Blockchain

Distributed Secure Database

Consists of strings of blocks each one record a data that's been encrypted and given a unique identifier called a hash.

Mining computers validates a transcation and add them to the blocks they are building and then broadcast the completed block to other nodes so that all have a copy of the database because there is no centralized component to verify the alterations to database The blockchain depends upon a distributed consensus algorithm in order to make an entry

On to the blockchain database, all the computers have to agree about its state so that no one computer can make an alteration without the consensus of others. Once completed a block goes into the block-chain as a permanent record, each time a block gets completed a new one is generated.

There are countless blocks in a blockchain and all connected to each others by links in a chain in proper linear chronological order

Blockchains are designed so that transcations are mutable meaning they cannot be deleted. each block contains a hash value that is dependent upon the hash of the previous block so they are all linked together meaning if one is changed then all the other blocks linked to it going forwards will be altered, this works to make

the data entered tamper proof.

Blockchain technology works to create a permanent and secure database, this makes blockchain suitable for the storage of a record or transcation that involves valueor in some way it needs to be a secure and trusted source of information.

These secure distributed records are called distributed ledgers. It is a consensus of replicated shared and synchronized digital data geographically dispersed across multiple sites, countries or institutions without centralized administration., being mainted by a distributed network of computers.

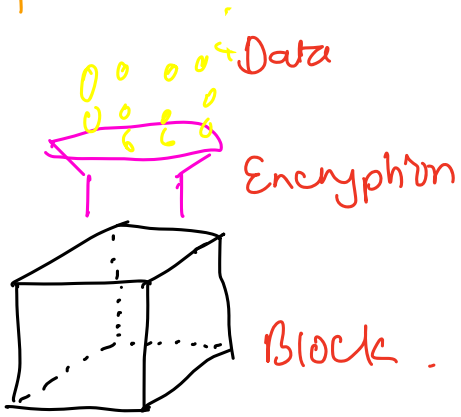
Second Generation Blockchains offers the possibility to automate the workings of these networks through smart contracts. Smart

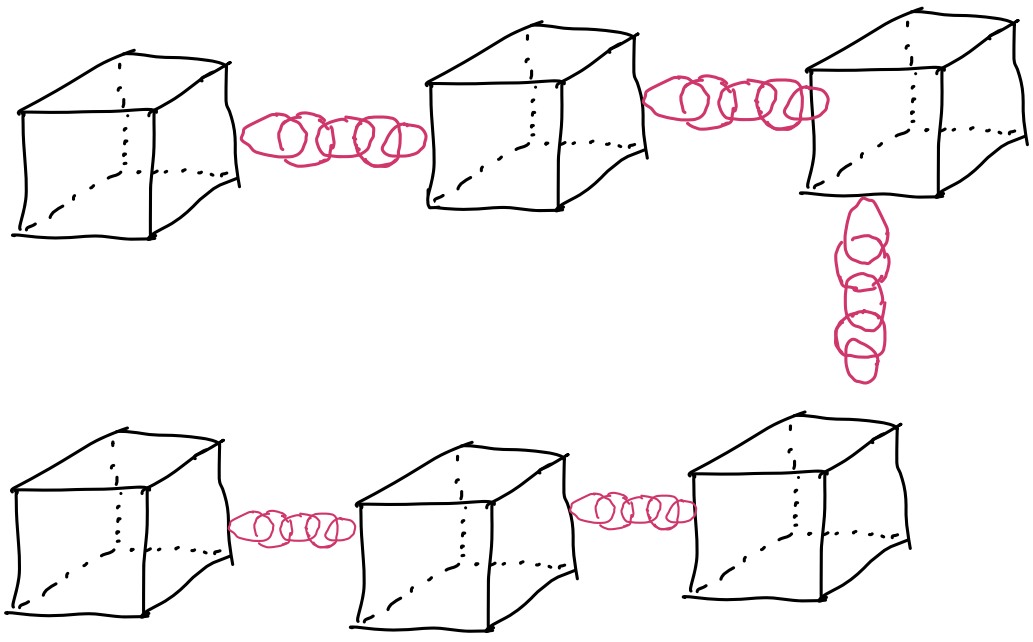
contracts are computer code that is stored inside the block-chain which encode contractual agreements ; these smart contracts are self executing contracts with the terms of the agreement or operation directly written into line of codes which are stored and executed on the block-chain

[Discovery, valuation, transfer of all discrete unit of value and the development of distributed organizations via token market systems.]

