How Bitcoin Works.

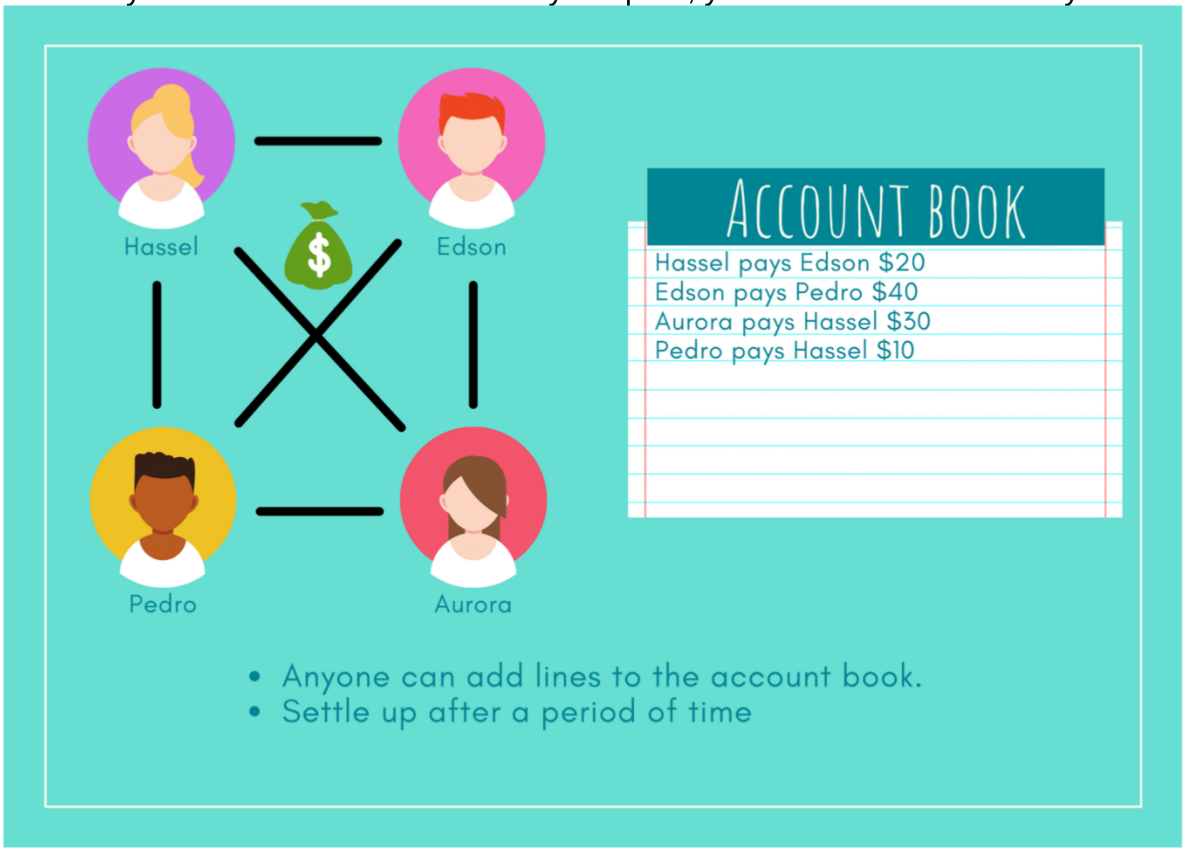
Nowadays, commerce on the internet as known as eCommerce has become an indispensable requirement for buying and selling products. The transactions needed to validate and process electronic payments are made almost exclusively for financial institutions. However, why is needed a trusted third party to validate transactions? In 2008, Satoshi Nakamoto propose a solution for this. He proposed an electronic payment system based on cryptographic proof instead of trust and a peer-to-peer network, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

Nakamoto's solution also proposed a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The currency used to make a transaction is known as Bitcoin.

Bitcoin is an electronic coin defined by a chain of digital signatures, with no government to issue it and no banks needed to manage accounts and verify transactions but there is a clever system of decentralized trustless verification.

