BLOCKCHAIN 101

An Introduction to Blockchain & Web3 Ecosystem.

Web3Assam Winter Cohort 2025

By JKonChain

About Me

Jishantu Kripal
aka
JKonChain

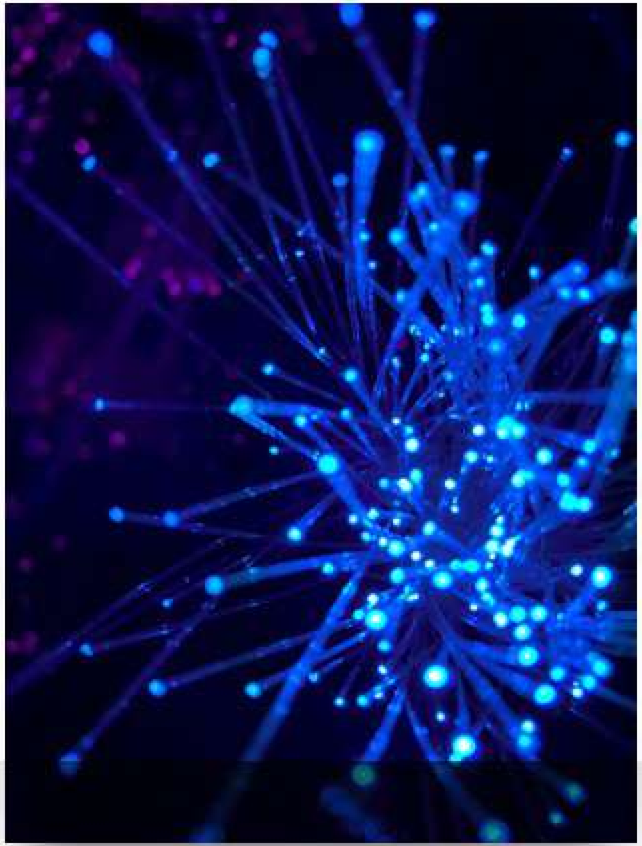
Web3 Vibe Coder | **Prompt Engineer** |
Content Strategist | **Researcher & Community Manager**

