WHAT IS BLOCKCHAIN?

A blockchain is continuously growing list of records called blocks, which are linked and secured using cryptography.

Blockchain is a public record of transactions. It’s also distributed, so instead of one person controlling everything, there are thousands of computers around the world connected to a network, and these thousands of computers together come to an agreement on which transactions are valid.

Whenever someone makes a transaction, it is broadcasted to the network, and the computers run complex algorithms to determine if the transaction is valid.

This chain of linked transactions is known as the blockchain.

Distributed ledger technology (DLT) — It is an accounting system where the **ledger** (record of transactions) is **distributed** among a network of computers.

A peer to peer network is one in which two or more pc’s share data and access to device such as printers without requiring sever computer server software.

blockchain networks are often referred to as peer-to-peer networks.

Every blockcahin is copied to every computer in the network

So at its core, blockchain technology is a record-keeping tool.

What makes blockchain technology unique?

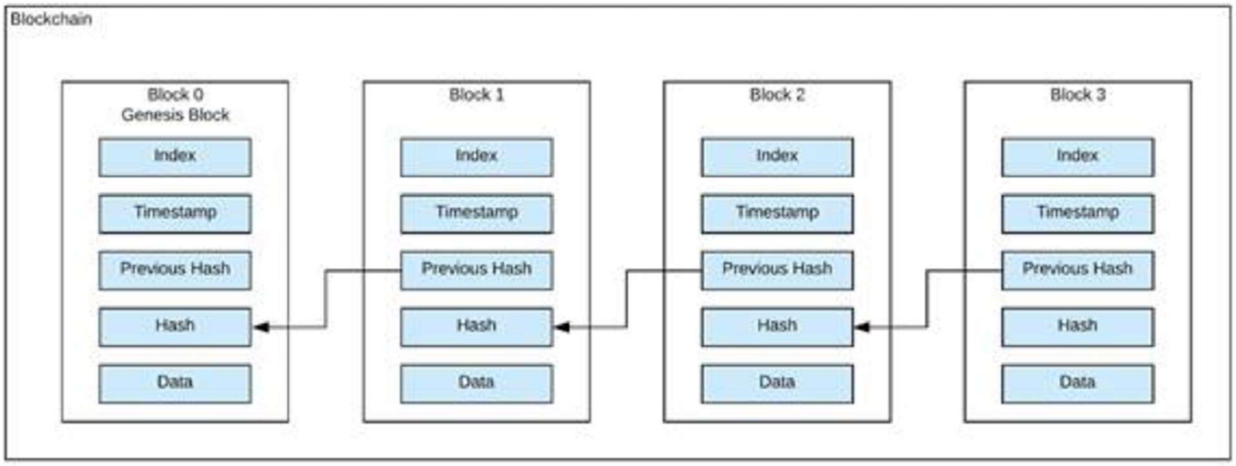
- **Decentralized:** Because blockchains are managed by a network of nodes rather than a central authority, they are fully decentralized. This prevents any one entity from having any control over the network.

- **Transparent:** Transactions on a blockchain are constantly being recorded and stored on the blockchain across nodes. This means that all participants can view all transactions on the network in real-time.
- **Immutable:** Blockchains are designed to enable permanent record keeping so that stored data cannot be altered after being added. This makes it an extremely stable and reliable record-keeping system.
- **Secure:** It is hard to change or destroy blockchains because of its distributed nature. For example, if someone hacked into one of the computers on the network and altered information there, the network would remain unaffected.
    - **No transaction cost** — The Blockchain carries no transaction cost. Passing information from A to B on the Blockchain does not require paying a third party for simply initiating a transaction on the blockchain.

The Blockchain is:

- **A time-stamped series of data** - this means that each piece of data has a time stamp on it.
- **Immutable or un-corruptable record of data** - this means that data on the blockchain cannot be altered.

- **Managed by a cluster of computers** — This means that the data on the blockchain is managed by millions of computers distributed worldwide.



Hashing Algorithms

Apply mathematical calculation on some kind of data and output is given as some hexdecimal.

A **cryptographic hash** (sometimes called ‘digest’) is a kind of ‘signature’ for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text.

