12/10/2023

=Blockchain Council=

- Certified Blockchain Expert -

1) Origin of the Blockchain

→ Electronic Systems and trust

• Before blockchain, the idea of cryptocurrency and the systems reliable to operate that currency was just a dream. The internet was required to be distributed, reliable and it needed to be used by almost all of the population as it digitally connects the world together.

• The development of TCP IP networking architecture made a huge impact on the usage of the internet. It established the standard for communication such as HTTP, which is used to provide web browsing and SMTP, which is an electronic mail delivery service.

The system always required two different types of trust:

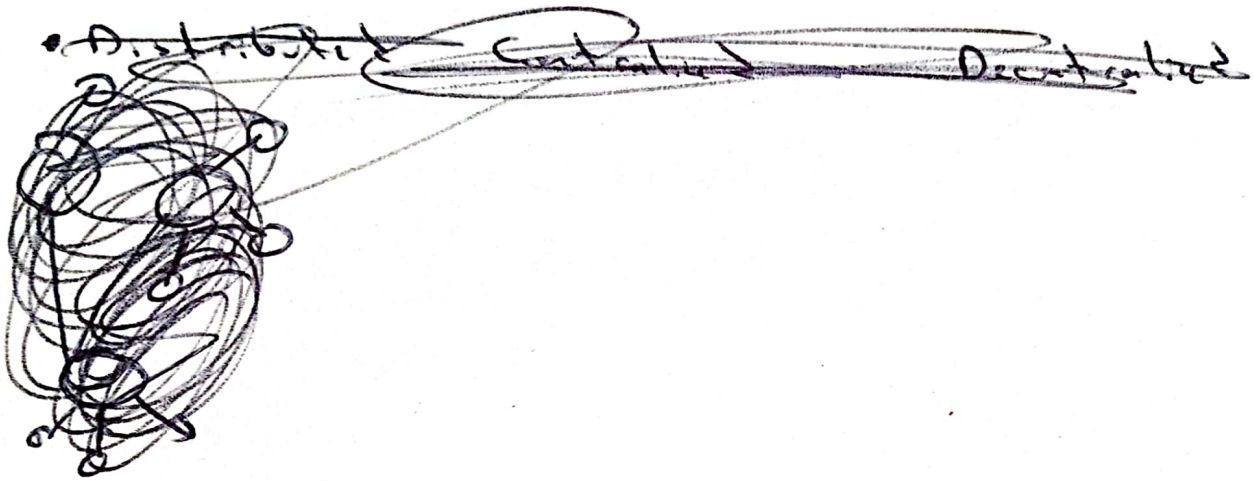
1) Intermediary Trust: Person who is relied on to make relations and fair decisions

2) Insurance Trust: A third party trust.

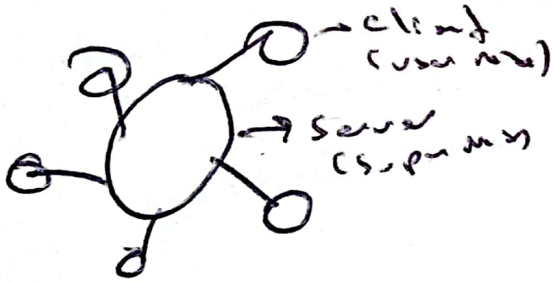
→ Trust is never stable in the financial world

(2008 crisis)

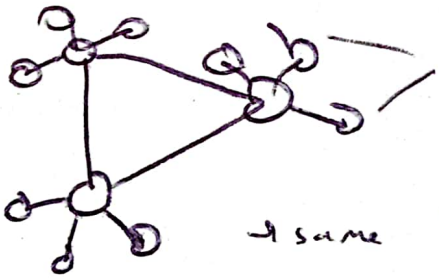
→ This is one of the main reasons in the pile of events that lead to the creation of the mighty digital currency BITCOIN.