- *In Web3 since 2022*
- *Joined Web3Assam in 2023 as Mentee*

Contents

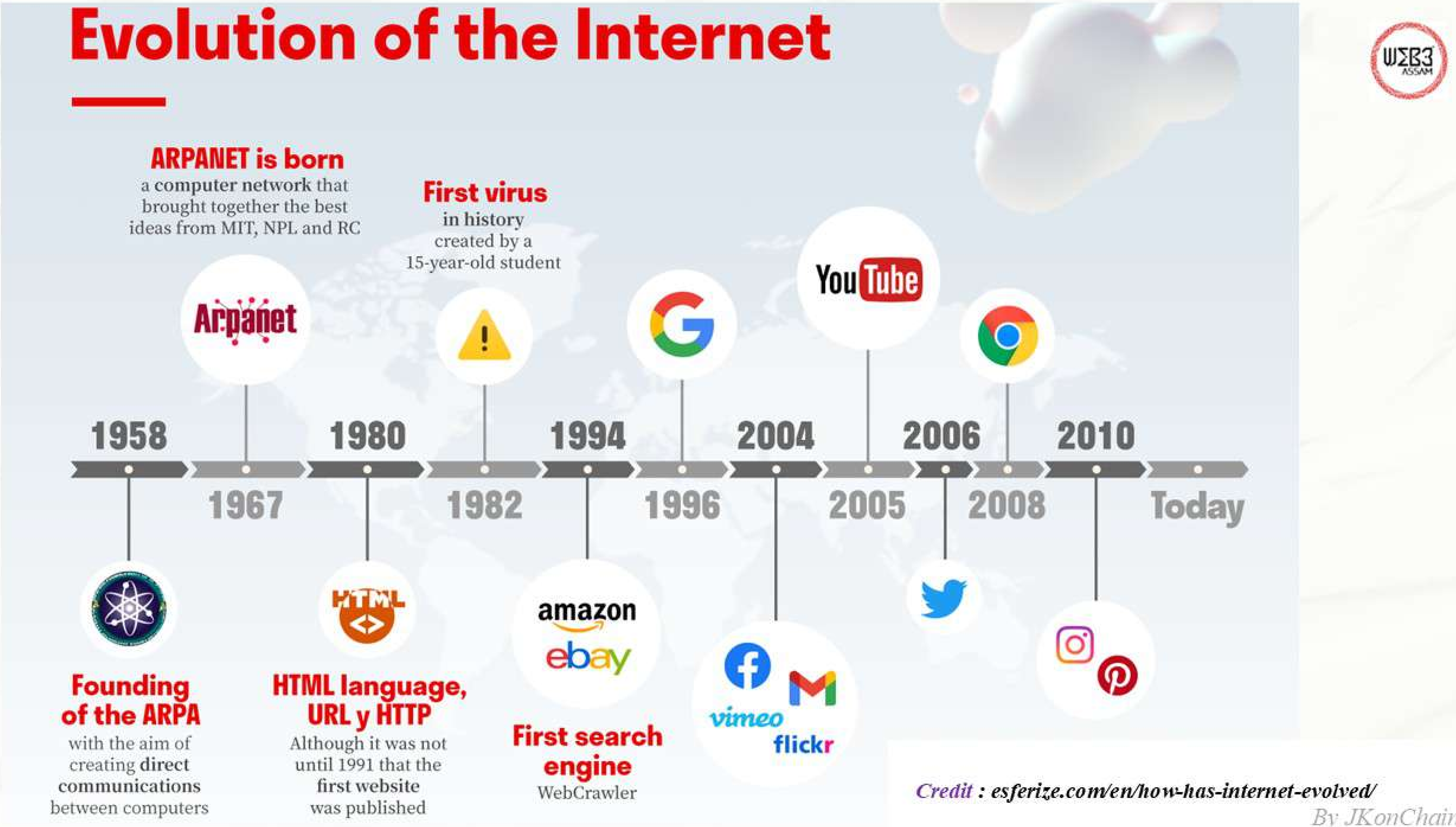
Session Length: 3.5 Hours

The Evolution of Internet



Web3Assam Winter Cohort 2025

By JKonChain



Credit : esferize.com/en/how-has-internet-evolved/

By JKonChain

WEB3 ASSAM

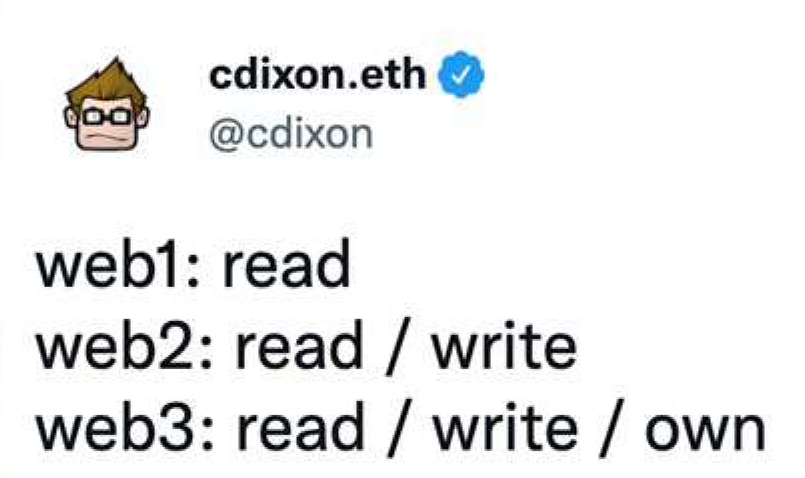
By JKonChain

Web 2.0 - The Social Web

- ❑ Time period: **2004 – Present (mainstream web)**
- ❑ **Content:** Dynamic, user-generated (UGC)
- ❑ **Users:** Both consumers and creators
- ❑ **Data ownership:** Controlled by centralized companies
- ❑ **Technology:** JavaScript, APIs, Cloud, Databases
- ❑ **Examples:** Facebook, YouTube, Twitter, Google, Amazon
- ❑ **Monetization:** Data-driven ads, subscription models
- ❑ **Problems:** Centralization of power, Privacy concerns, Data exploitation
- ❑ **Key trait:** *Participation & central control*

Web 1.0 - The Static Web

- ❑ Time period: **1990s – early 2000s**
- ❑ **Content:** Static HTML pages
- ❑ **Users:** Consumers of information (no contribution)
- ❑ **Data ownership:** Controlled by website owners
- ❑ **Technology:** HTML, HTTP, basic CSS
- ❑ **Examples:** Yahoo!, AOL, Britannica Online
- ❑ **Monetization:** Display ads, basic e-commerce
- ❑ **Key trait:** *Information publishing*



Web 3.0 - The Decentralized Web

- Time period: **Emerging (2020s onward)**
- **Content:** Decentralized, tokenized, transparent
- **Users:** Owners and stakeholders in the ecosystem
- **Data ownership:** Controlled by individuals via blockchain wallets
- **Technology:** Blockchain, Smart Contracts, Cryptography, IPFS, AI
- **Examples:** Ethereum, Polygon, Uniswap, OpenSea, Lens Protocol
- **Monetization:** Token economies, NFTs, decentralized finance (DeFi)
- **Benefits:**
  - Transparency & security
  - True digital ownership
  - No intermediaries
- **Challenges:**
  - Scalability, regulation, UX complexity
- **Key trait:** *Decentralization & user empowerment*