{0-9, a,b,c,d,e,f}

64 character long, 2 power 256 possibilities of hash

- One way generate hash
- Deterministic --- length of output always same
- Digital finder print
- Fast computation
- Avalanche effect- make a little in text string whole hash changes
- Withstand collision- 1 in 60 million

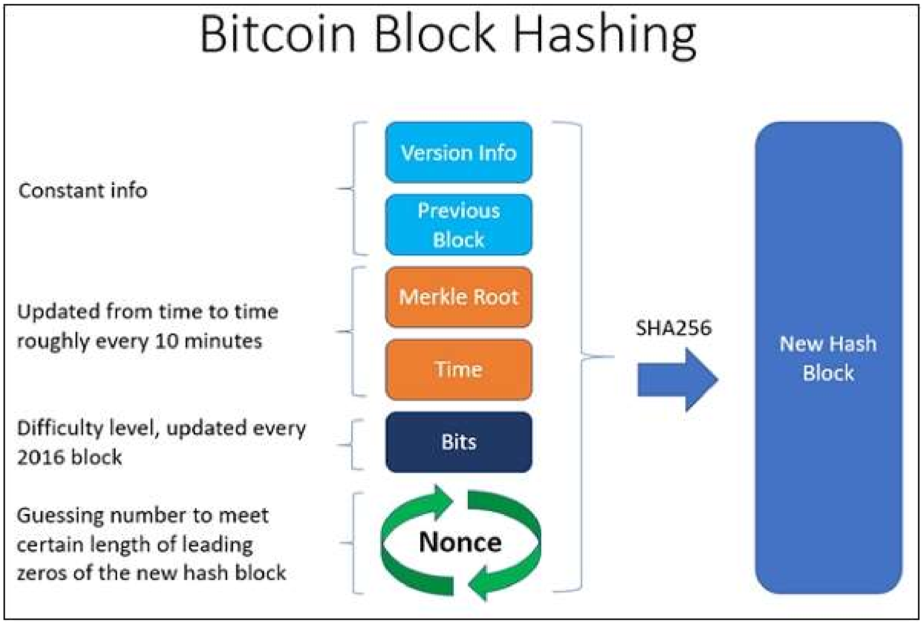
NONCE:

Nonce is the central part of this Proof of Work. The Nonce is a random whole number, which is a 32-bit (4 byte) field, which is adjusted by the miners, so that it becomes a valid number to be used for hashing the value of block. **Nonce is the number which can be used only once**.

Main focusing in mining a block and controls the hash i.e.

(block number + previous hash + Nonce number)

As the nonce value change the hash values changes.


Bitcoin Block Hashing
Constant info
Version Info
Previous Block
Updated from time to time roughly every 10 minutes
Merkle Root
Time
Difficulty level, updated every 2016 block
Bits
Guessing number to meet certain length of leading zeros of the new hash block
Nonce
SHA256
New Hash Block

Byzantine fault tolerance

Decentralized system,it’s a kind of pollong of saying yes like 51% attack

Consensus protocol :

