Bitcoin, blockchain, crypto

Carlomaria Occhipinti
Liceo Scientifico Arturo Tosi

Giugno 2018

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.

Questo paragrafo comprende le parole chiave che rendono il Bitcoin una valuta unica, che non si era mai vista prima.

Decentralizzata:

Privata:

Deinflazionaria:

Sicura:

–no, leggendolo attentamente non include nessuna di queste parole. sistemo dopo

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

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/significa una catena di blocchi. Come la figura mette bene, tutte le transazioni di BTC sono permanentemente, incancellabilmente 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 "miners", 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 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. 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 (come gestire paragrafi uso elettricità, profitti e effetti su ambiente?

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 Watt 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 How and where Bitcoin is stored

2.2.1 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" Sono quelli che cominciano con 1 i piu schifosi ma tristemente i + famosi

P2SH SegWit Cominciano con 3, sono cool

bech32 SegWit I piu veloci e belli ma poco ompatibili

Cold wallets 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.

2.2.2 Keys

Every Bitcoin address is associated with a private key. A private key, as the name suggests, is a key that gives full access to the coins stored in its address.

2.2.3 Seeds

Most hot wallets work with 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.

PARLARE DI ALTRI ALGORITMI E ALTRE VALUTE, AJCHE SE PARLO DOPO DELLE ALTE VALUTE, ONON SO CSAO FARE AOITUO.....

2.3 Cuscinetti / integrazioni

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.

2.3.1 Segregated Witness

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

2.3.2 Lightning Network

Il Lighning 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 Conservare Bitcoin

A wallet is the software used to make the user interact with their coins / that makes you send and recieve Bitcoin. It can be an app for smartphones, a program on a computer, or even an online service. Bitcoin can be stored in two different ways: cold wallets and hot wallets.

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 btc è questione di secondi. Una volta acquistato, è consigliabile spostare i propri bitcoin su un "wallet" indipendente dal sito dell'exchange. Coinbase è la più sicura e attendibile, ma ci sono stati tragici episodi di exchange hacked, mln lost. (v sub...)

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 https://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

Vendere roba Se si vende qualcosa su internet o nella vita reale si può comunicare ai clienti che è preferibile accettare pagamenti in Bitcoin.

3.3 Spendere Bitcoin

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 servizi. Nonostante ciò, sempre più negozi online e nella vita reale stanno cominciando ad accettare criptovalute come forma di pagamento. Esiste una pagina (FARE LINK DIDASCALIA IN BASSSO https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/) con una lista che comprende (ma non è limitata a) luoghi e siti web sui quali si può pagare in bitcoin. La lista comprende un numero limitato di attività commerciali, ma in realtà sono molti di più. Tra i più rilevanti ci sono: ELENCO PUNTATO Oltre a questi servizi, è anche possibile acquistare merce su siti che non accettano ancora criptovalute. Bitcoinsuperstore.us, coinbought.com

4 Non solo Bitcoin

Esistono numerosissime criptovalute. Il sito https://coinmarketcap.com ne lista ben 1640. Ritengo indispensabile spendere almeno qualche pagina per parlare delle valute più rilevanti, perchè a common misconception is that Bitcoin is the only cryptocurrency. This is simply not true. 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/