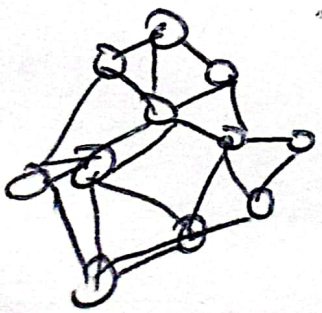
Centralized Arc



Decentralized Arc



Distributed Arc



No super nodes/

No central owner

→ users have the same level of data access

Centralized Architecture

Advantages:

→ It is simple for deployment

→ The development time is relatively short

→ It is cheaper

→ It is practical when there is a need to control the data at one location

Disadvantages:

→ There is always a chance that the systems is prone be failure.

→ Higher security and privacy risks for users

→ It requires longer time for accessing the data for users who are pysically far from the server

Decentralized Architecture

Advantages:

→ The system is less likely to be unavailable for users than centralized system.

→ It assures better performance in availability and response time.

→ It provides space for diverse and flexible systems.

The disadvantage

→ There are some security and privacy concerns to be taken care of as the data is available at multiple location

→ Higher cost

→ Needs to be properly optimized.

Distributed Architecture

- The pros of distributed systems are:
  - → The system is highly fault-tolerant
  - → The network is transparent and more secure
  - → It promotes resource sharing that can reduce burden on single or selected machines.
  - → The network can be extremely scalable
- The cons of using distributed systems are:
  - → It is more difficult to deploy a network
  - → The maintance costs are higher than any other method.

→ Predecessors Of Blockchain

- Digicash → company : David Chaum → Blind Signature
- HashCash → email filter → the sender calculates a hashcash stamp which is appended to the email header
- HashCash uses 160 Bit SHA-1 encryption scheme. The PoW used by the HashCash is designed to have the first 20 bits to be zeros thus leaving 2^{140} combinations.
- B-Money early age distributed cash systems.

- E-gold was digital gold currency.
- Bitgold → most known decentralized virtual currency projects. Idea before Blockchain. Was similar to (Bitcoin) → Byzantine Fault Tolerant, Bitgold system → non-fungible

→ Bringing Bitcoin to Life

Compelling Components

- Open Source
- Bitcoin has 3 unique components that attract the developers in a unique way.
- Value = In the Bitcoin blockchain, the unit is BTC. A unit to account the tokens in a transaction
- Distribution: The bitcoin network follows a distributed infrastructure.
- Consensus = The Proof-of-work consensus uses the validators called Miners.

Achieving Consensus

Genesis Block ← □ → 50 BTC

first Block

→ client App
→ world-wide nodes
→ Concede the new block

is called Achieving Consensus. →

1) Block Discovery

2) Validation transaction

→ The accounting type of Bitcoin is uniquely design for saving transaction. It is called Unspent Transaction Output (UTXO). (inputs ve outputs)

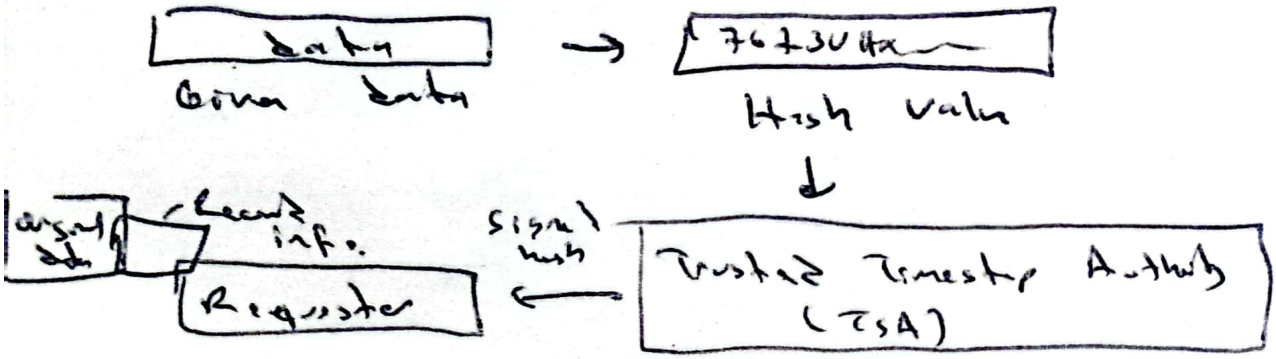
→ Bitcoin Experiment

→ Bitcoin is a decentralized digital currency. (P2P)

