria. Firme digitali sono? parte della soluzione, ma i benefici principali sono persi se un ente di terza parte creduto? è sempre/comunque richiesto per prevenire la doppia spesa. Proponiamo

[1] "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.

[2] http://bitcoin.org/bitcoin.pdf

[3] Da pari a pari, senza la necessità di passare da un ente centrale come una banca

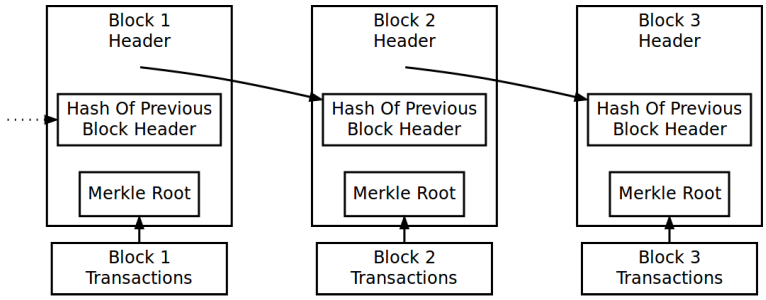

Fig. 1: Schema semplificato della blockchain

una soluzione al problema della doppia spesa usando una rete *peer-to-peer*. La rete registra? le transazioni hashing? them in una catena ongoing di hashbased pow, formando un registro che non può essere modificato senza ripetere la pow. La catena più lunga non serve solo come prova per la sequenza di eventi testimoniati/accaduti, ma la prova che è venuta/derivata dalla pool più grande di potenza cpu. Finché la maggioranza del potere cpu è controllato da nodi? che non stanno cooperando per attaccare la rete, genereranno la cantena più lunga e supereranno gli attaccatori. La rete stessa richiede una struttura minimale. I messaggi sono trasmessi su una base del miglior sforzo, e i nodi possono lasciare e rientrare la rete a voglia, accettando la più lunga pow catena come prova di cos'è avvenuto mentre erano via.

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.

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. Le transazioni hanno un determinato peso espresso per comodità in kilobyte fare paragrafo mempool+foto, dove lo metto? (domanda:come fanno le transazioni ad essere messe nei blocchi?) Tutte le transazioni di BTC sono permanentemente, irreversibilmente (nella maggior parte dei casi, V X.X) 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 Gi-

gabyte. 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 attiva (quando definizione full node?) l'intera rete del Bitcoin e il registro delle transazioni rimangono autentiche e inviolate. 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*.

2.1 Mining

Sebbene non sia tecnicamente corretto, il modo più semplice per spiegare il concetto di "mining"(corsivo?) 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 (*application specific integrated circuit*), dei computer specializzati a risolvere un certo tipo di algoritmo. Algoritmo, perchè il processo di mining dipende interamente dalla matematica. Questa è quella che nel whitepaper Satoshi definisce come *proof of work*.

Proof of work Tradotto "prova di lavoro" o "di funzionamento" è il sistema che rende il Bitcoin una rete sicura... difficile... irreversibile

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.

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 come il "confine" sotto al quale tutte le hash sono accettabili. (temp) se le hash sono numeri da 1 a ..., il target è uno di quei numeri. Tutte le hash trovate dai miners che hanno valore minore del target sono valide, e portano alla scoperta di un nuovo