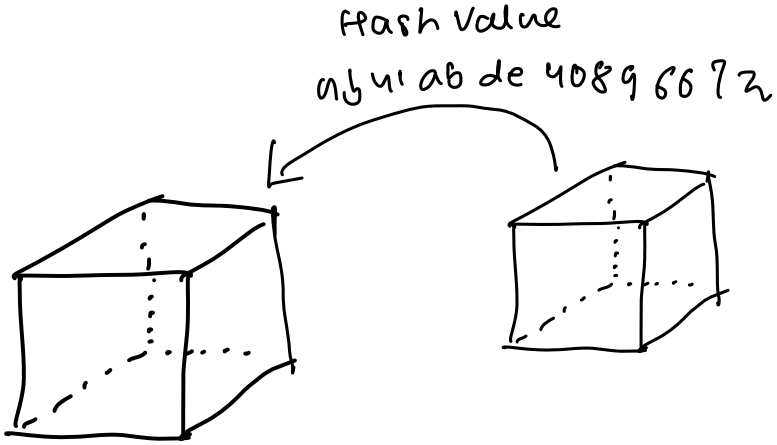
Tokenomics visual aspect.

Blockchain is a set of protocols and cryptographic methods that enable a network of computers to work together to securly record data within a shared open database.





Linked and secured by crypto-graphy.



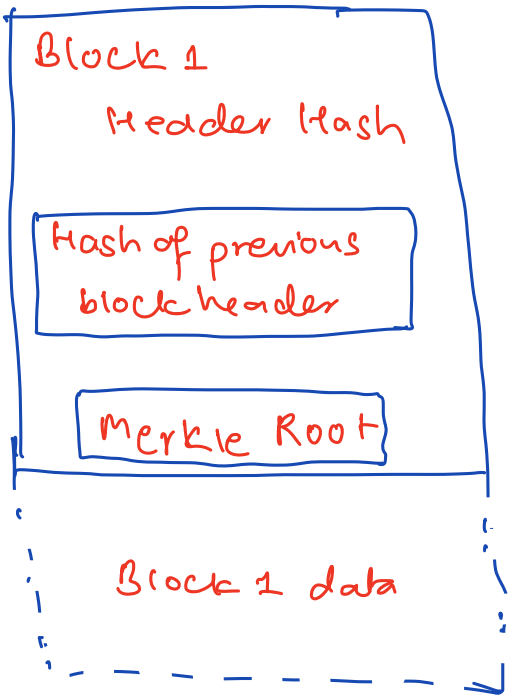
Database stores information in blocks, which are linked together through hash value. With enmies to this database being made by computers that all have a copy of the database and all must come to consensus about its state before they can update it

Blocks

Mining

Consensus

Blocks.



New Blocks are formed as participants create new data or wish to update the existing data, these blocks are encrypted and given a hash value that represents a unique identifier of the data within that block. This hashing works by standard algorithm being run over the blocks data to compress it into a code which is called the hash which is unique to that document no matter how large the file or what information contained. It is compressed into a 64 character secure hash, this hash value can be recalculate from the underlying file confirming that the original contents have not changed but the reverse

is not possible. (given the hash value. you cannot recreate the blocks data contained within it which is encrypted)

Block-chain security methods include the use of public key cryptography. A public key which is a long random looking string of numbers is an address on the block-chain.

Value tokens sent across the network are recorded as belonging to that address, a private key is like a password that gives its owner a access to their digital assets or the means to otherwise interact with the corresponding data. A public key is associated with the private key so that anyone can make an encrypted transaction to the public key address but that encrypted message can only be deciphered with the private key that corresponds to that public key in such a way effective Security only requires keeping the private key private. The public key can be openly distributed

Proof of work.

It describes a system that requires a not-significant but a feasible amount of effort usually by requiring computer processing time.

