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(?) del Bitcoin, un documento 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 [1]:

> **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*[2] 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 una soluzione al problema della doppia spesa usando una rete *peer-to-peer*. La rete registra? le transazioni hashing? them in una catena

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

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

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 su *alcune* transazioni di bitcoin Tutte le transazioni di BTC sono permanentemente, irreversibilmente (nella maggior parte dei casi, V X.X) memorizzate nella Blockchain. Volendo, posso vedere quanti bitcoin X ha spedito a Y. Ogni blocco, infatti, contiene informazioni su tutte le transazioni che sono state compiute nell'intervallo di tempo che passa dalla scoperta del blocco precedente a quello nuovo (foto). In che senso "rimane attivo"? Quando un blocco diventa "inattivo"? Mi tocca introdurre il concetto di "mining". (mi manca la parte sul peso in kb delle tx, cos'è in pratica la blockchain (file)).

2.1 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 "risolti" 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 consiste esclusivamente nella matematica. L'obiettivo del mining è quello di indovinare la "parola chiave", chiamata "hash" che serve per risolvere un blocco. Il Bitcoin usa l'algoritmo SHA-256, quindi le hash indovinate dai miner sono una serie di numeri e lettere lunga 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(?) esadecimale un carattere "pesa" 8 bit, quindi $256 : 8 = 64$. Una hash del sistema(?) SHA-256 deve rispettare determinati parametri per essere considerata tale, di cui non scriverò per evitare di com-

plicare 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. MA NON E FINITA CUI! https://en.bitcoin.it/wiki/Target 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 tentativi 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 (v dopo, o posso scriverlo qua?). Perchè, allora, c'è gente che spende tutti questi soldi per fare il lavoro di mining? PROOFG OF WORK SOMEWHERE AAAAAAAAAA Ebbene, quando si "risolve" un blocco, il miner riceve una quantità pari a 12.5 bitcoin, oggi pari a circa €90000 (parlare di halving whand?). Quasi mai, però, i 12 btc finiscono a una singola persona: indovinare la stringa che mina il block è estremamente difficile! Per questo esistono le "pool" di mining, dei siti in cui più miners uniscono gli sforzi per risolvere il blocco. Una volta indovinato, la ricompensa si spartisce fra tutti i miner, in base a quanto ciascuno si è impegnato per trovarla. Torniamo a noi, cosa succede quando il blocco è minato, e si passa a quello successivo? Tutte le transazioni effettuate mentre i miner erano alla ricerca del nuovo blocco vengono memorizzae nellba vlohack ?? Per questo, una transazione è considerata conclusa quando si passano almeno 6 blocchi dopo quello in cui è stata iniziata. 3 perchè.....?? e da qualche parte devo parlare di DIFFICULTY è così che funziona la blockhain bla b la

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 per funzionare /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 (*return on investment*), 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 ($717 : 4 = 179.25$). Questo è quanto vale per *una* singola unità di mining 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, 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 "Soft forks"

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.

2.2.1 Segregated Witness

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

2.2.2 Lightning Network

Il Lightning Network è un network lightning.

2.3 How and where Bitcoin is stored

2.3.1 Keys

Seeds A seed is kind of a password that gives you access to your coins (stored online?) a seed is typically 12 or 15 english words that, when put into the wallet ocnfiguration makes magically appear all your coins. That's the reason why "seed stealing" is the most common tactic of stealing funds: with a bunch of apparently useless words, new users can be tricked into sending them to a scammer who quickly steals alltheir coins and runs away. A seed is associated with x different Bitcoin addresses, for privacy purposes: despite not being linked with private information such as name, surname and address, we saw that every transaction is permanently written into the blockchain, and anyone can see any address' current BTC balance. For this reason, having different addresses helps in making the user less traceable (SCRIVERE PRIMA COME SI POSSONO TRACCIARE), as it's impossible to link the seed's different addresses. Wallets that use seeds still report the total balance as the sum of funds in each seed's address.

2.3.2 Addresses

The coins are stored in addresses, a string of 26 to 35 characters that starts with either 1, 3, or bc1 (I'll explain the differences between those later). An address can be seen as an IBAN address, or even an email address.

"Legacy" Con "legacy" mi riferisco al primo formato di indirizzo, utilizzato esclusivamente fino all'agosto del 2017. Questi indirizzi si riconoscono dal fatto che iniziano col carattere '1', per esempio mioindirizzo.

P2SH SegWit P2SH significa "Pay 2 Script Hash",

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

2.3.3 Wallets

A wallet is the software used to let the user interact with their coins. not really, non sono gli hot? It can be an app for smartphones, a program on a computer, or even an online service.