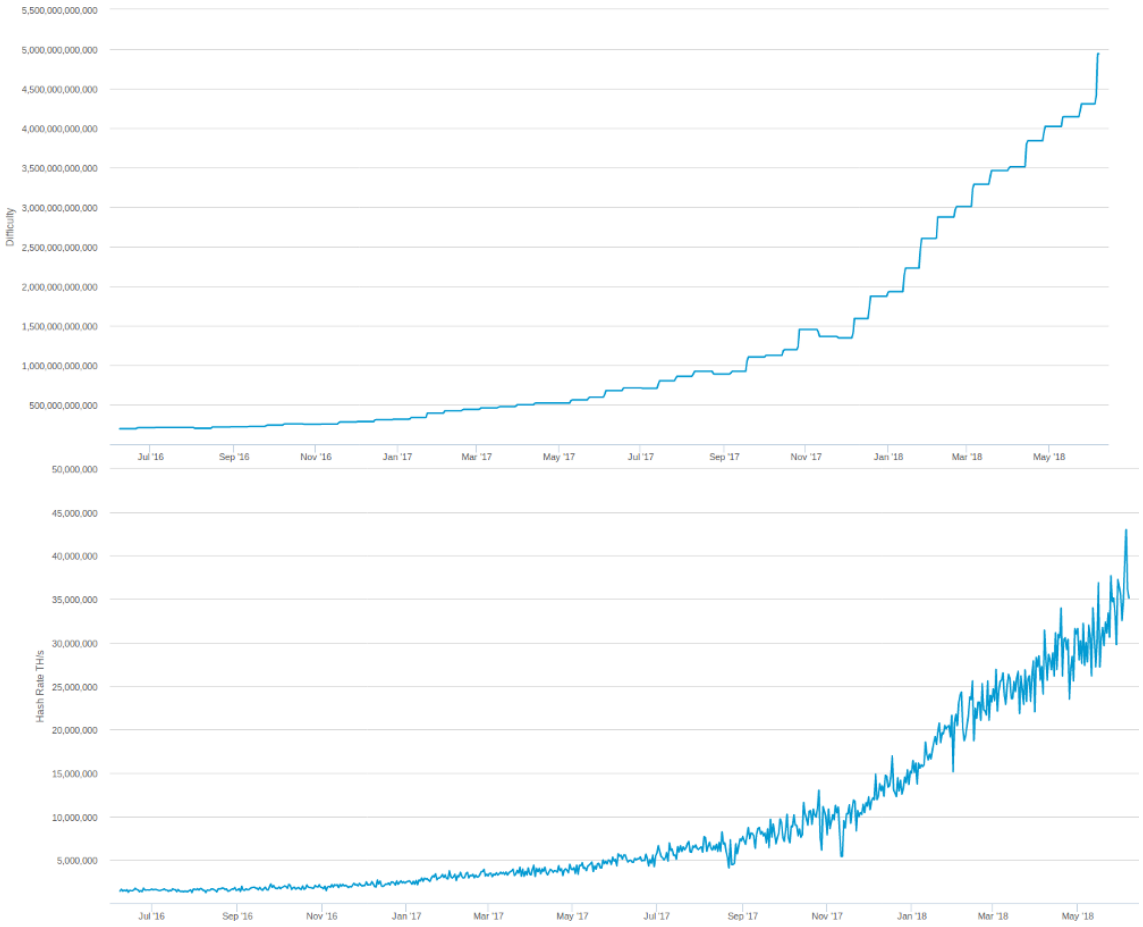

Fig. 2: Confronto tra difficoltà (sopra) e hashrate globale (sotto)

blocco. Con "difficoltà" si intende, ovviamente, quanto è difficile trovare un blocco, e se facciamo ragionare un po' la testolina possiamo capire che è in un modo o nell'altro collegata al valore 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? Satoshi ha deciso che ogni blocco deve impiegare un tempo di circa 10 minuti per essere scoperto (perché?). 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.

Aumentando la difficoltà in modo proporzionale all'*hashing power* si fa in modo che in media i blocchi continuino ad essere trovati ogni ~10 minuti. 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. Il *nonce* è un numero di 32bit (...) che determina la quantità di zeri dell'*hash* del blocco.

nome paragrafo? I miner di Bitcoin che si usano oggi lavorano a velocità comprese tra i 10 e i 14 TH/s (tera-hash al secondo) 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 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* finisce a una singola persona: indovinare l'hash che trova il blocco è estremamente difficile! Per questo esistono le *pool* di mining.

Mining pools Le *pool* sono dei siti in cui più miners[4] 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. Esistono diversi sistemi per spartire il "bottino". Tra i più diffusi troviamo:

- PPLNS: *Pay Per Last N Shares*
- PPS:
- Score:
- FPPS:

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.

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/commissione è espressa in sat/byte, satoshi[5] per byte. Una tassa più elevata riduce il tempo di conferma della transazione, perché preferita dai miner.