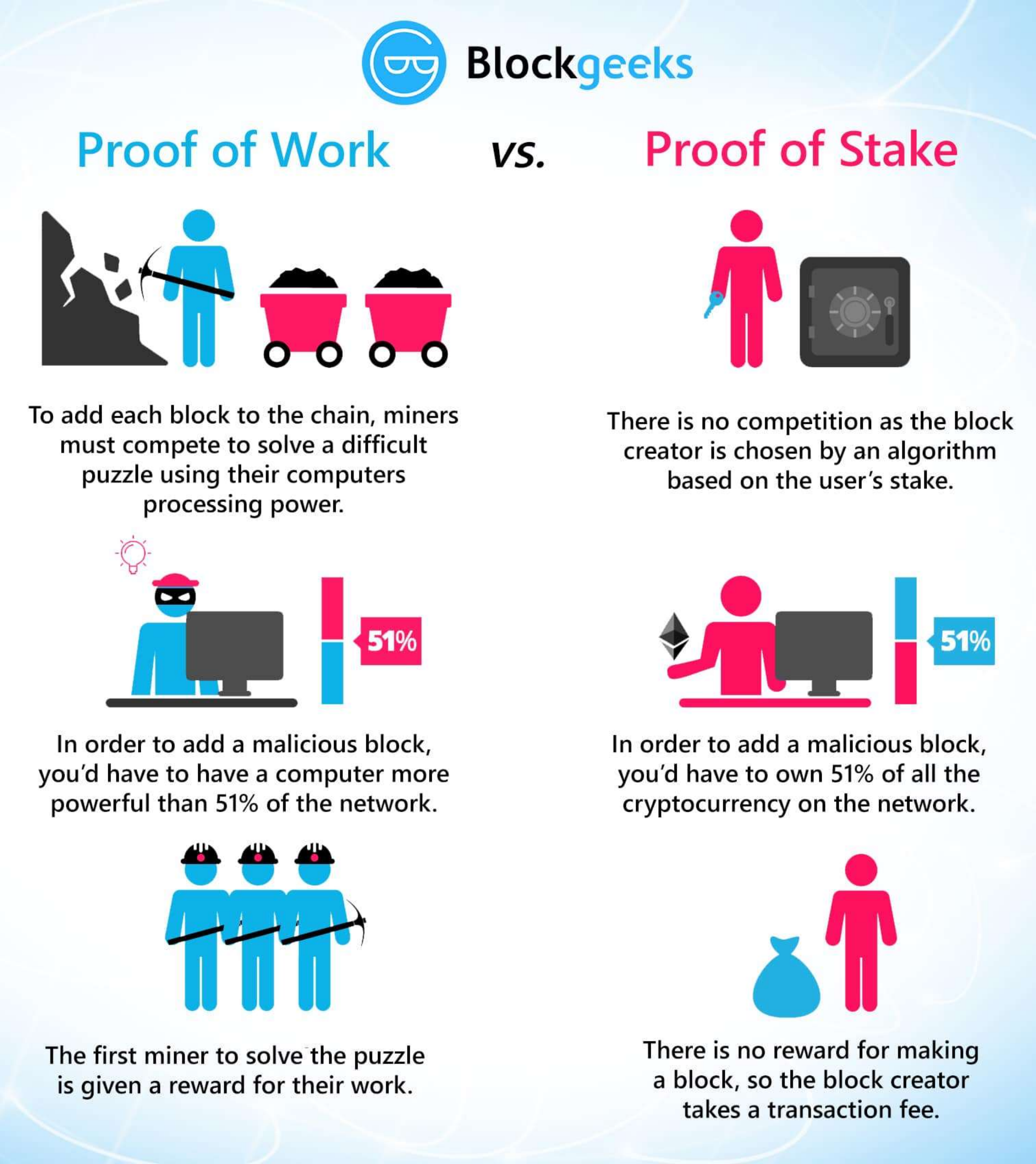
POW - proof of work ---- Bitcoin

POW is the number or pice of data that the miner have to find in order to mine a new block.

(hard to find but easy to verify).

POS (proof of state)-----ether there is selection algorithm work and a miner can mine a block if he/she selected.

Verification part of block mined is correct or not.



Blockgeeks

Proof of Work vs. Proof of Stake

To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.

There is no competition as the block creator is chosen by an algorithm based on the user's stake.

In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.

In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.

The first miner to solve the puzzle is given a reward for their work.

There is no reward for making a block, so the block creator takes a transaction fee.

miners help to confirm bitcoin transactions and provide security to the bitcoin network.

PoW is called mining because every time a new block is created, a new Bitcoin is minted. The computer that manages to create a valid block will inform the rest of the network and become the owner of the new Bitcoin and recipient of all transaction fees for that block. This block will be added to the blockchain and, provided that the majority of the nodes are honest, this chain will grow the fastest and become the longest chain.