Miners compete to add the next block in the chain by racing to solve a very difficult cryptographic puzzle; the first to solve the puzzle wins the lottery as a reward for his or her efforts the miner receives the small amount of newly minted bitcoins and a small transcation fee. The consensus algorithm like bitcoins proof of work functions to ensure that the next block in the blockchain is the one and only version of the truth and it keeps powerful adversaries from derailing the system.

Block.chains are trying to create a secure trusted, shared database and they do this through encryption and hashing proof of work and network consensus. The hashing and linking of blocks makes it difficult to go back and change a previous block once it's entered. Proof of work system intentionally makes it computationally more difficult to alter the database thus making it extremely difficult to alter all the blocks

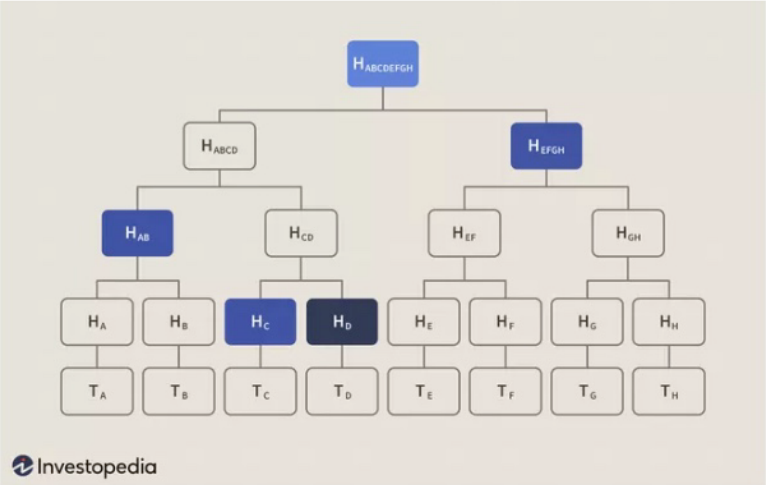
Small transcations are off-chain basis using lightning method. not recorded in the main ledger.

Merkle Tree → a binary tree

↳ for authentication.

It is useful because it allows users to verify a specific transactions without downloading the whole block-chain (over 321 Gb at the end of 2021)

The Merkle tree is useful because it allows users to verify a specific transaction without downloading the whole blockchain (over 350 gigabytes at the end of June 2021).[4] For example, say that you wanted to verify that transaction T_D is included in the block in the diagram above. If you have the root hash ($H_{ABCDEFGH}$), the process is like a game of sudoku: you query the network about H_D, and it returns H_C, H_{AB}, and H_{EFGH}. The Merkle tree allows you to verify that everything is accounted for with three hashes: given H_{AB}, H_C, H_{EFGH}, and the root $H_{ABCDEFGH}$, H_D (the only missing hash) has to be present in the data.



Transcation- ledger blockchain - BTC.

Timestamped append-only log → Auditable database

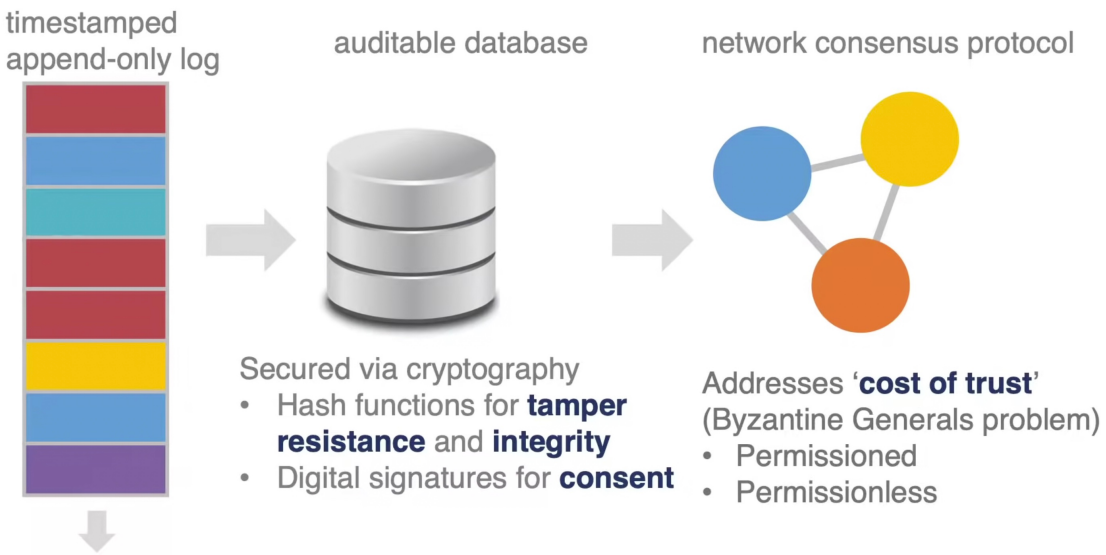
Blocks are added in every 10 minutes.
7sec for Eth.