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

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

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 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/byte[6] per scoprire quanto paghiamo effettivamente possiamo ricavare la quantità di BTC dalla proporzione.

$$nSat : 1byte = tassa : pesoTx$$

o semplicemente utilizzando la formula $xtassa = \frac{nSat \times pesoTx}{1byte}$.

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.

2.1.1 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, il più debole (4 TH/s) 1000 W. In media, un S9 che lavora in una *pool* di mining fa guadagnare circa 0.00082 BTC al giorno, ovvero circa €5.5. Considerando che le *farm* sono locate in paesi in cui l'elettricità costa poco, intorno ai €0.04/KWh, 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 [7], 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

[6] Spiegherò come si viene a conoscenza di queste due nel punto X.Y
[7] *return on investment*

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, ovvero 60.000 miliardi di Joule consumati all'ora. Questo consumo di elettricità corrisponde a (piu di 0.13, perche dati dic 2017, cercare nuovi) dell'utilizzo di elettricità in tutto il mondo. ... ... (citazione a powercompare.co.uk)

2.2 Come e dove si conserva il Bitcoin

2.2.1 Indirizzi

Gli indirizzi sono delle stringhe di circa 30/40 caratteri che sono il luogo(?) in cui ci sono i bitcoin. suona male. cioè nella blockhain si dice "a indirizzo x sono associati y btc" Un indirizzo Bitcoin può essere visto come un codice IBAN se si vuo,e rimanere in un contesto finanziario, o anche come un indirizzo 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.

P2SH SegWit P2SH significa "Pay 2 Script Hash". Gli indirizzi P2SH sono stati ideati il 18 Ottobre del 2011 con il BIP-13 e mandati live l'1 Aprile del 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 software/full node? stavano includendo nei blocchi transazioni ritenute invalide dai loro software (ripetizione, suona male). La differenza sostanziale con gli indirizzi "normali" è che ..multisig...sigh...è difficile

bech32 SegWit Gli indirizzi Bitcoin bech32 implementano SegWit al 100%, e di conseguenza sono quelli con le tasse di transazione/i più inferiori. Questo tipo di indirizzo è stato creato nel XXXX, ed essendo sotto un punto di vista tecnico molto diverso dagli indirizzi tradizionali (che cominciano con 1 e 3), non sono supportati da una moltitudine di siti di compravendita e da portafogli, (di cui parlerò in seguito). Gli indirizzi bech32, infatti, hanno il prefisso "bc1", e tutt'oggi cose

2.2.2 Keys

Ogni indirizzo Bitcoin è composto due chiavi: una *public key* e una *private key.* dovementtto come si generano e che ne esistono un casino?

Public key Da non confondere con l'indirizzo in sé, la chiave pubblica(key lo dico in ing o ita?)Every public key is 256 bits long — sorry, this is mathematical stuff — and the final hash (your wallet address) is 160 bits long. The public

key is used to ensure you are the owner of an address that can receive funds. The public key is also mathematically derived from your private key, but using reverse mathematics to derive the private key would take the world's most powerful supercomputer many trillion years to crack. dal sito dei dammis. quando dico n tot indiriziz? dopo devo anche scrivere di come funziona lo storage offline (come indirizzo email che puo ricevere ma non mandare v preferiti windows

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 key sono numeri di 256 *bit*, che nel sistema numerico esadecimale sono codici di 64 caratteri tra numeri e lettere. A differenza delle *hash* SHA-256, però, le private key devono essere comprese tara 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 una serie di parole (solitamente 12 o 15) che svolgono una funzione simile a quella della *private key*: se inserite in un software di wallet, ripristinano tutti i bitcoin associati ad esso. La differenza con le private keys è che a un seed non corrisponde *una* private key, bensì circa/fino a ... indirizzi, ovvero ~X coppie di private e public keys. Con il BIP-39 [8] è stato introdotto...? 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 privacy dello spenditore? Come abbiamo visto nella blockchain chiunque può accedere alle informazioni di chiunque (suona male), così per rendere i fondi meno tracciabili si possono usare diversi indirizzi per diverse operazioni... spiegare.