Wallet :

Balance

Keys—1.public key -----sender (used for verify signature)

2. Private Key ----- only for user (used to generate signature)

Digital signature:

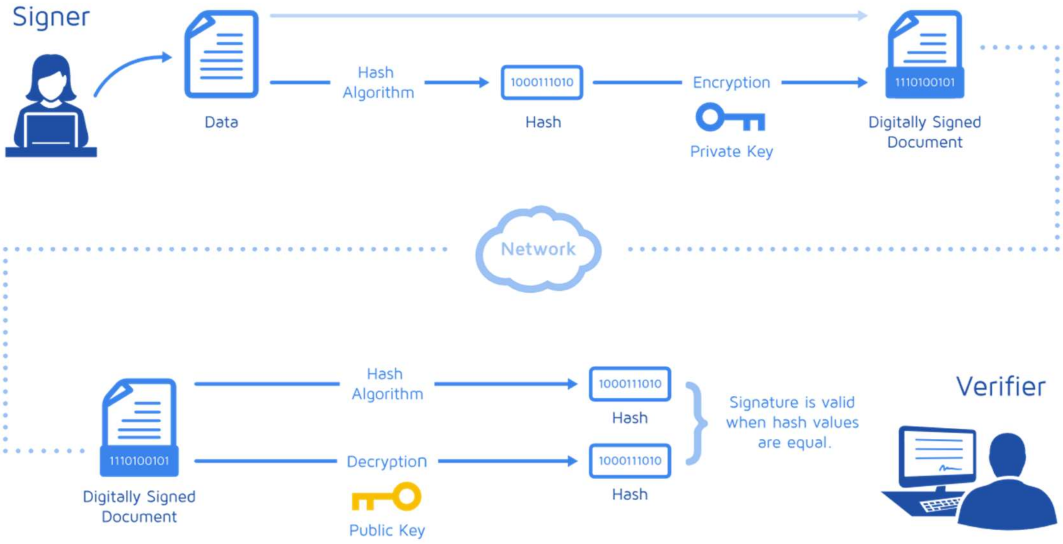
A digital signature (DS) is the detail of an electronic document that is used to identify the person transmitting data.

It is a mathematical technique used to validate the authenticity and integrity of a message.

It is like an electronic “fingerprint”.

PKI(public key infrastructure):

It is a standard, accepted format to provide the highest levels of security and universal acceptance.



Transaction:

All transaction in the network are atomic(full operation run or not at all)

Transactions are the object that capture the information behind the exchange of currency between two individuals.

Input --- timestamp, balance, public key, private key, address(sender,recipient)