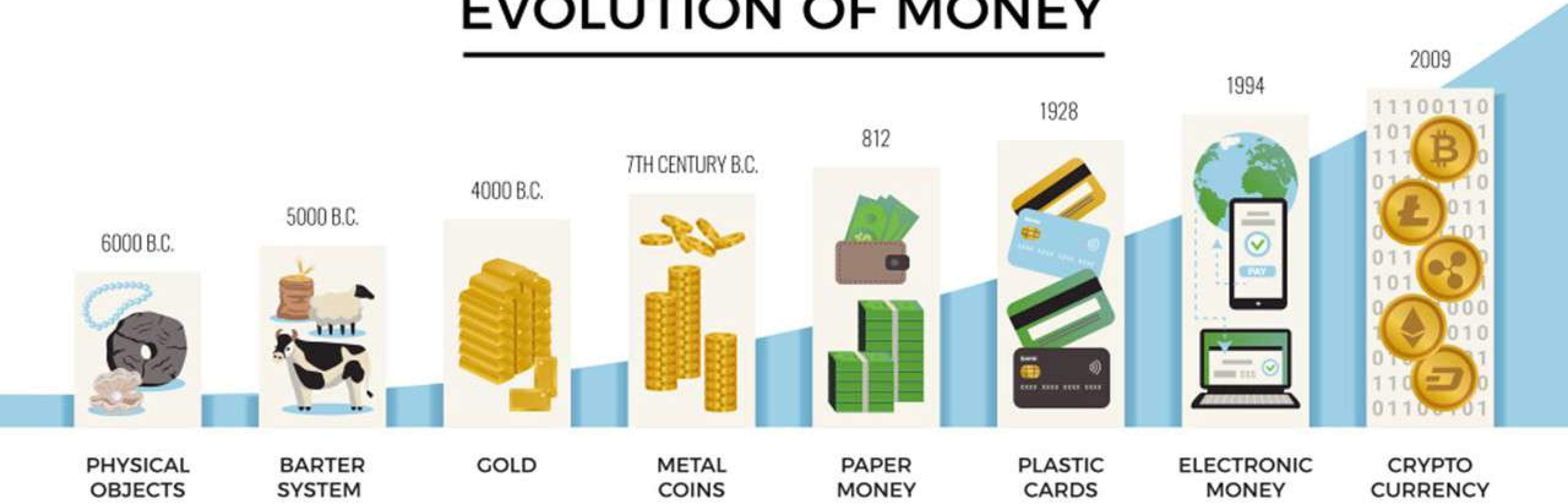
By JKonChain

The *Evolution* of **Money**

Web3Assam Winter Cohort 2025

By JKonChain

EVOLUTION OF MONEY



Lehman Brothers Collapse (2008 Financial Crisis)

- Lehman Brothers: One of the largest global investment banks (founded 1850).
- Main business: Mortgage-backed securities (MBS) and financial derivatives.
- Operated heavily in the U.S. housing market.

What Went Wrong?

- Banks started giving subprime loans (loans to people who couldn't repay).
- These risky loans were packaged and sold as "safe" investments.
- When people defaulted on mortgages, the entire system collapsed.
- Lehman Brothers had massive exposure to these toxic assets.


THE WALL STREET JOURNAL.

AIG, Lehman Shock Hits World Markets

AIG Faces Cash Crisis As Stock Dives 61%

The Collapse:

- September 15, 2008 → Lehman Brothers filed for bankruptcy (~$600B debt).
- Triggered a global financial crisis — stock markets crashed worldwide.
- Millions lost jobs, homes, and savings.
- Governments bailed out major banks using taxpayers' money.

- Author: Satoshi Nakamoto
- Published On: October 31, 2008.

Key Problems in Centralized System :

- ❑ Single Point of Failure
- ❑ Mismanaged Economies
- ❑ Monopolization & Pricing Power
- ❑ Economic & Social Inequality