2.2.3 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.

Cold storage *Cold storage* Con il *cold storage*[9], *public* e *private* keys sono conservate offline, ovvero in un posto(?) non collegato a internet. I principali tipi di *cold storage* sono:

- Digitale: le keys sono salvate sottoforma di file su un computer, un CD, una chiavetta USB...

[8] *Bitcoin Improvement Proposal*
[9] Archiviazione a freddo

Fig. 3: Un Ledger Nano S

- Carta: si possono scrivere le keys su un pezzo di carta, o stamparle su un "portafoglio" bello tipo figo.. (foto + descrizopne dopo) 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.
- *Hardware wallet*:I portafogli hardware, come suggerisce il nome, sono dei piccoli dispositivi simili a chiavette USB (singolare o plurare?), in cui la *private key* è contenuta.

METTERE FOTO DI UN FOGLIO STAPATO FIGO ACCANTO Esistono anche dei veri e propri "Bitcoin" fisici, ovvero delle monete materiali con incise le keys (gia caricatte a volte, si)? Hot wallets are like checking accounts while cold wallets are similar to savings accounts.x me poi tolgo

Hot wallets Gli *hot wallets* sono invece dei portafogli che utilizzano un collegamento a internet per permettere di effettuare pagamenti *da* l'indirizzo associato?importato? che si usa? Gli *hot wallets* esistono come software, ma è comunque possibile dividerli in tre principali categorie:

- App per smartphone
- Programma per computer
- Servizio online

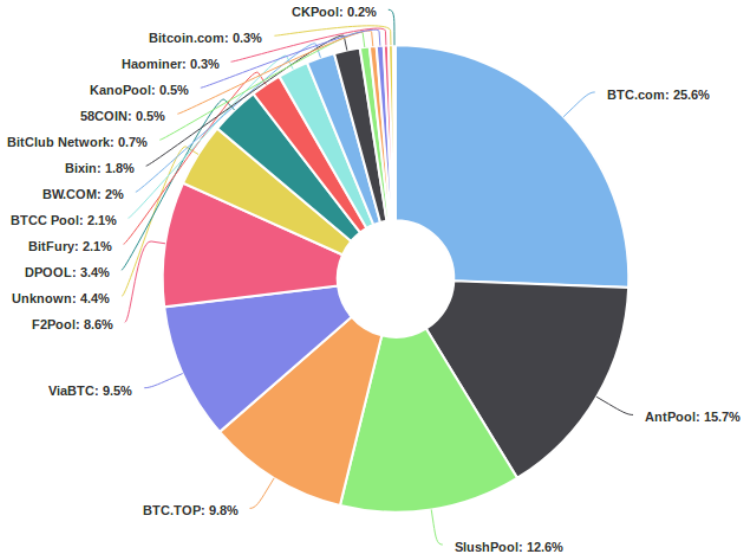

Fig. 4: pie-chart della percentuale di hashrate controllata dalle più grandi pool

2.3 I problemi del Bitcoin

2.3.1 La parziale centralizzazione

L'intenzione di Satoshi, con la creazione della blockchain e di un sistema di mining universale, fu/è/era quella di creare una valuta decentralizzata, e in parte ci è riuscito. Purtroppo, il lavoro dei miners è concentrato in una piccola (nicchia? giro? gruppo?) di pools. https://medium.com/@homakov/stop-calling-bitcoin-decentralized-cb703d69dc27 poi aggiungerlo alla bibliography se capisco come si fa

aa

2.3.2 Gli attacchi al network

2.3.3 Il limite dei blocchi da 1 Megabyte

2.4 Soluzioni ai problemi

Il Bitcoin è la prima criptovaluta mai creata, e questo la rende anche la più vecchia e obsoleta sotto il punto di vista tecnologico. Come vedremo in seguito, infatti, oggi esistono molte valute che riducono, o in certi casi sistemano i principali "problemi" del Bitcoin.

2.4.1 Segregated Witness

Segregated Witness (comunemente abbreviato in SegWit) è una roba che riduce le tasse

2.4.2 Lightning Network

Il Lightning Network è un network lightning.