Secured via cryptography

→ Hash functions for tamper resistance and integrity

→ Digital signatures for consent
consensus for agreement.

Blockchain Technology



Merkle Tree - Way to compress data and sort through that data.

Bitcoin - Technical Features

→ Cryptographic Hash Functions

→ Timestamped Append-only logs (Blocks)

→ Block Headers and Merkle Trees

→ Assymetric cryptography and Digital Signatures

→ Addresses

→ Consensus through Proof of work.

→ Network Nodes

→ Native Currency.

→ Transcation Inputs and Outputs

→ Unspent Transcation output (UTXO)

→ Scripting Language.

3.25 BTC to mine a block

Cryptographic Hash Functions

→ Digital fingerprints for Data.

General Properties.

- Maps input x of any size to an output of fixed size - called a 'hash'.
- deterministic : Always the same Hash for same x.
- Efficiently computed

Cryptographic properties

- Preimage resistant (one way) : infeasible to determine x from Hash(x)
- Collision resistant : infeasible to find and x and y where Hash(x) = Hash(y)

Can you break the hash cryptograph SHA 256?

→ Bitcoin could transition

(Quantum Computing)

↓

chances for hash functions to collide

Avalanche effect: change x slightly and Hash(x) changes significantly.

Puzzle friendliness: knowing Hash(x) and part of x it is still very hard to find rest of x.

Hash functions: pointers for different blocks on the BTC.

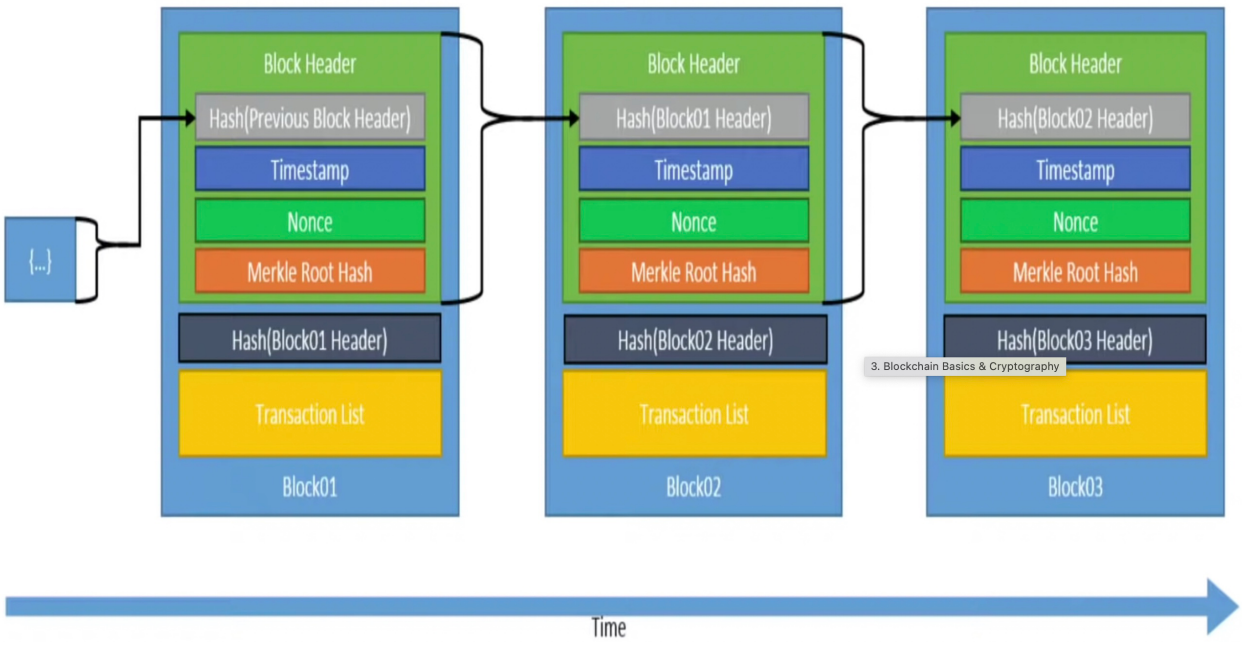
Bitcoin Hash Functions:

