Bitcoin

Abstract

Need to be able to send money to a person directly without going through a central entity like a bank.

We need to prevent double spending.

Digital signatures do not solve this problem fully, checks if the info is coming from a verified source-> sign the document with a private key which can be verified the public key. However this does not prevent double spending as let's say we have a coin, we can sign the same copy of the coin twice and send it to different people.

We need to try to solve this problem in a pure P2P network.

Intro

Completely non reversible transactions are not really possible. Like every transaction is basically new.

In physical world everything is purely transactional, however if u communicate with a bank we have to share excessive info with them.

Everything boils down to cryptography.

We need to make it very difficult to add a fraudulent transaction.

Transactions

How do we maintain a chronological order of transactions-> we maintain a chain of digital signatures. Signature is formed using the private key, like the basis of cryptography is that it's computationally infeasible to decrypt the private key .

Each next transaction is formed by making a signature.

We form the sign using the our own private key and the public key of the next owner and the hash of previous transaction.

This does not solve the double spending problem though, we still need to solve the problem in such a way that the participants agree to a single history of order of the coin.

Also when we do a transaction we need to make sure we don't do any double spending and also the person who we are sending the coin to should also be sure no double spending has taken place.

Timestamp Server

We take a hash of a block of items to be timestamped, the block serves as a buffer. Whenever a node in a network gets a transaction it tries to add the transaction to a block, this block contains multiple such transactions.

Each block contains multiple transactions.

Each timestamp includes the previous timestamp in its hash.

ProofOfWork

Anyone can add chains to the block. These can contain fraud transactions. We need to prevent this or make it extremely different to do so.

We add a nonce to the block , the nonce has to be such that the hash of the block starts with a certain amount of zeroes.

Why 0?->Becuz ig when we do a Sha 256 hash of a value it is very hard to even get a single 0 in the hash, getting multiple 0s in the beginning will be super hard.

We have to keep iterating through the nonce which is a 32-bit number so it is large af till we get the required amount of zeroes.

This will require a decent amount of CPU work.

Since the block starts with a certain amount of zeroes , if you change a small thing in the block, the hash of the block will not start from zero and so people will not it is fraudulent also every subsequent block in the chain will also be affected.

Say u want to add a fraudulent transaction in the chain , from the point u add the fraudulent transaction u will have to go to every next transaction and try to recreate the nonce which requires a large amount of CPU power.

This is basically a concept of relying on CPU based voting instead of Ip based voting, as the more servers u have the more ips but cpu does not increase in such a manner.

Every node in the network will get the entire ledger , I get multiple chains , we treat the longest chain as the correct chain as it is more difficult to spoof that chain.

If we are the added fraudulent transactions we will need to have a lot of CPU power as we need to outpace the longest chain which is still growing and as subsequent blocks are added the chain the probability of an attacker caching up decreases exponentially as the honest nodes are minting blocks faster and adding to the chain.

Network

1. New transactions are broadcasted to all the nodes.
2. Each node collects these into a block.
3. Each node works in finding a proof of work for it's block.
4. When a node finds its proof of work it broadcasts the block to all nodes.
5. Node accepts the block only if all transa