To understand how bitcoin works, let's suppose that you and your friends have an account book where all write the information of payments, paying your share of the dinner bill and such. It can be inconvenient to exchange cash all the time, so decide to write in the account book all the payments you and your friends intend to make in the future, and these records will be something public and accessible to everyone, like a website where anyone can go and just add new lines. At the end of a period of time, i.e. every month, you and your friends look through the list of transactions and tally up everything.

- If you have spent more than you received, you put that money into the pot.
- If you have received more than you spent, you take that much money out

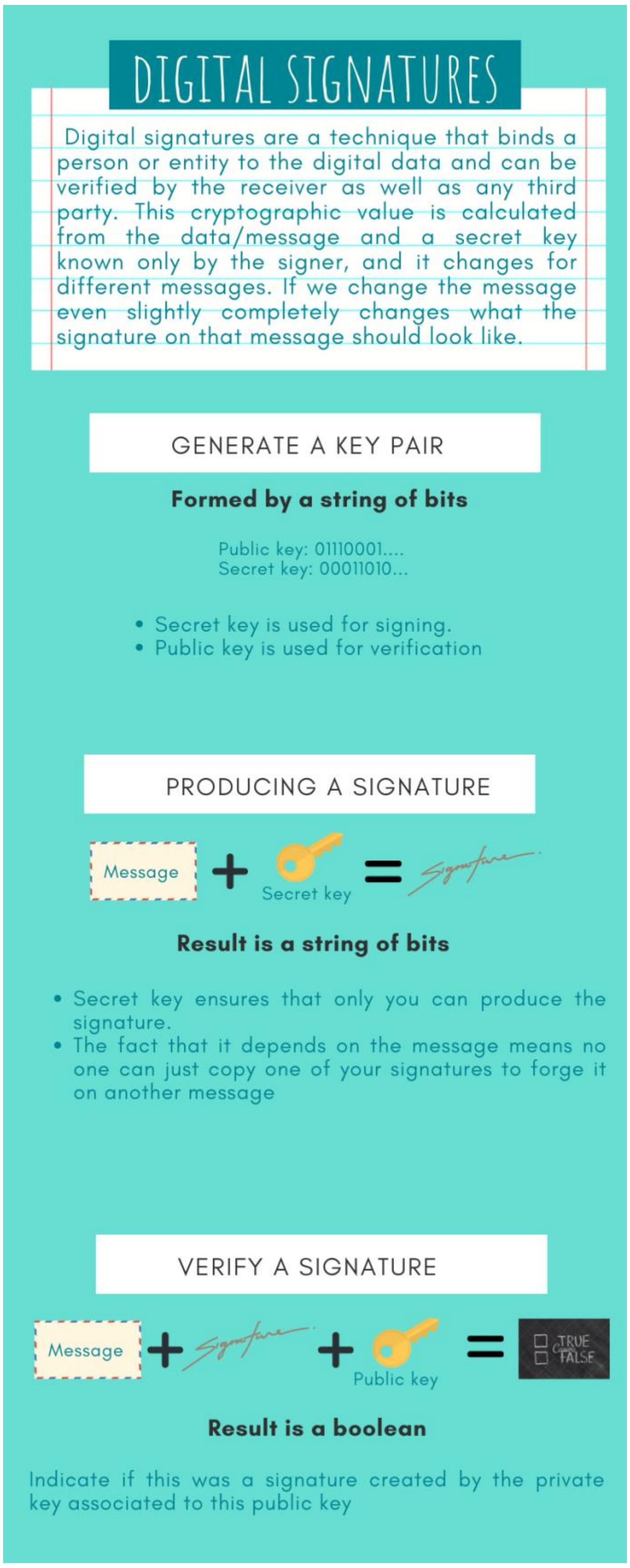


Hassel pays Edson $20
Edson pays Pedro $40
Aurora pays Hassel $30
Pedro pays Hassel $10

- Anyone can add lines to the account book.
- Settle up after a period of time

Protocol to add records to account book.

What is the problem with this? Well, if you public account book and anyone can add a line, how to prevent that anyone from going in and write a new register without approving? How are we supposed to trust that all these transactions are valid? The answer for these questions is given by cryptography and an important technique named *Digital signatures*. The idea is that the person who add a record to account book, it also must include a signature that proves that the other one has seen it, and approved of it.