→ Header and Merkle Trees - SHA256

→ Bitcoin Addresses - SHA256 and RIPEMD160

Why two?
If one of them is broken, it's less likely the other one will broke too.

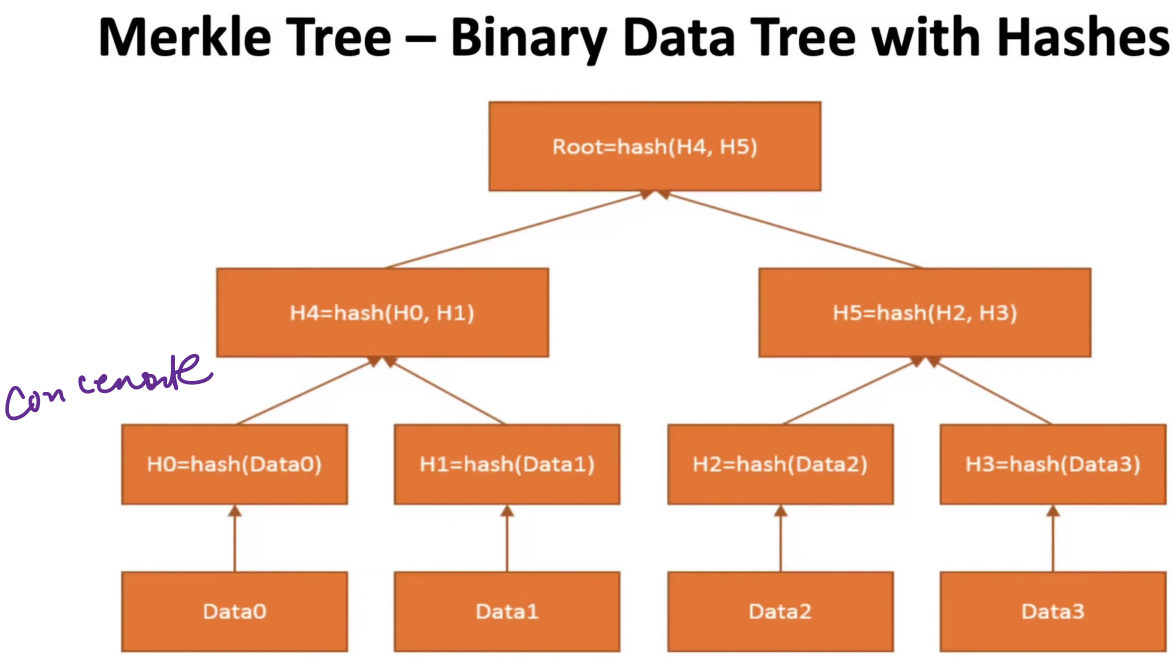
Timestamped Append-only Log - Blockchain



Merkle Root Hash

Lway to grab alot of transcations.

Nonce → no. of ones



Merkle roots are a very efficient way to take thousands of transcations, store it up, have one spot.

Hash functions are basically a way to compress a lot of data, have a fingerprint, make sure that it's basically commitment.

Private / public key

In cryptography, it's a way to kind of scramble information.

Symmetric cryptography → same keys used in both side.
to decrypt info.

Asymmetric cryptography → private / public key.

Private key is based on the random number.

Elliptine curve.