Cold storage Cold wallets (also known as "cold storage") are the best option for those who are interested in keeping their coins safe, without actually spending them. A cold wallet is not connected to the internet, and this makes it impossible for hackers to breach into an online database and steal the private keys: FORSE NON è CORRETTO, SEND HELP. LE PRIVAKE KEYS Cold wallets can be literal pieces of paper, with a public address and public key written on it. This makes it possible to store bitcoin in a bank, by putting said pieceofpaper in a safe. Cold wallets, as I said, are not advisable to HOW TO SPEND FROM COLD?

Hot wallets Hot wallets, unlike cold wallets, are the most useful wallets because they allow the user to send BUT WHY?????

Hardware wallets Hardware wallets are, as the name sucggests, small devices as big as a USB drive that are usedf definitely the safest way to store cryptocurrency as the private key is exclusively stored on the device itself, and noone can access them. Unhackable, net even sunvb.

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) HOW ARE ADDRESSES MADE 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 cartacredito?? 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/

Mining e il crollo del mercato di schede grafiche In precedenza mi sono concentrato sul processo di mining del Bitcoin, ma come quasi tutte le valute (nano xk no mining?) 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 rende Ethereum "minabile" da chiunque ha/avesse un computer, e di conseguenza i miner di ETH sono per quantità molti più dei miner "tradizionali". Il boom del mining di ETH, come quello del prezzo di tutte le criptovalute, avvenne tra la fine del 2017 e l'inizio del 2018.

4.2 Litecoin

Litecoin è una criptovaluta creata nel 2011 dallo sviluppatore Charlie Lee. L'obbiettivo di questa valuta è quello di comportarsi come l'argento fa con l'oro / se bitcon è l'oro, ltc è l'argento. Come per questi metalli, infatti, l'oro è usato

come uno *store of value*, una riserva di valore, 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 come forma di pagamento. 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]. Questa è la differenza principale, ma di certo non l'unica. https://www.coindesk.com/information/comparing-litecoin-bitcoin/ adesso no sbatty

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.

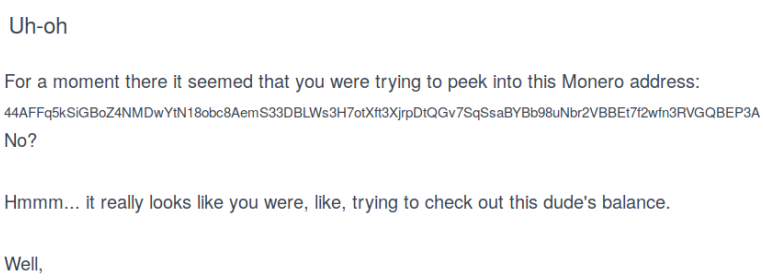


Fig. 1: Sul sito moneroblocks.info viene mostrato il seguente messaggio se si cercano informazioni legate a un indirizzo

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 (V CONTROVERSIE O ADOPTION?). Monero ha tuttavia dei limiti e non si può considerare come una valuta "perfetta": non eccelle nel campo "transazioni veloci e cheap????": in confronto al Bitcoin POST SU RMONERO BC NON TROVO INFO.

4.4 Nano

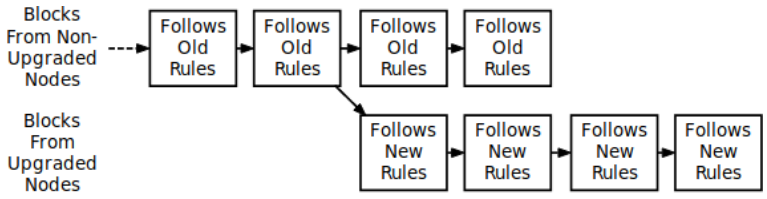
Inizialmente chiamata RaiBlocks, Nano è una criptovaluta creata nel da. È veramente interessante sotto il punto di vista tecnico perché è la prima che usa la tecnologia *Block Lattice* (BLOK LAH-DES): in sostanza, anzichè dipendere da una singola blockchain come fanno tutte le altre valute, ogni singolo indirizzo *è* una blockchain a sè/se/sé stante. Questa tecnologia permette di effettuare transazioni estremamente veloci rispetto a quelle del Bitcoin (che impiegano in media 20 minuti), con una durata inferiore ai 2 secondi, talvolta letteralmente istantanee. Non è l'unico vantaggio. Ho spiegato in 1.1/2? che ad ogni transazione di Bitcoin è necessario pagare una piccola tassa di conferma che varia da un centesimo a un'Euro a seconda di quanto i blocchi sono "intasati" di transazioni. La *Block Lattice* , poichè...SPIEGARE, rende tutte le transazioni di Nano completamente gratuite. Nano inoltre non richiede mining perché... reddit? ricerca?