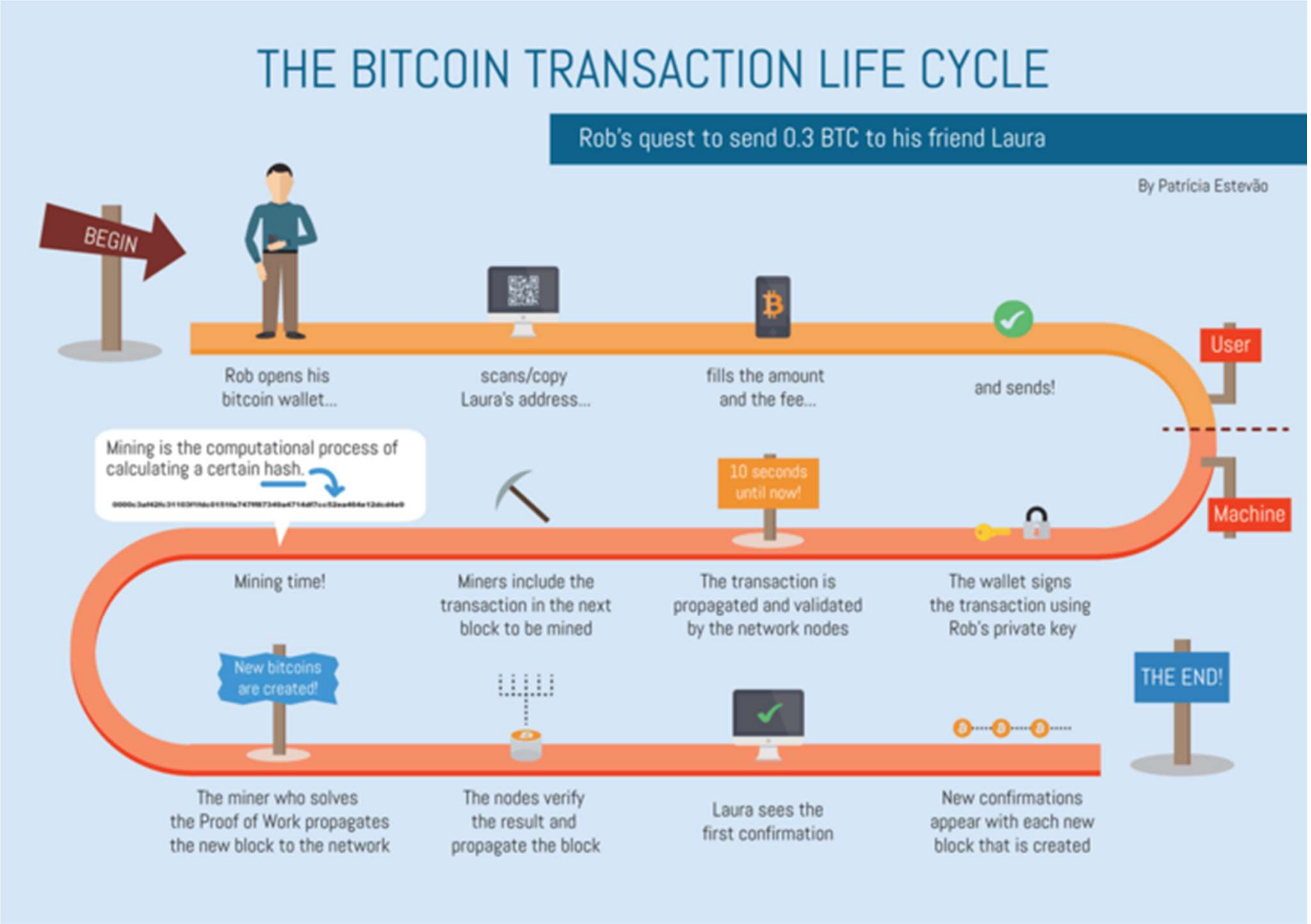
Output --- amount, address

The ledger is distributed across several nodes, meaning the data is replicated and stored instantaneously on each node across the system. When a **transaction** is recorded in the **blockchain**, details of the **transaction** such as price, asset, and ownership, are recorded, verified and settled within seconds across all nodes.

Transaction pool:

Transaction pool is the place where contains all of unconfirmed transactions. Transaction pool is stored on a special device and its contents can be accessed, observed in real time.

It is a data structure which will collect the transaction that are created by wallets's in the network.(array/map/graph)


THE BITCOIN TRANSACTION LIFE CYCLE
Rob's quest to send 0.3 BTC to his friend Laura
By Patrícia Estevão
BEGIN
Rob opens his bitcoin wallet...
scans/copy Laura's address...
fills the amount and the fee...
and sends!
User
Machine
Mining is the computational process of calculating a certain hash.
10 seconds until now!
Mining time!
Miners include the transaction in the next block to be mined
The transaction is propagated and validated by the network nodes
The wallet signs the transaction using Rob's private key
New bitcoins are created!
THE END!
The miner who solves the Proof of Work propagates the new block to the network
The nodes verify the result and propagate the block
Laura sees the first confirmation
New confirmations appear with each new block that is created

All transactions in Transaction pool have the different transaction fees, so the miners can look for the transaction that has the highest fee.(POW)

Forks:

Hard forks-changes the consensus rules (i.e blocksize,mining algo)

Soft fork – software update, it is a change of rules that still creates new block recongnized as valid by the old software.

Smart contracts:

Lines of code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met.(Immutable and distributed

)

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

A *smart contract* is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a *contract*. Smart *contracts* allow the performance of credible transactions without third parties.

One of the best things about the blockchain is that, because it is a decentralized system that exists between all permitted parties, there’s no need to pay intermediaries (Middlemen) and it saves you time and conflict. Blockchains have their problems, but they are rated, undeniably, faster, cheaper, and more secure than traditional systems, which is why banks and governments are turning to them.