DIGITAL SIGNATURES

Digital signatures are a technique that binds a person or entity to the digital data and can be verified by the receiver as well as any third party. This cryptographic value is calculated from the data/message and a secret key known only by the signer, and it changes for different messages. If we change the message even slightly completely changes what the signature on that message should look like.

GENERATE A KEY PAIR

Formed by a string of bits

Public key: 01110001....
Secret key: 00011010...

- Secret key is used for signing.
- Public key is used for verification

PRODUCING A SIGNATURE

Result is a string of bits

- Secret key ensures that only you can produce the signature.
- The fact that it depends on the message means no one can just copy one of your signatures to forge it on another message

VERIFY A SIGNATURE

Result is a boolean

Indicate if this was a signature created by the private key associated to this public key

Use of digital signatures

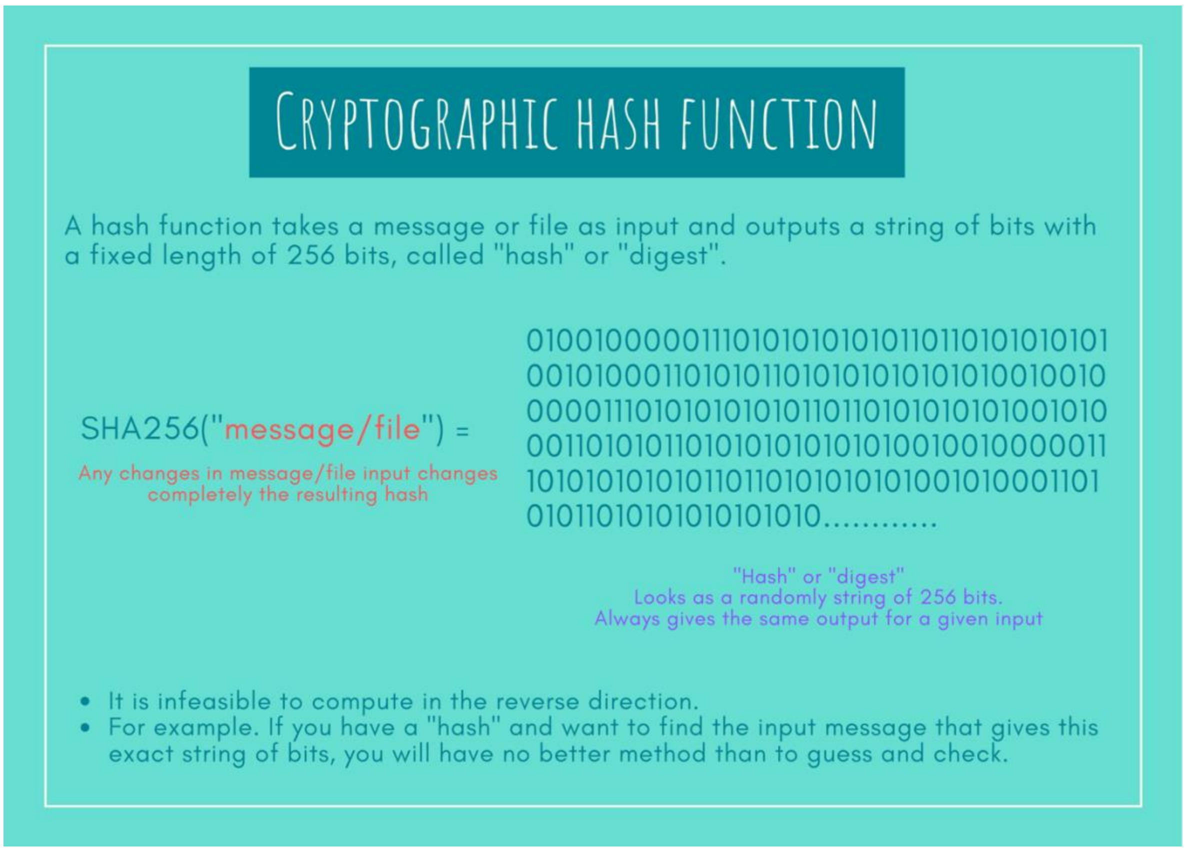
The signature that is added has a size of 256 bits and it should be infeasible to find a valid signature if you do not know the secret key. If a person wants to know or used a technique to try to forge the signature, there is no better strategy than just guessing and checking if random signatures are valid using the public key until you hit one that works, however, there are 2^256 possible signatures with 256 bits, and you would need to find the one that works. Based on this, when you verify a signature against a given message and public key, you can feel confident that the only way someone could have produced it is if they knew the secret key associated with the public key.