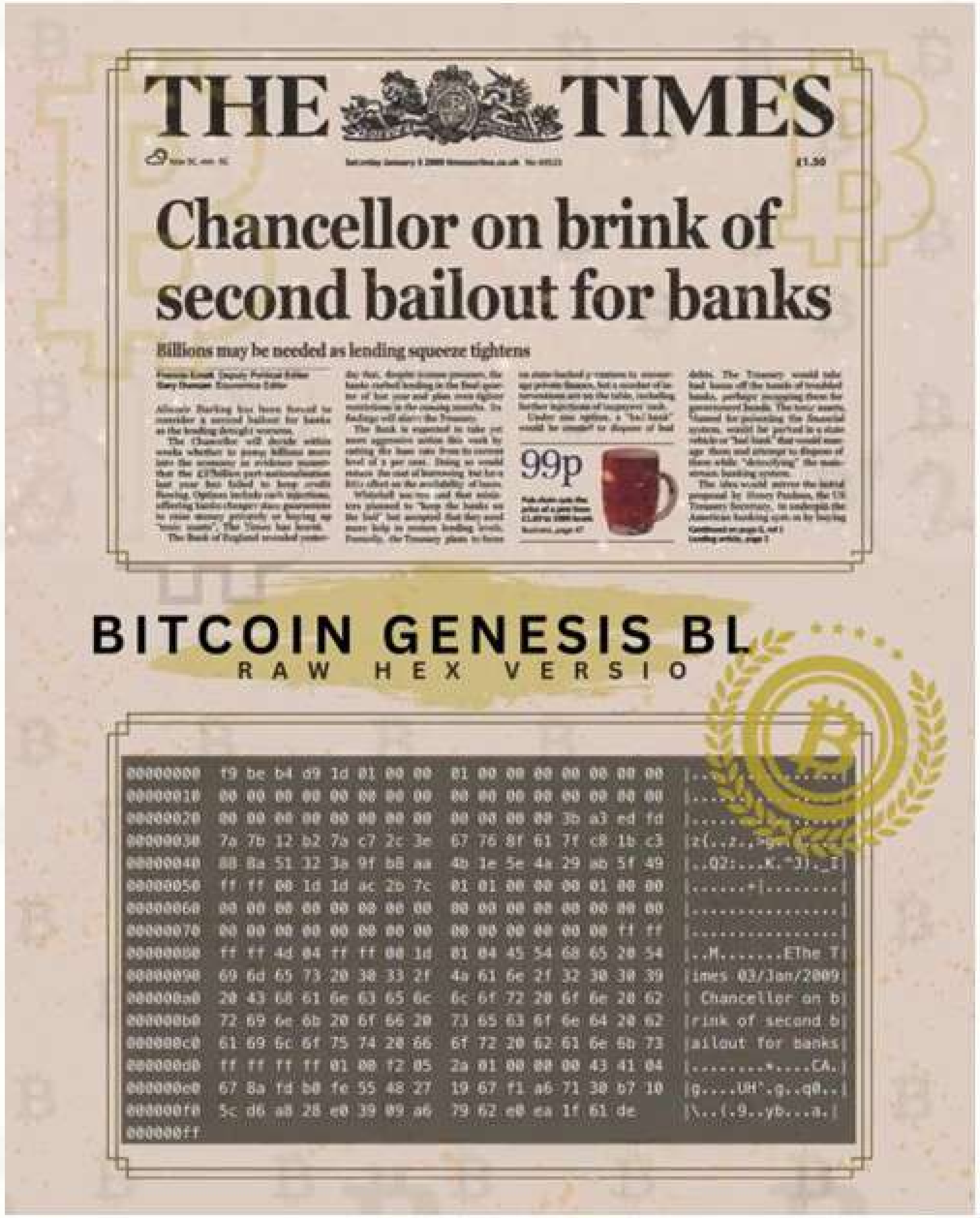
Technical Problems Satoshi Need to Solve

✅ **Byzantine Generals Problem:** It describes the difficulty of achieving agreement in a distributed network where some participants may act dishonestly or send false information. Blockchain solves it using consensus algorithms like Proof of Work or Proof of Stake, ensuring all honest nodes agree on one version of truth.

✅ **Double Spending Problem:** It's the risk of a digital currency being spent more than once because digital files can be easily copied. Blockchain prevents this by recording every transaction on a transparent, immutable ledger verified by the network.

BITCOIN

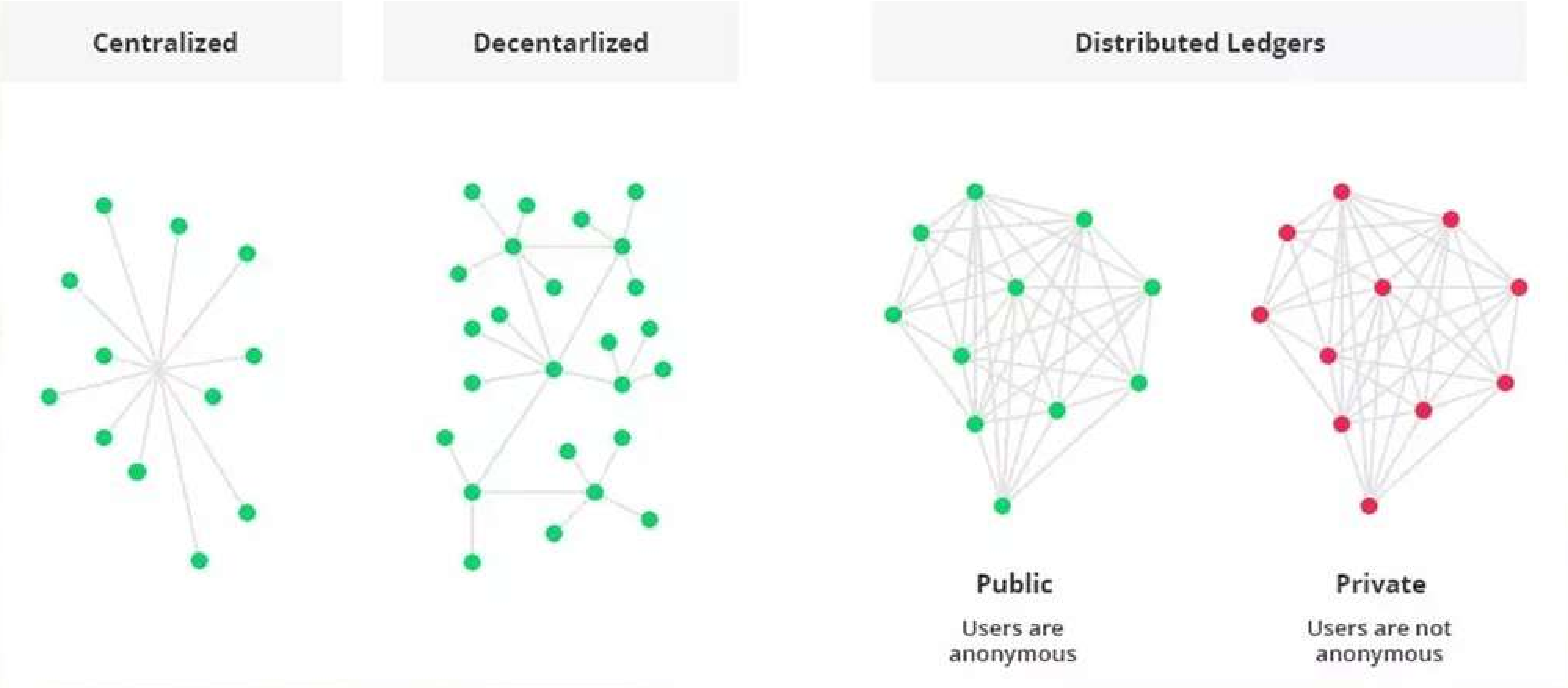
- ✓ **Mined on:** January 3, 2009, by *Satoshi Nakamoto*.
- ✓ **Block reward:** 50 BTC (which cannot be spent).
- ✓ **Special message embedded in the data:**
- ✓ *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."*
- ✓ This message referenced a headline from *The Times* newspaper, symbolizing Bitcoin's purpose — a **reaction to the failures of the traditional banking system** and a call for **decentralized financial freedom**.