4.5 Ripple

Ripple è un altcoin che è brutto perche legato alle banche centralizzato il 90% è posseduto dai ricconi ma comunque riesce ad essere al terzo posto per market cap smh

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.



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

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 ul-

teriormente 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/sè, 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

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,[3], tra cui: Questi Oltre a questi servizi, è anche possibile acquistare merce su siti che non accettano ancora criptovalute. bitcoinsuperstore.us e coinbought.com

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

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?

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

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 loro(?) 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 E quindi sì.

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

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

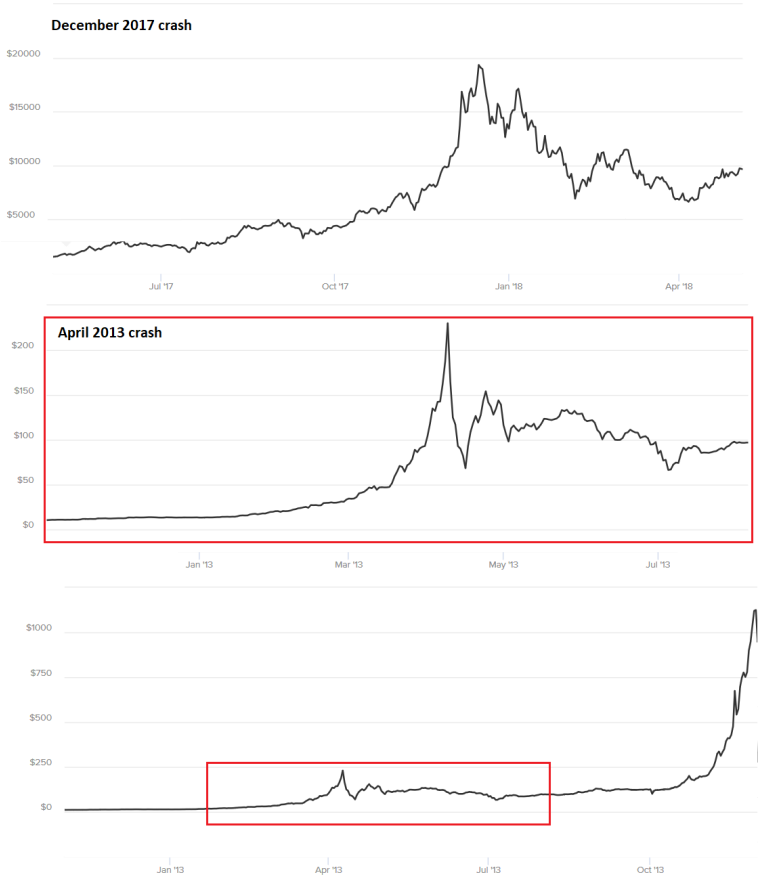


Fig. 2: Confronto tra il crollo del prezzo del Bitcoin nel 2013 e nel 2017

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 al cinema 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.

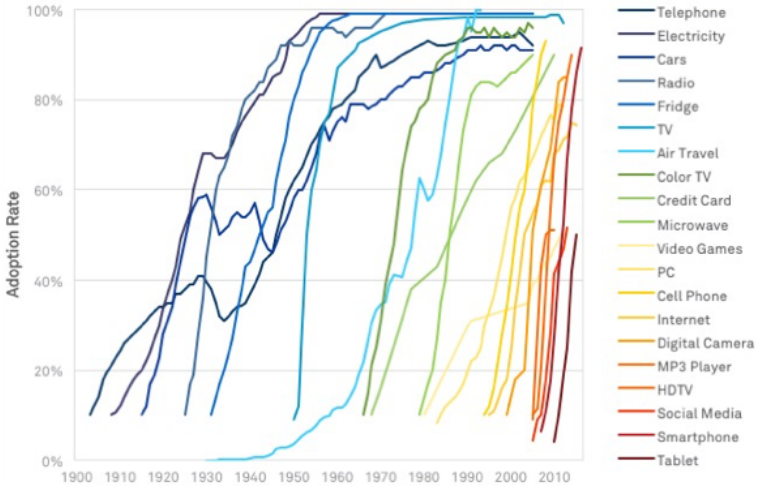


Fig. 3: Adozione del Bitcoin paragonata ad altre tecnologie