Once we ensure that only a transaction is added to the account book when includes a signature, it is necessary to prevent overspending, this means that a person spends more than the quantity available. To solve this, what you might do is start by having everyone pay a quantity into the pot, and have the first few lines of the account book will read the quantity available of everyone and do not accept a transaction when someone is spending more than they have available on the account book.

However, if we want to know if someone is overspending, means that it is necessary to know all the history of transactions to verify that a new one is valid, this is the key to removing the connection between account book and physical money, and to understand the core of Bitcoin and any other cryptocurrency. If everyone in the world uses this account book, you could live your whole life just sending and receiving money on the book without ever converting it to real money.

The history of transactions is the currency and is put in some public place, like a website where anyone can add a new record. But, we go back to the main problem of financial institutions, it requires a trusting central location to validate transactions. To remove that bit of trust, we will have everyone keep their own copy of the account book, to make a transaction you broadcast into the world for people to hear and record transactions on their private book. There is a problem here because now it is necessary to implement a protocol to ensure that everyone else received and recorded the same transaction in the same order.

The solution for this was presented in the original Bitcoin paper, which involves cryptographic hash functions.



CRYPTOGRAPHIC HASH FUNCTION

A hash function takes a message or file as input and outputs a string of bits with a fixed length of 256 bits, called "hash" or "digest".

SHA256("message/file") =

Any changes in message/file input changes completely the resulting hash

01001000001110101010101011011010101010101
00101000110101011010101010101010010010
0000111010101010101101101010101001010
00110101011010101010101010010010000011
101010101010110110101010101001010001101
0101101010101010101010............

"Hash" or "digest"
Looks as a randomly string of 256 bits.
Always gives the same output for a given input

- It is infeasible to compute in the reverse direction.
- For example. If you have a "hash" and want to find the input message that gives this exact string of bits, you will have no better method than to guess and check.

Cryptographic hash function.

Hash functions are used to prove that a particular list of transactions is associated with a large amount of computational effort without having to go through that same effort yourself. This is called a "proof of work". All the work is intrinsically tied to a specified list of transactions, if a transaction change, it would completely change the hash, so you would have to go through another billion guesses to find a new proof of work.

How does this solve our problem with our account book situation? Everyone is broadcasting transactions, we want a way for everyone to agree on what the correct ledger is and to have everybody trust whichever account book has the most work put into it. The way this works is to first organize a given account book into blocks, where each block consists of a list of transactions together with a proof of work. That is a special number so that the hash of the whole block starts with a bunch of zeros.

In the same way that a transaction is only considered valid if it is signed by the sender, a block is only considered valid if it has proof of work. Also, to make sure there is a standard way to order these blocks, we'll make it so that a block has to contain the hash of the previous block.

If you change any block or try to swap the order of two blocks, it would change the block after it, which changes that block's hash, which changes the next block, and so on. That would require redoing all the work, finding a new special number for each of these blocks that makes their hashes start with the bunch of zeros needed.
Because blocks are chained together like this, instead of calling account book, this is commonly called a "BlockChain". Now, this protocol allows anyone in the world to be a "block creator".

A "block creator" listen for the transactions being broadcast, collect them into a block, then do a lot of work to find the special number that makes the hash of this block start with the bunch of zeros, and broadcast out the block they found. To reward a block creator for all the work, when put together a block, they are allowed to put a special transaction at the top and this is called the "block reward".