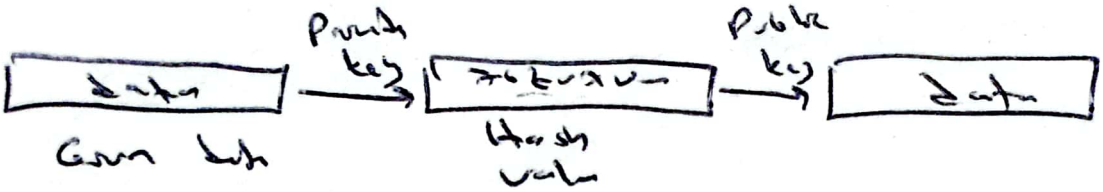
→ the laisest chain ✓

→ Time stamp servers are typical form of servers that are used cryptographically sign, authenticate and validate a digital signature

→ Creation Time stamp



Time stamp Verification:



Storing data in Blockchain

1) The block is broken into chunks

2) After splitting the data in chunks, each chunk will be encrypted to limit the access to only the owner unless it is specified.

3) Next data chunks or files will be distributed across the network in such a way that all your data will be available, even if a part of the network is unavailable

Advantage:

→ The download speeds of the networks will be increase exponentially by using peer-to-peer network similar to torrents

→ The data is globally distributed which means access at any time and anywhere.

→ No need for privacy issues

→ Data storage cost is relatively cheap such as €2 per TB per month

→ The immutability feature of the Blockchain ensures the files are protected.

→ Problems and limitations:

→ The security depends on size of network

→ The overhead of the central connection is huge.

= What is Blockchain =

Blockchain Technology

- Storing personal data
- Managing digital asset
- Maintaining supply chain for enterprises
- Empowering computer games in Metaverse

Note → Whatever can be represented as a number can be treated as a digital asset.

→ Cryptocurrencies are nothing but digital tokens defined as number in the Blockchain which are tracked from day zero.

→ Book Analogy

Book: Blockchain

Page: Block

An entry in page: Blockchain Transaction

→ How Does Blockchain Works

User request for a transaction → Block is created → Network of nodes validates the transaction