Digital signature was created from the private key. and the public key was created from the private key.

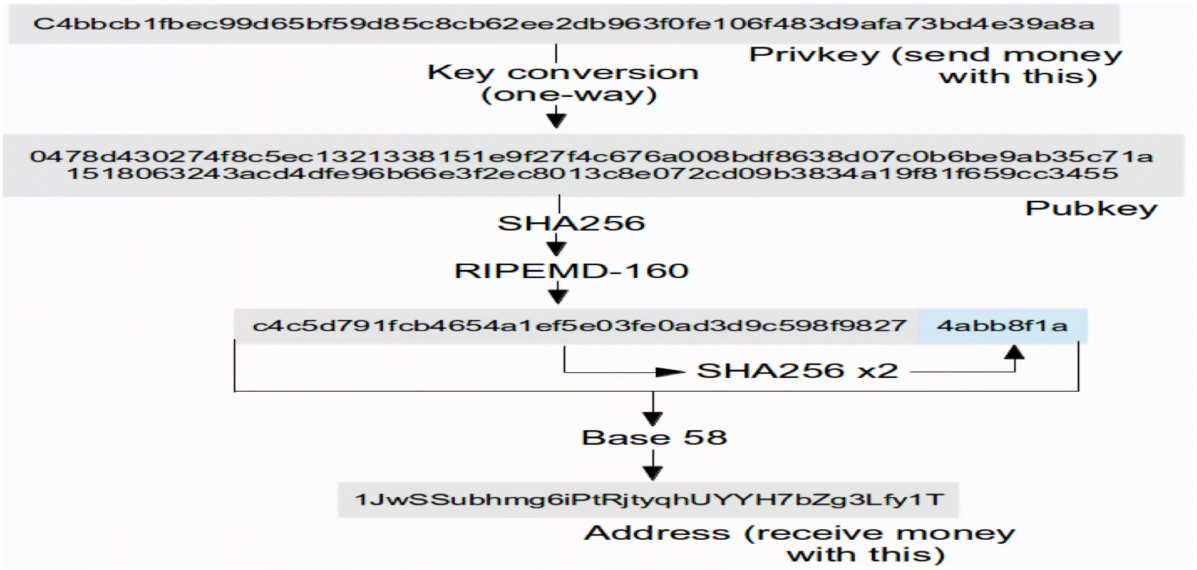
Asymmetric Cryptography & Digital Signatures

- Digital Signature Algorithms
  - Generate Key Pair - Public Key (**PK**) & Private Key (**sk**) - from random number
  - Signature – Creates Digital Signature (**Sig**) from message (**m**) and Private Key (**sk**)
  - Verification – Verifies if a signature (**Sig**) is valid for a message (**m**) and a Public Key (**PK**)

- Properties
  - Infeasible to find Private Key (**sk**) from Public Key (**PK**)
  - All valid signatures verify
  - Signatures infeasible to forge

- Bitcoin Digital Signature Function
  - Elliptic Curve Digital Signature Algorithm (EDCSA) … y2 = x3 + 7

Bitcoin Addresses



The Byzantine Generals Problem

Orphan blocks / stale blocks / worthless info.

↓

longest to 2/3 blocks.

memory.

Bitcoin Proof of work Difficulty

→ Targets 10 minute average block generation time.

→ Defined by the # of leading zeros Hash output requires to solve proof of work.

→ Adjusts every 2016 blocks - about every 2 weeks.

Genesis block - first block in Jan. of 2009.

Network.

Full Nodes - store full Block-chain and able to validate all transactions

Pruning Nodes - Prune transactions after validation and again.

Lightweight Nodes - Simplified Payment verification (SPV) nodes - store Block-chain header only.

Miners - Performs Proof of work & Create new blocks - do not need to be a full node.

Mining Pool Operators

Wallets - Store, View, Send and receive transactions & create key pairs.

Mempool - Pool of unconfirmed (yet validated) transactions

locktime
↳ when the transaction can happen.

How transactions are validated?

Input - Output = fee.

Input = Output.

Unspent Transactions Output.

dust

↳ Separate database that is not in the Bitcoin blockchain.

Bitcoin Script