3 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.

3.1 Creazione del portafoglio

Come descritto in X.X, il portafoglio è quel software (ma non solo.. questione del cold) che ci dà l'accesso ai bitcoin salvati nella blockchain (dire che è sbagliato dire che sono *nel* portafoglio) Per comodità è consigliabile usare un app per smartphone, ma volendo esistono anche programmi per computer e servizi online. A proposito di 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 e cominciato il processo di setup (?) SEED, ...

3.2 Come ottenere criptovaluta

Exchange Il metodo più veloce e utilizzato è quello di acquistarlo su un sito di exchange (cambio valutario). Esistono moltissimi siti che permettono di acquistare Bitcoin con bonifico bancario o semplicemente con una carta di credito, come se si stesse acquistando un oggetto. Coinbase è di gran lunga l'exchange più famosa del mondo. Basta aprire un account, collegare il proprio conto o la carta di credito, e compare bitcoin è questione di secondi. Una volta acquistato, è consigliabile spostare i propri bitcoin su un "wallet" indipendente dal sito dell'exchange. Quasi tutte le exchange più reputabili sono dotate di sistemi di sicurezza ad elevatissimo livello che riducono la possibilità di una *security breach* 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 (fee, higher trade price) 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.

Mining Come spiegato in precedenza, il processo di mining porta i miners a guadagnare criptovalute, che possono essere vendute (se parlassi pirma delle altre valute??) per btc, o soldi veri e propri. Nonostante i costi dell'equipaggiamento di mining e dell'elettricità utilizzata, i miner ricavano comunque un profitto dai coin che guadagnano. Ovvio che per una persona inesperta il mining è fuori portata, ma è certamente un modo valido per ottenere dei coin

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. Per esempio,

3.3 Trasferire Bitcoin

Una volta che i bitcoin sono arrivati al nostro indirizzo, è possibile interagirci con un apposito "portafoglio". Un portafoglio può esser bla bla Tutti i portafogli degni di essere chiamati tali hanno la funzione di inviare bitcoin ad altri indirizzi, e per riceverli lol 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 (che brutto) "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.

4 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, che è semplicemente invero. Tutte le criptovalute che non sono Bitcoin prendono il nome di Altcoin (alternative coin).

4.1 Ethereum

Ethereum è una valuta creata da Vitalik Buterin, uno sviluppatore slavico xd CHE PALLE

https://github.com/ethereum/wiki/wiki/White-Paper

https://www.ethereum.org/ether
https://theethereum.wiki/w/index.php/MainUNDERSCOREPage
https://www.coindesk.com/information/ethereum-smart-contracts-work/

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[10]. La più grande differenza tra i due algoritmi è che Ethash richiede una quantità di RAM[11] ben maggiore di quella dei miner ASIC. spiegare DAG Le schede grafiche dei computer desktop, comunemente chiamate GPU[12], grazie alla maggior quantità di RAM (superiore a 4GB nella maggior parte delle schede moderne), sono effettivamente l'unico mezzo 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 (come abbiamo visto in...? o se lo mettessi già su?) sono grandi minacce per la decentralizzazione della valuta. Le schede grafiche sono possedute da chiunque possieda/possedesse un 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 concentrazione dell'*hashing power* in siti singoli?come dire?, di conseguenza riducendo la possibilità di attacchi alla rete descritti in X.X. parlare del dilemma gpuvsasic?

L'inflazione del mercato di schede grafiche Come si dice qunado costa di piò? Il boom del mining di ETH, 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 acquistare GPU in negozi veri(?) e online. (posso mettere che anche io lo faccio?) Certi miners di Ethereum, però, acquistarono schede grafiche in quantità colossali per creare delle vere e proprie *farm*, con centinaia, se non migliaia di GPU ciascuna. Si verificò una vera e propria crisi nel mercato delle schede grafiche: i negozi erano quasi costantemente *sold out??*, e appena arrivava un nuovo carico(?) di GPU queste venivano istantaneamente acquistate. Ovviamente i mercanti videro questa come un'opportunità per aumentare i profitti della loro merce, e così aumentarono esponenzialmente i prezzi di tutti i modelli di scheda/e grafica. Per esempio le AMD RX 580 8GB con MSRP[13] pari a €159 raggiunsero prezzi ben oltre €300. Questa inflazione

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

[11] *Random Access Memory, memoria ad accesso casuale che serve per memorizzare cose...*

[12] *Graphics Processing Unit*

[13] *Manufacturer's Suggested Retail Price*, il prezzo di un oggetto consigliato dal manufattore

è in corso tutt'oggi, e FOTO FARM DA QUALCHE PARTE

Genesis mining video, cose.