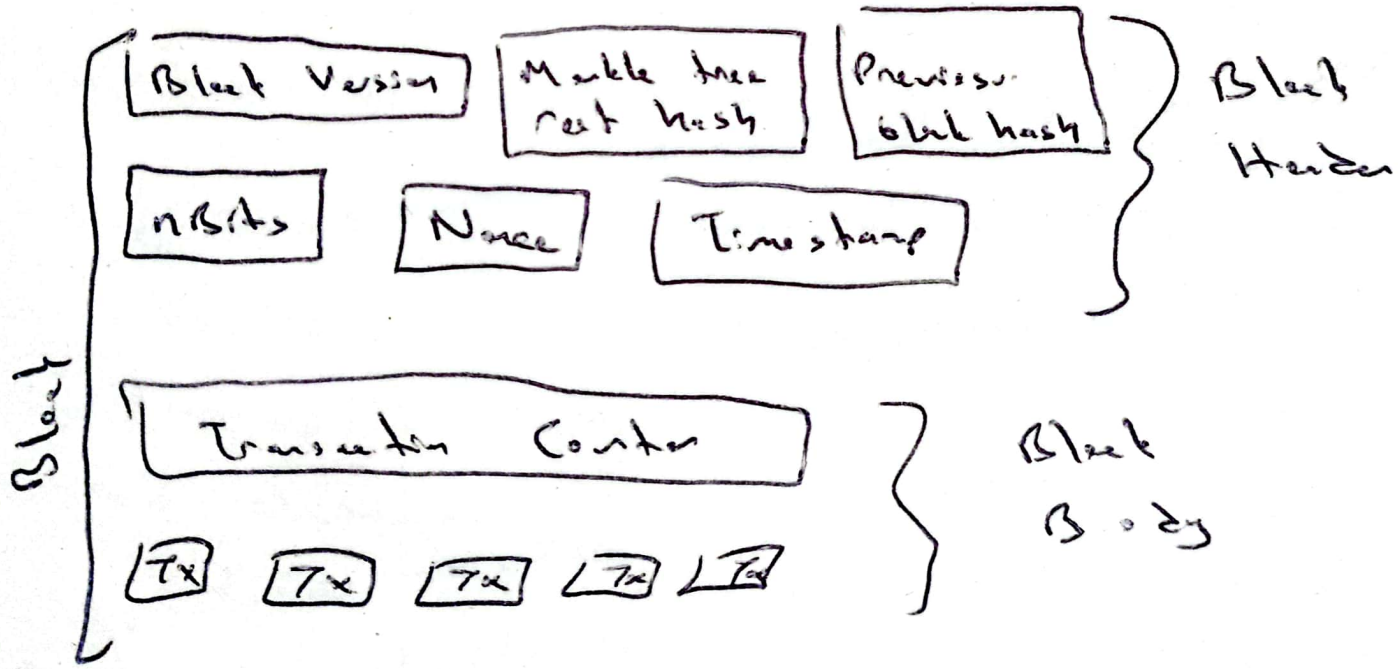
↓

Transaction is validated by other nodes in the network

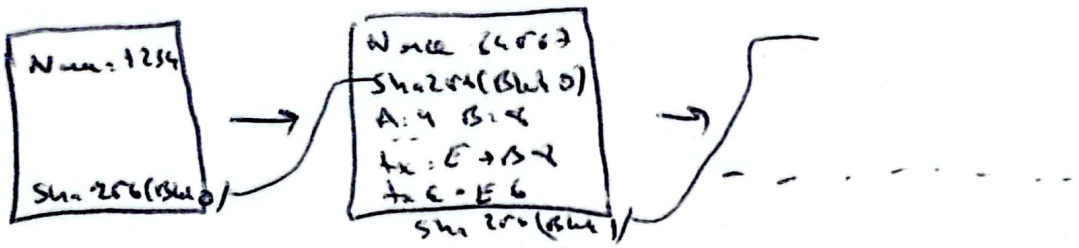
← The new block is added to the existing blockchain

← Transaction is complete

Block Overview



How Blockchain looks like ?



Genesis Block 0

Block - 1

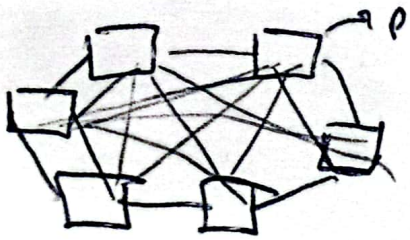
→ What makes Blockchain diffent

1) No Central Authority
2) Verifiablity and Auditability
3) Disintermediation
4) Confidentiality and Integrity
5) Robustness

→ Why is the Blockchain A distributed P2P Network

Peer - to - Peer Network

- A P2P or peer to peer network consists of a group of devices that collectively store and share files.



→ peer

→ No central authority

→ All nodes are equal to each other.

→ Anyone connected to the network

→ Peer to Peer System are categorized into three main types.

Unstructured

- There is no specific organization of the participating nodes
- Resilient for several nodes
- Requires higher memory and CPU usage

Structured

- Provides a precision search for the content that is not available generally
- Requires higher maintenance and setup costs.
- Less robust

Hybrid

- Can manage connections between peers via a central server
- Provide an improved overall performance

Blockchain Vs Cryptocurrency

- A blockchain is a decentralized ledger of all transaction across a peer-to-peer network, whereas cryptocurrency is medium of exchange, created and stored electronically in the blockchain

→ Miners can obtain fees verifying transactions (Stakes) (PoW)

Types of Blockchain

1) Public Blockchain

- Permissionless. (Anyone can join and access data)
- Decentralized
- More complex rules and consensus algorithm
- Bitcoin, Ethereum, LiteCoin

2) Private Blockchain

- Permissioned
- Are only controlled in a small that permissions are vested in a central trusted entity.
- Faster and cost-effective system

3) Federated / Consortium Blockchain

→ more than central entity.

Different Blockchain Tech.