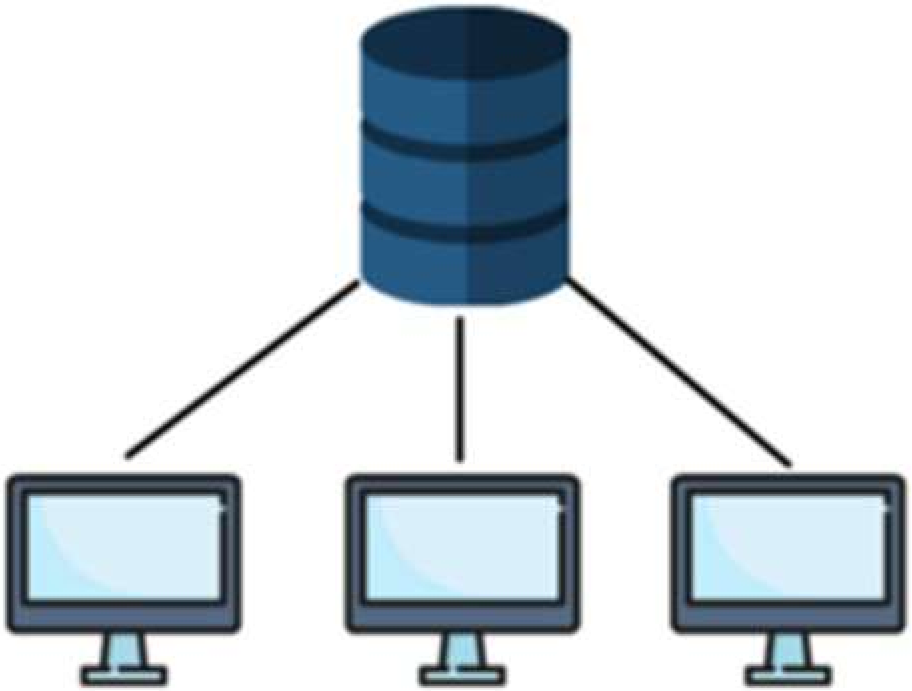
Web3Assam Winter Cohort 2025

By JKonChain

Blockchain is a **distributed digital ledger** that records transactions or data **across** a network of computers (**nodes**) in a way that is **secure**, **transparent**, and **tamper-proof**.



Client Server Architecture



Peer to Peer Architecture

The blockchain is a decentralized, distributed ledger (public or private) of different kinds of transactions arranged into a P2P network. This network consists of many computers, but in a way that the data cannot be altered without the consensus of the whole network.

Key Features of Blockchain:

- **Decentralization**: There is no central authority making it difficult to censor blockchain or manipulate it.
- **Immutability**: Once data is added to the blockchain, it can't be tampered making is trust worthy way to store information.
- **Transparency**: Anyone can view the transactions and blocks of the blockchain, making it challenging to hide illegal or fraudulent activity.
- **Consensus Mechanism**: This prevents addition of fraudulent transactions entering the blockchain by using the decision-making process to ensure that the majority of the nodes agrees to the data's validity.

Most Common Myth

BITCOIN ≠ BLOCKCHAIN

By JKonChain

BITCOIN

A digital currency to address the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems.