4.2 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. Tecnicamente, Litecoin è una fork del Bitcoin (ma hard come quelle dopo?) Come per questi metalli, infatti, l'oro è usato come uno *store of value*[14], essendo un metallo prezioso con elevato valore (oggi circa €42 per grammo). L'argento è un metallo più comune con valore ben inferiore all'oro (oggi circa €16 per grammo), 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(perché?). Questo rende 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.

4.3 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 tutti gli altri coin, 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 viene utilizzato anche da evasori delle tasse, truffatori e da venditori di merce illegale Monero ha tuttavia dei limiti e non si può considerare come una valuta "perfetta":

4.4 Nano

Inizialmente chiamata RaiBlocks[15], Nano è una criptovaluta creata nel MESE 2015 dallo sviluppatore Colin LeMahieu. A differenza delle valute che dipendono

[14] Riserva di valore

[15] il passaggio da RaiBlocks a Nano è avvenuto il 31 Gennaio 2018

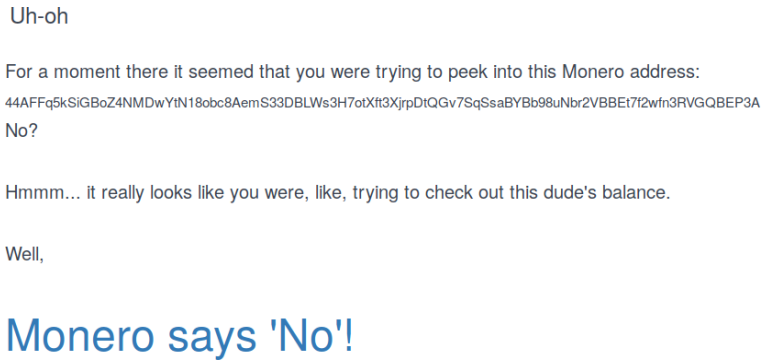

Fig. 5: Sul sito moneroblocks.info viene mostrato il seguente messaggio se si cercano informazioni legate a un indirizzo

da *proof of work*, Nano non prevede l'impiego di miners per validare le proprie transazioni https://nano.org/en/faq. sistma di representers... ecc. dovrei metterlo dopo? 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*[16] 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* , poichè...SPIEGARE, rende tutte le transazioni di Nano completamente gratuite.

4.5 Ripple

Ripple è un altcoin creato nel dalla Ripple Foundation. (each transaction destroys a small amount XRP, is the supply of coins getting smaller?)

La sua particolarità sta nel fatto che Ripple mira ad essere una valuta fortemente legata all'ambito bancario, utilizzata per...? 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. Per questo, la Ripple Foundation possiede oltre il 50% di tutti i ripple, circa 50.000.000.000 XRP. Questo le permette di modificare artificialmente il prezzo.

[16] Da non confondere con la parola italiana, *lattice [/'let.is/]* significa reticolo, intreccio

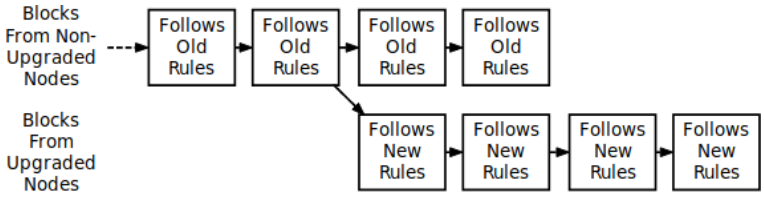

Fig. 6: Hard fork: Non-Upgraded nodes reject the new rules, diverging the chain

4.6 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.