1) Bitcoin
2) Ethereum → (smart contracts) (PoS)
3) NeO → (different programing language)
4) Hyperledger - hosted by Linux Foundation, (No native cryptocurrency)
5) EOS → (Delegated Proof-of-stake Consensus) (DPoS))
6) Corda → distributed ledger (JVM based)
7) Quorum → Jpm coin based network

= Understanding Tokens =

- Token on a blockchain are representation of any store of value, equity, use or physical or digital.
- Tokens are not limited and restricted to one specific role.
- Tokens can be fungible or non fungible

→ Benefits of crypto tokens over non-blockchain Tokens
- Usability
- Cost and Speed of Exchange
- Transparency

= Ethereum Token Standards

→ ERC → A document called as "Ethereum Request for Comments" (ERC)

→ Well-known most used ERC is ERC20

→ ERC20 ⇝ Token standard for fungible tokens

→ ERC-721 ⇝ NFTs

→ ERC-777 ⇝ Aims to address the limitations of ERC20
↳ Reduces friction in Crypto transactions

→ ERC-1155 ⇝ standard interface for contracts that manage multiple token types
↳ ~~Combination~~ of NFTs and fungible tokens
support conversion
to

→ ERC-4626 ⇝ Standard to optimize and verify the technical parameters of yield-bearing vaults.

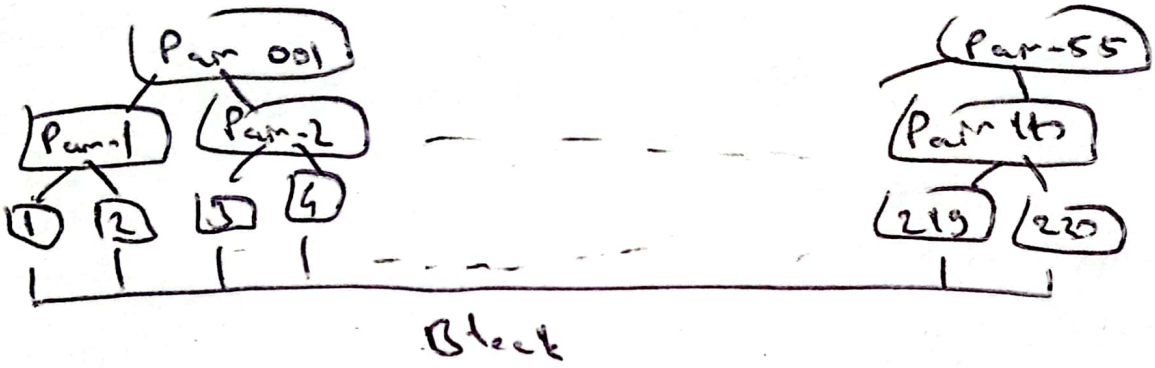
→ Ethereum Improvement Proposals (EIPs)

— Blockchain Ecosystem =

- Merkle Tree and Hashing

- Merkle tree is a hash-based data structure wherein each leaf node is a hash of a data block.

- Merkle trees are created by repeatedly hashing pairs of nodes until there is only one hash left, known as the Root hash, or the Merkle Root.



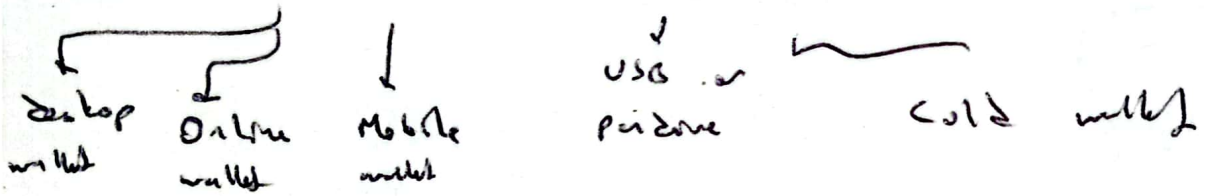
Benefits that using a Merkle Tree in blockchain offers:

- Using this data structure proves both the integrity and validity of data while significantly reducing the memory requirements
- Merkle trees are incorporated in the system to help verify that the latest block is built upon an earlier version and the constructed data is received securely
- checking validity of individual parts of a block.

