Blockchain architecture

Application a presentation layer

Smart Contract Chain code dApp [illegible]

Consensus layer

pow pos dpos pOET pBFT

Network layer

peer-to-peer (p2p)

Data layer

Data Structure

Digital Signature Container Services Messaging

pow: proof of work

NFT: ~~proof of Stake~~ Non-Fungible Token

poS: proof of Stake

DpoS: delegated proof of Stake

pOET: proof of Elapsed Time

pBFT: practical Byzantine Fault Tolerance

Consensus layer: Only Validated transactions are added to the blockchain

Application layer: ~~ex~~ wallet, browsers, NFT platform, DeFi App.

Here Storage is decentralized

CAP theorem: known as Brewer's theorem is states that in distributed data stores.

- Consistency: All nodes have current, single & identical copy of data.
- Availability: Nodes are up, Accepting request & respond when required
- partition Tolerance: System continue to operate despite network failures.

Why Consensus is a hard problem

- Copies are consistent
- Delay: can Affect TX order
- Network partition
- ~~Node~~ crashed
- Corrupt node.

- Definition (Cryptographic hash function)

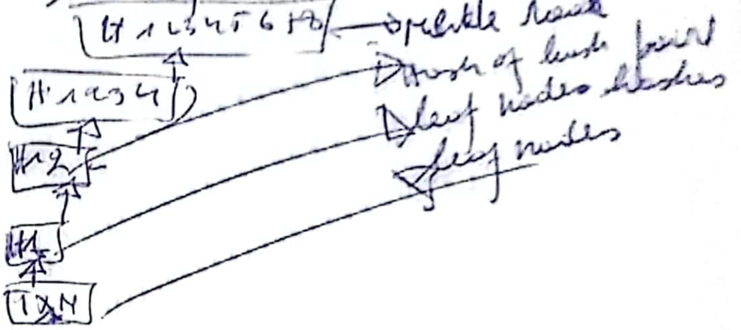
↳ An efficiently computable function, $H: \mathcal{M} \Rightarrow T$, where $|M| >> |T|$

Key/bytes → $\overbrace{\text{Hash value}}^{\text{32 bytes}}$ $T: \{0,1\}^{256}$

- Definition (Collision)

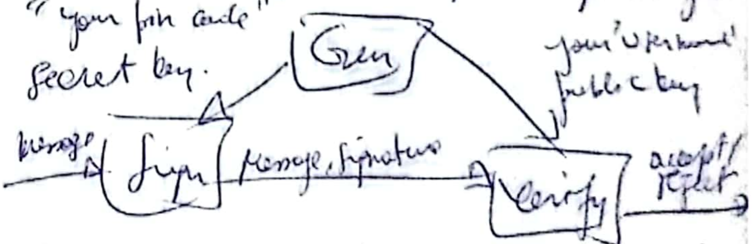
A Collision for $H: \mathcal{M} \Rightarrow T$, is a pair $x \neq y$ such that $H(x) = H(y)$

Merkle tree is a data structure in which each leaf node is a hash of block of data and each non-leaf node is ~~[illegible]~~ a hash of its children!



Digital Signature Scheme is Triple of Algorithms

- Gen(): Output a key pair
- Sign (sk, msg): outputs signature σ
- Verify (pk, msg, σ): outputs 'accept' or 'reject'



A consensus Algorithm: is a procedure through which all the peers of the blockchain network reach a common agreement about the present state of the distributed ledger.

Currencies using pow	Currencies using pos
Litecoin Ethereum Monero Coin Dogecoin	Peercoin NXT Ethereum (Casper Update)

→ miner must complete to solve difficult puzzle.

pow	pos — zero competition
there is reward	No reward
51% Computing	

mining : is the only way new bitcoin are created in the bitcoin system.

After a node creates a block, it will attempt to make it final by propagating it to all other nodes in the network.

Bitcoin mining : is a process of solving the pow puzzle and selecting the next valid block in way that is undisputed and helps achieve consensus on the current blockchain state.

- Bitcoin uses the Hashcash pow Algorithm for its mining.

$$\text{Difficult} = \frac{\text{Highest-Target}}{\text{Current-Target}}$$

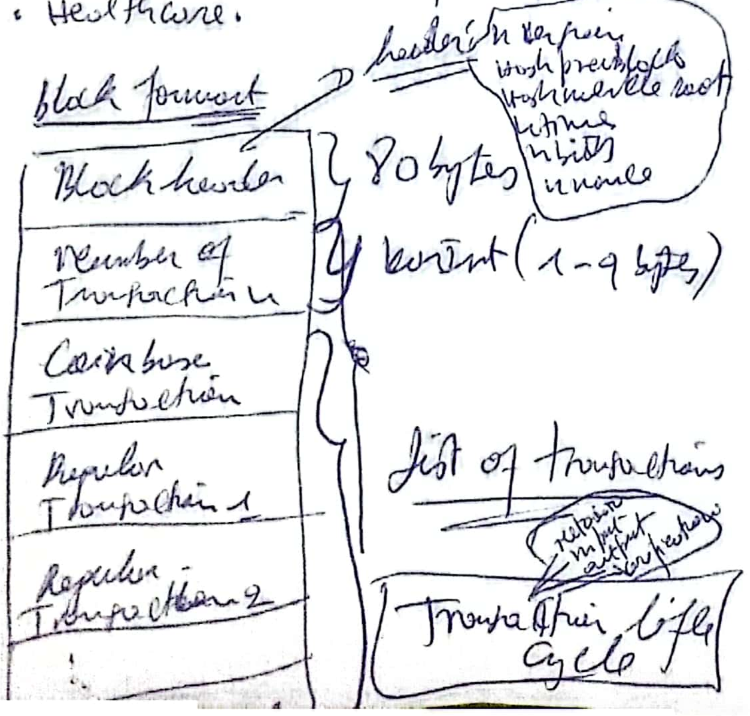
Smart contract : IS self-executing contract btn agreement btn buyer and seller being directly written into lines of codes.