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.

4.6.1 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, finanziando progetti (?) e tenendo discorsi (??). Da Agosto 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 BCH (pagati o no non si sa), è quella che BCH introduce delle modifiche al codice di Bitcoin che rendono le transizioni notevolmente più veloci, sicure e con una tassa di transazione inferiore. Bitcoin Cash infatti ha come principale differenza un'incrementata dimensione del blocco (V. 1.2), che anzichè limitarsi a 1MB arriva fino a 12MB (come abbiamo visto, ogni transazione pesa tot kb. essendo il blocco più grande può farci stare più transazioni, senza "intasarsi"). 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 (valute decentralizzate, internazionali, v 1.1). 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. 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 600? persone e fu eventualmente costretto a tornare alle vecchie denominazioni delle valute che, purché volontariamente misleading, non facevano apparire BCH come il "vero" Bitcoin. 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

5 Crypto oggi

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

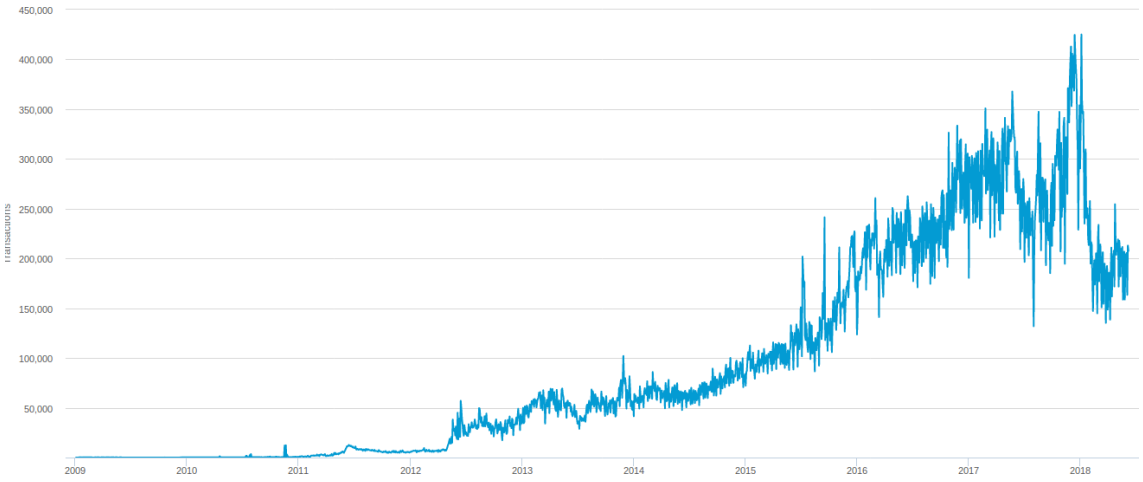

Fig. 7: Transazioni giornaliere a partire dal 2009

5.1 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 negozi online e nella vita reale stanno cominciando ad accettare criptovalute come forma di pagamento,[17], tra cui:

- case...
-
-
-

Oltre a questi servizi, è anche possibile acquistare merce su siti che non accettano ancora criptovalute. bitcoinsuperstore.us e coinbought.com Un fattore concreto che indica l'adozione del Bitcoin è il numero di transazioni giornaliere:

aa

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

Elizavetovska: il villaggio in Ucraina in cui tutti utilizzano criptovalute è bellus

[17] https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/

5.2 La bolla del 2017: cause e conseguenze

A partire da 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?

5.2.1 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. Questo è estremamente simile a quello che è successo al Bitcoin perché sì.

La ricorrenza dei "crash" dei mercati A seguito

5.3 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.