= Blocks, Wallets and Addresses =

- A blockchain wallet is a software program that enables users to buy, sell and monitor balance for their digital currency or assets.
- A wallet stores private key and public keys for a user

Wallet : Software, hardware, paper wallet



→ Hot wallet → digital cryptocurrency wallet
- Cold wallets → physical devices that store crypto

Private key / Public key

1) Private Key —(elliptic Alg)→ Public Key

2) Data + Private key —(Hash)→ Signature

3) Data + Public key + Signature → (Validation) Yes / No

→ Private key —(elliptic)→ Public key —(Hash)→ (Address)

→ The two main types of cryptographic algorithms used for blockchains are:

- Asymetric - key algorithms
- Hash functions

→ Transaction

1. Stage - 1 : Initiation of transaction proposal
2. Transaction is broadcasted (Mempool node list)
3. Transaction verification
4. Transaction is committed

Components of Blockchain Ecosystem

- Projects
- Users
- Applications
- Miners
- Exchanges
- Developers

What is Mining

- Mining is the process of recording the pending transaction by adding a new Block into the Blockchain through a math puzzle
- Miners are the people create a new block.
- Longest Chain is king.

Miners
- CPU
- GPU
- ASIC

- Types of Mining -

Solo Mining

Pool Mining

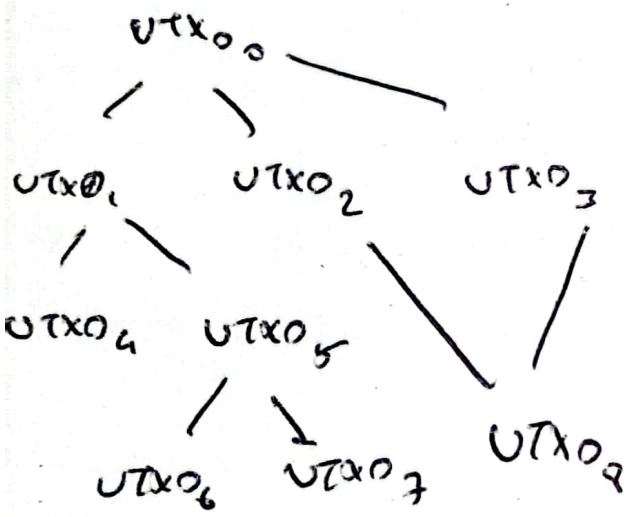
- UTXO Model vs Account Model

UTXO

BTC

Account/Balance → Private key account
(Contract Code Acc

ETH



State n — Acc A — Bal t0

State (n+1) — Acc A — Bal t1
Acc B — Bal t1

State (n+2) — Acc A — Bal t2
Acc B — Bal t2

State (n+3) — Acc A — Bal t3
Acc B — Bal t3
Acc C — " t3

→ Smart Contracts

- Automatic execution program in the blockchain

What is Consensus

→ Consensus mechanisms ensure all nodes are sync. and agree on which transactions are legitimate and are added to the blockchain.

Byzantine General Problem ('Majority is win)

Type of Consensus Algorithm = POW, PoS, Delegated PoS

Byzantine Fault Tolerance Mech.

→ Others Consensus:

- Proof-of-Capacity (PoC)
- Proof-of-Activity (PoA)
- Proof-of-Burn (PoB)
- Proof-of-Weight (PoW)
- Leased Proof-of-Stake (LPoS)

Steps to Create Your Blockchain Solution

1) Identify a suitable use-case
2) Identify the most suitable consensus mech.
3) Identify the most suitable platform.
4) Designing the Nodes
5) Design the blockchain instance → Permissions
6) Build the APIs
7) Design the Admin and User Interface

Address format
Key formats

Asset issuance
Asset creation
Atomic changes
Key management
Multi signature
Parameters

Blockchain Use Cases in Finance and Business

- Payment Across Borders
- Insurance (signature)
- Accounting and Auditing (deWisdom)
- Supply Chain Management
- Healthcare
- Clinical Trials
- Election
- Additive Manufacturing
- Gaming

Central Bank Digital Currency (CBDC)

- Retail
- Wholesale