Bitcoin

Carlomaria Occhipinti

May 16, 2018

Contents

1 Il funzionamento del Bitcoin

1.1 Blockchain: cos'è e come funziona

La tecnologia rivoluzionaria utilizzata dal Bitcoin e da tutte le altre criptovalute è chiamata Blockchain (technology?). 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 in cui quel blocco rimane "attivo". In che senso "rimane attivo"? Quando un blocco diventa "inattivo"? Mi tocca introdurre il concetto di "mining". 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. Il mining consiste in (l'ho gia detto 3 o 4 volte lol) indovinare la "parola chiave", chiamata "hash" (non la droga xd) che serve per risolvere un blocco. Questa parola chiave è una stringa lunga circa XXXX caratteri. Come uno può immaginare, indovinarla è molto difficile, infatti i miners lavorano a velocità esorbitanti. Il miner di Bitcoin che si usa oggi lavora a 13.5 TH/s (terahash al secondo), ovvero PIU DI TREDICI TRILIONI DI TENTATIVI IN UN SECONDO. Questi apparecchi sono molto costosi (minimo 1000 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? PROOFG OF WORK SOMEWHERE AAAAAAAAAAAAAAAAAAAAAAA Ebbene, quando si "risolve" un blocco, il miner riceve una quantità pari a 12.5 Bitcoin, oggi pari a circa 90000 euro (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 che si sono accumulate nel blocco precendente (quello che i miner stavano cercando di risolvere) vengono confermate, e impiantate nella blockchain. Per questo, una transazione è considerata conclusa quando si passano almeno 3 blocchi dopo quello in cui è stata iniziata. 3 perchè.....?? è così che funziona la blockhain bla b la

1.1.1 Gli effetti del mining sull'ambiente

eh è brutto lol, ma non quanto i banker skifosi xd

1.2 Wallets, addresses, seeds, keys: how Bitcoin is stored DIVIDERE IN SUBSUBSECIONS

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. While wallets are the software itself, they are not the "place" where bitcoins are stored. The coins are stored in addresses, a string of x 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. Bitcoin can be stored in two different ways: cold wallets and hot wallets. Cold: Hot: hot wallets are the most useful kind, as you can..... 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. New (as in.....)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.....

1.3 Come ottenere e 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.

1.3.1 Exchange

Il metodo più veloce e utilizzato è quello di acquistarlo su un sito di exchange (come si dice in ita??). 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 by far 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...)

1.3.2 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://nuiasbdiasnd.lol.

1.3.3 Mining

Come spiegato in precedenza, il processo di mining porta i miners a guadagnare criptovalute, che possono essere venudre (se parlassi pirma delle altre valute??) per btc, o soldi veri e propri. Nonostante i costi dell'equipaggiamento di minning e dell'elettrricità utilizzata, i miner ricavano comunque un profitto dai coin che guadagnano. Ovvio che per "the average Joe" il mining è "out of their league", ma è certamente un modo valido per ottenere dei coin

1.3.4 Vendere roba

Se si vendfe qualcosa su i nternet o in real live si può comunicare ai clienti che è preferibile accettare pagamenti in bvitoicnoin.

2 Le origini del Bitcoin e il suo obiettivo PE RPRIMA OCASà

nasce.... eprche..... Satoshi creò una valuta con numerosi pregi: ELENCO PUNTATO decentralizzata, anonima, veloce, ...?, universale Spiegare elenco puntato.

3 Non solo Bitcoin

Esistono numerosissime criptovalute. Il sito https://coinmarketcap.com ne lista X00. Ritengo indispensabile spendere almeno qualche pagina a discutere/?????? delle valute più rilevanti, perchè a common misconception is that Bitcoin is the only cryptocurrency. This is simply not true. Tutte le criptovalure che non sono Bitcoin prendono il nome di Altcoin, "alternative coin".

3.1 Ethereum

get vitalik on ze line xd

3.2 Litecoin

arise chickun lal

3.3 Monero

donkey kong

3.4 Nano

BEST COIN

3.5 Stellar?

idk much tbh smh

3.6 Bitcoin "hard forks"

btg btcp.....

3.6.1 Roger Ver e la truffa di "Bitcoin Cash"

bcash bcash xd

4 Bitcoin oggi

si sta usando un po', blabla

4.1 Lo stato attuale dell'adozione

Sempore più negozi, serivzi, droga.....

4.1.1 Il villaggio in Austria.. come si chiama?

è bellus

4.2 Il boom del 2017: cause e conseguenze

MOOON BOIS LAMBO LETS GO

4.2.1 La ricorrenza dei "crash" dei mercati

foto che compara, succede tante voplte, hodl godl podl.

4.3 Controversie

Il Bitcoin e le criptovalute in generale

5 Il futuro delle criprtovalute

Come si può vedere dalla figura, nel 2018 ci troviamo alla primissima fase dell'adozione di questa nuova tecnologia.