5.3.1 Il ban del Bitcoin in certi stati

boh

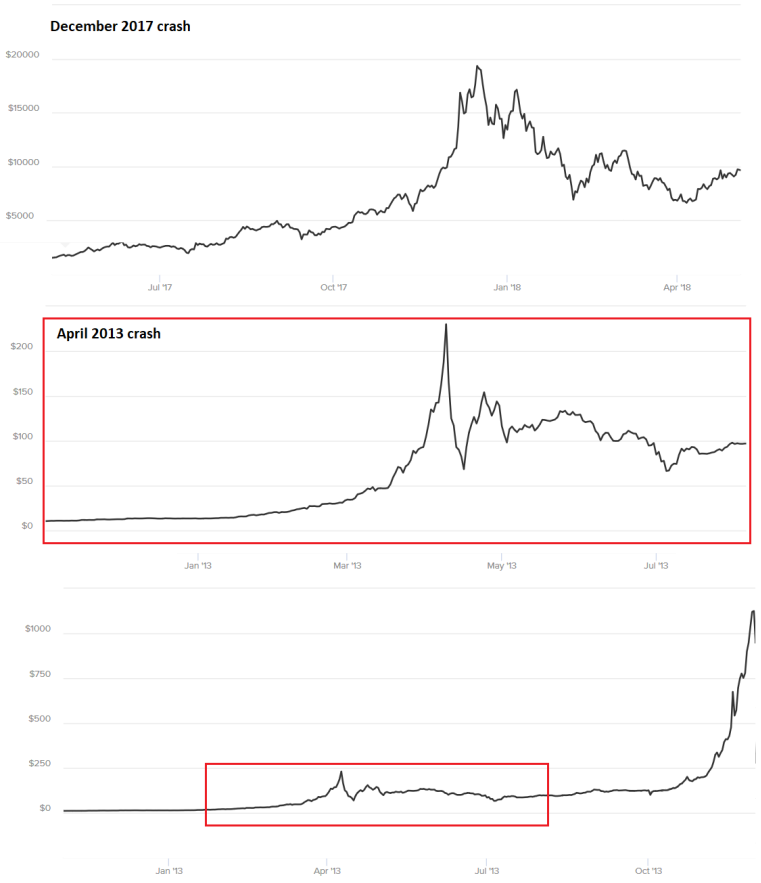

Fig. 8: Confronto tra il crollo del prezzo del Bitcoin nel 2013 e nel 2017

5.3.2 Mt. Gox

Mt. Gox è il primo grande sito di exchange di Bitcoin, creato a Tokyo nel 2013. Ai tempi il Bitcoin aveva un valore ben più basso del ~9000 di oggi: il giorno in cui l'hack è avvenuto un bitcoin valeva "solo" €500.

5.3.3 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 negli anni '30(??????) compiendo ripetutamente questo tipo di truffa. Oggi tutti coloro coinvolti nel pubblicizzare Bitconnect, soprattutto Youtuber (spiegare chi sono?) sono sotto investigazione

5.4 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.

aa

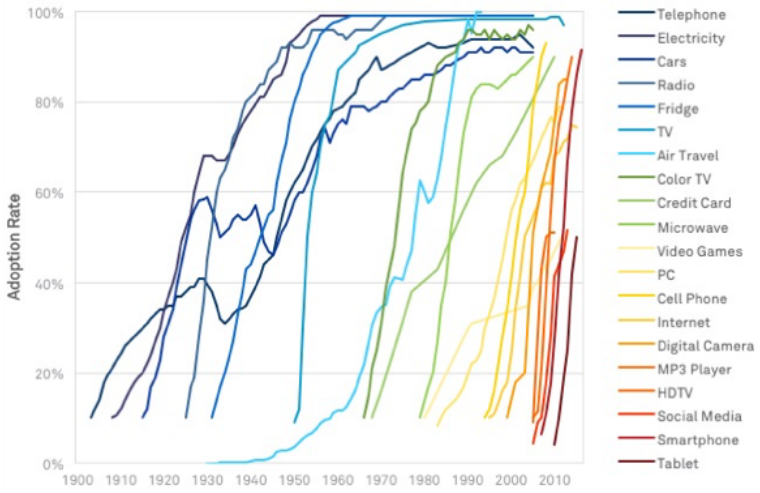

Fig. 9: Adozione del Bitcoin paragonata ad altre tecnologie

Donazioni

Se la tesina ti è piaciuta dammi soldi gratis! indirizzo btc ltc xmr nano eth