A "block reward" is a special kind of transaction. It does not come from anyone, so it does not have to be signed. It also means that the total number of currencies in our economy increases with each new block. In the beginning, this reward was 50 bitcoin per block, and for every 210,000 blocks, that reward gets cut in half and because this reward decreases geometrically over time, there will never be more than 21 million bitcoin in existence.

Creating blocks is often called "mining" since it requires a lot of work, and it introduces new bits of currency into the economy. Miners are creating blocks, broadcasting those blocks, and getting rewarded with new money for doing so. In addition to the block reward, miners can also pick up transactions fees.

A transaction fee is a small quantity that will go to the miner of whatever block includes that payment. This is to incentivize miners to include the transaction you broadcast into the next block.

From the miners' perspective, each block is like a miniature lottery, where everyone is trying to guess the correct number that makes the hash of the block start with many zeros until one finds one and wins the reward for doing so.

Who everyone else who just wants to use the system to make payments, instead of listening for transactions they start listening for blocks being broadcast by miners, and updating their copy of the blockchain. If you hear two different blockchains with conflicting transaction histories, you defer to the longest one, the one with the most work put into it. If there is a tie, wait until you hear of an additional block that makes one longer.

So even there is no central authority, and everyone is maintaining their copy of the blockchain, if everyone agrees to give preference to whichever blockchain has the most work put into it, we have a way to arrive at a decentralized consensus.

When a new block is heard for a miner, they should not necessarily trust that new block immediately. Instead, they should wait for several new blocks to be added on top of it. If you still have not heard of any longer blockchains, you can trust that this block is part of the same chain everyone else is using.

In summary, the main ideas involved in this are:

- Digital signatures.

- The account book is the currency
- Decentralized
- Proof of work
- BlockChain

And this distributed account book system based on proof of work is how the bitcoin protocol works and many other cryptocurrencies.

Benefits.

- Bitcoin has user autonomy because its price is not linked to specific government policies. This means that users and owners of the cryptocurrency are in control of their money.
- Transactions are pseudonymous, this means that they are not completely anonymous, the transactions can be identified only by using a blockchain address. An individual can have multiple addresses, just as they can have multiple usernames and passwords for a single account.
- Bitcoin transactions are conducted on a peer-to-peer basis. The Bitcoin payment system is purely peer-to-peer, meaning that users can send and receive payments to or from anyone on the network around the world. Unless they are sending or receiving bitcoin from a regulated exchange or institution, the parties to a transaction do not require approval from an external source of authority.
- Bitcoin payments are mobile. Bitcoin users can pay for their coins anywhere that they have Internet access.
- Bitcoin transactions are irreversible. One of the characteristics of Bitcoin's blockchain is that it is immutable. Therefore, transactions using the blockchain are irreversible and cannot be amended by a third party, such as a government entity or a financial services agency. Also, it is not possible to file a charge-back for bitcoin sent to someone else. The only way to reverse Bitcoin transactions is by having the recipient send back the original bitcoin.
- Bitcoin transactions are secure. Bitcoin is not a physical currency. Therefore, thieves can't palm it off the holder. Hackers can steal a person's cryptocurrency if they know the private keys for the wallet. However, with proper security, it is technically impossible to steal bitcoin.
- Accessibility. Because users can send and receive bitcoins with only a smartphone or computer, Bitcoin is theoretically available to populations of users without access to traditional banking systems, credit cards, and other methods of payment.

Why bitcoin is a good idea?

When it was launched, Bitcoin was conceived as a medium for daily transactions. The idea behind a decentralized cryptocurrency was to eliminate centralized control of money from government agencies and ensure speedy processing of transactions. However, very few daily transactions are conducted using Bitcoin as a medium of exchange.
But the idea of an alternate currency, outside the purview of governments and federal agencies, is important. Some supporters like the fact that cryptocurrency removes central banks from managing the money supply since over time these banks tend to reduce the value of money via inflation

Other supporters like the technology behind cryptocurrencies, the blockchain, because it's a decentralized processing and recording system and can be more secure than traditional payment systems.

I think Bitcoin is a good idea because removes intermediaries and its pseudonymous design that eliminates the need for identification information for both parties. Both characteristics expedite transactions and remove unnecessary steps for transactions.