Benefit of Smart contract

- Speed, efficiency and Accuracy : is digital & Automated.
- Trust and transparency : No third party involved.
- Security : record are encrypted.
- Savings : Remove needs of intermediaries

Application of Smart contract

- Government : voting system
- Management : Automated system, single ledger as source of trust.
- Supply chain : Automates tasks & payment
- Automobile : Insurance company can be connected for claim.
- Real estate : No needs of brokers.
- Healthcare.



Blockchain

IS open, distributed ledger that can record transaction btn two parts efficiently and in verifiable and permanent way without the needs for a central Authority.

key characteristic of blockchain

- open : Anyone can Access
- distributed or decentralised : No under control
- efficient : fast & scalable
- verifiable : Everyone check validity info
- permanent : Transactions done are persistent.

types of blockchain

- public blockchain : Accessed by any one ex: Bitcoin
- private blockchain : closed network, exclusively to Authorised users ex:
- Consortium blockchain : A network controlled by a group of entity or organization

Distributed system : are a computing paradigm whereby two or more nodes work with each other in a coordinated fashion to achieve a common outcome.

Node is a computer (or device) Connected to the blockchain network.

Disadvantages of traditional transaction

- Cash used only in low amount transaction locally
- Huge waiting time in processing of transactions
- Needs for third party for verification & execution transaction makes process complex.
- If central server like bank is compromised, the whole system is affected including the participants.
- Organization doing validation charge high process thus making the process expensive.

Building Trust block chain,

5 Attributes of blockchain

- Distributed : Ledger is shared & updated
- Secure : No unauthorized access
- Transparent : Every node has a copy of data
- Consensus-based : All participant must agree that transaction is valid
- Flexible : Based on a certain condition to be written into the platform.

Transaction life cycle

1. A sender sends a transaction using wallet software
2. wallet software signs transaction using sender private key
3. Transaction is broadcasted to bitcoin network using flooding algorithm
4. mining node include this transaction in next block to be mined.
5. mining starts once a miner which solve the pow problem broadcasts the newly mined block to the network
6. Nodes verify the block and propagate, and confirmation starts to generate
7. Finally, confirmation starts to appear in the receiver's wallet and approximately six confirmations, the transaction is considered finalized and confirmed.

Transaction Structure Contains:-

- Metadata: contain some value such as size of transaction, nbr of input and output, hash of transaction, locktime field.
- Input: Each input spends a previous output. each output is considered Unspent Transaction Output (UTXO)
- output: Have only two fields; first contain amount of satoshis, second is locking script, contain conditions needed to be met in order for output to be spent.
- Verification: performed using bitcoin's Scripting language.

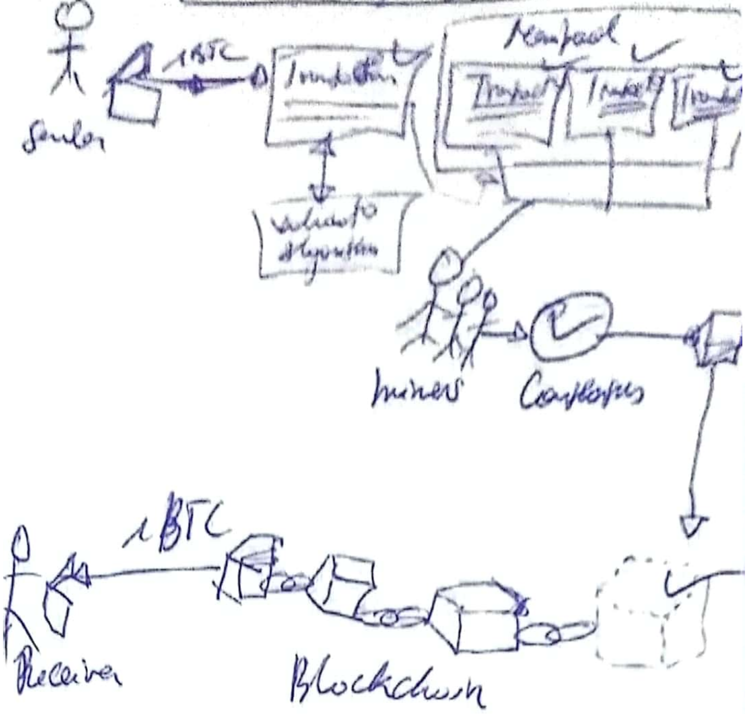
Metadata: - Transaction hash
- Housekeeping
- Not valid before
- Housekeeping

Input: - previous Transaction
- signature
- More inputs

Input address: - script sig
- script pubkey

Output: - output value
- Recipient address
- more outputs

Bit coin life cycle



1. Sender create transacts
2. Sender wallet validate the transacts
3. Transacts is sent to mempool
4. Miners get the transacts from mempool & start mining block using consensus Algorith.
5. After block is fully mined, It is added to a network.
6. Chain validates the new block and every peer in network will get the blockchain with the new block added.
7. finally, the Receiver get your BTCs

~~pool~~ Mempool: is where transactions stay until the miner is Ready to get them.

Application of Block Chain Scripts

- Escrow Transaction
- Green address
- Efficient micro-payment
- Lock Time
- Smart Contract.

Script

Forth

Similarities

Field way outcome bitcoin executed

① Execute successfully with no error, in which case the transaction is valid

② If there is any error, the transactions will be invalid and shouldn't be accepted into the block chain.