Advantages:

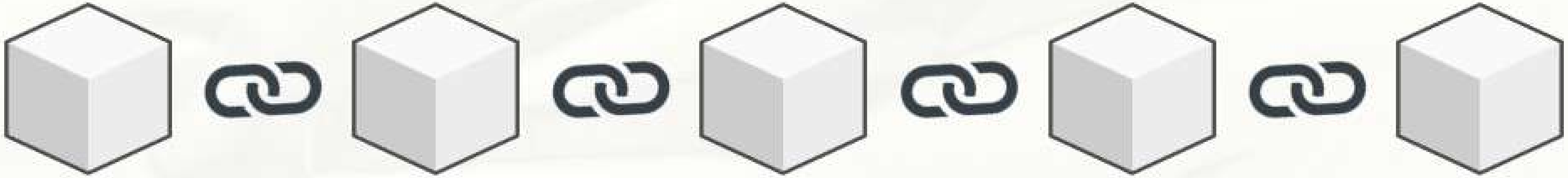
- **Cost-effective**: Bitcoin eliminates the need for intermediaries.
- **Efficient**: Transaction information is recorded once and is available to all parties through the distributed network.
- **Safe and Secure**: The underlying ledger is tamper evident. A transaction can't be changed; it can only be reversed with another transaction, in which case both transactions are visible

Bitcoin and blockchain are <u>not the same</u>. Blockchain provides the means to record and store bitcoin transactions, but blockchain has many uses beyond bitcoin. Bitcoin is only the first use case for blockchain.

The ***Blockchain*** as a **Technology**

Web3Assam Winter Cohort 2025

By JKonChain

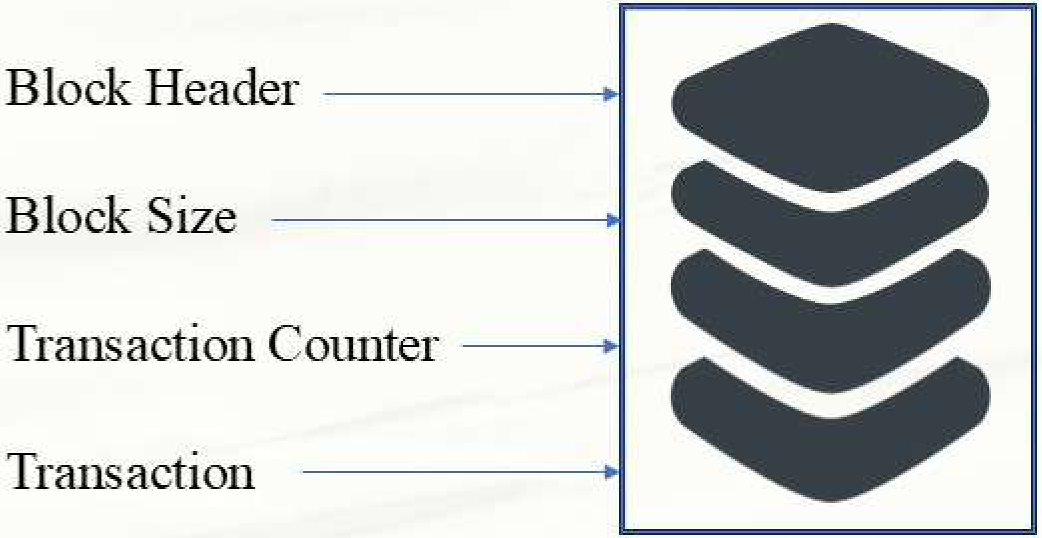


Blockchain is basically a digital ledger that records transactions and data then they are shared across a network of computers.

❑ *What is a block and its structure?*

Blocks are the basics data structure of blockchain. It serves as the repository for the transactional data. Essentially, blockchain is a sequence of interconnected blocks each holding valuable information.

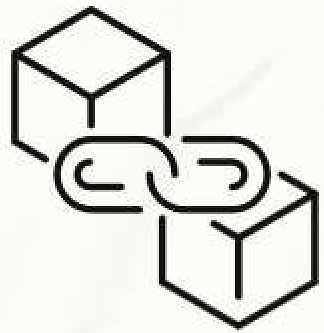
BLOCK COMPONENTS



Block

What's Inside a Block?

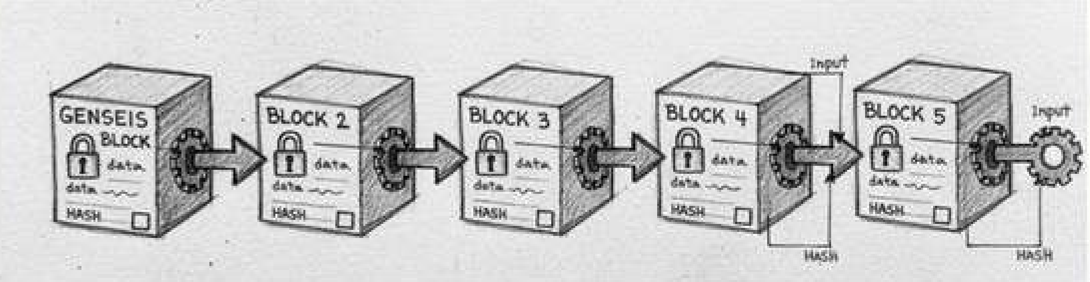
- **Block Header** – contains metadata:
  - **Block Version** → defines blockchain protocol version used.
  - **Previous Block Hash** → connects this block to the one before it.
  - **Merkle Root** → a hash representing all transactions in the block.
  - **Timestamp** → when the block was created.
  - **Nonce** → number used during mining (proof-of-work).
  - **Difficulty Target** → defines how hard it is to find the block hash.
- **Transaction Counter** – total number of transactions in that block.
- **Transactions List** – actual data of all verified transactions.

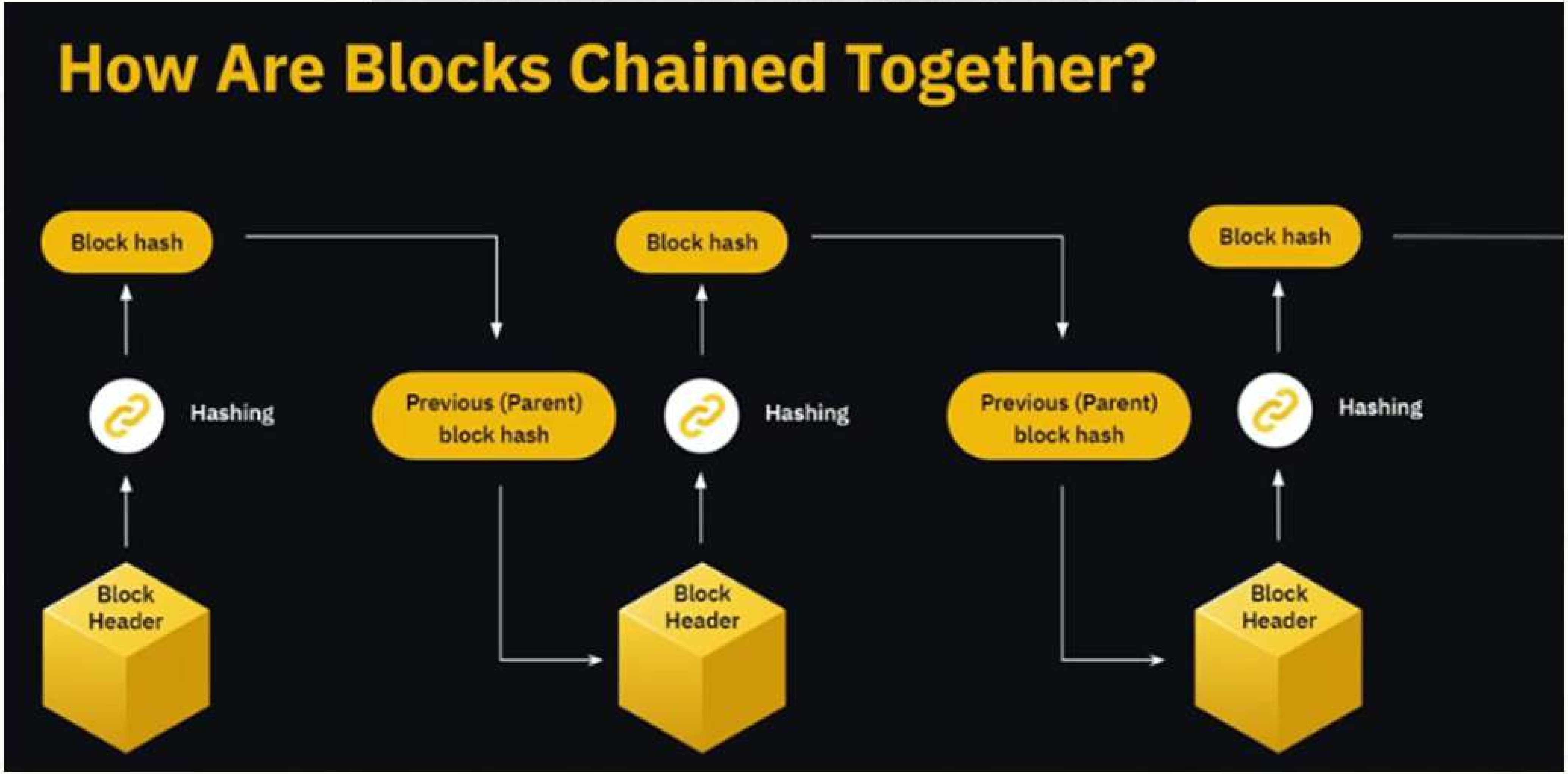


Genesis Block is the first ever block created in the blockchain. The Genesis Block has the block height 0

Block height refers to the position or number of a block in the blockchain i.e. how many blocks exist before it in the chain. It's like a block's serial number or index that tells where it sits in the blockchain sequence.

Block Height = The number of blocks preceding a particular block in the blockchain.


GENSEIS BLOCK
data
HASH
BLOCK 2
BLOCK 3
BLOCK 4
BLOCK 5
Input
HASH


How Are Blocks Chained Together?
Block hash
Hashing
Block Header
Previous (Parent) block hash
Block hash
Hashing
Block Header
Previous (Parent) block hash
Block hash
Hashing
Block Header

A ***cryptographic hash function*** is a mathematical algorithm that converts any input data into a fixed-length output (called a hash or digest). It's a core concept in blockchain, ensuring data integrity, security, and immutability. Example algorithms: SHA-256, SHA-3, MD5 (outdated).

Cryptographic Hash Function

Input

- **Mathematical Algorithms** : Cryptographic hash functions use complex mathematical formulas to process input data.
- **Deterministic** : The same input always produces the same output.
- **One-way Function** : It's impossible to reverse-engineer the original input from the hash.
- **Collision Resistant** : Two different inputs should never produce the same hash output.
- **Avalanche Effect** : A small change in input causes a completely different hash output ensuring unpredictability.

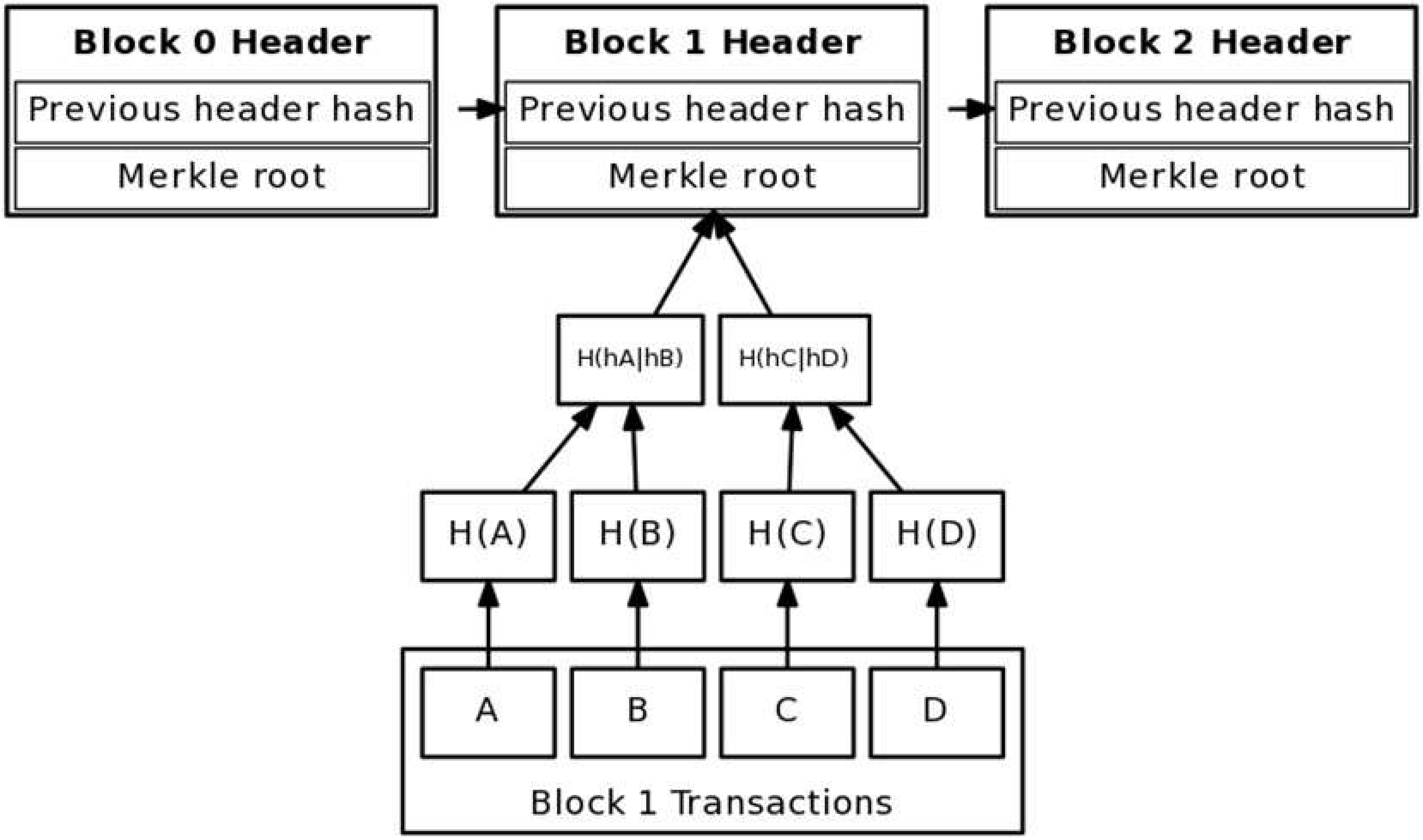
Output

Type of Blockchain

	Access Control	Decentralization Level	Transparency	Speed & Efficiency	Use Case / Industry	Examples
Public Blockchain	Open to everyone	Fully decentralized	High transparency	Slower (due to consensus like PoW)	Cryptocurrency, Smart Contracts	Bitcoin, Ethereum
Private Blockchain	Restricted (single organization)	Partially centralized	Limited to internal members	Very fast	Enterprise data management, Auditing	Hyperledger Fabric, Corda
Consortium (Federated) Blockchain	Controlled by group of organizations	Semi-decentralized	Shared among selected participants	Fast and efficient	Banking, Supply Chain, Energy	Quorum, Energy Web Foundation (EWF)
Hybrid Blockchain	Combination of Public & Private	Balanced (depends on setup)	Partial transparency	Moderate to fast	Supply chain, Government, Healthcare	Dragon Chain, IBM Food Trust

Merkle Tree

- The Merkle Tree is a tree-like data structure used in cryptography to ensure security by checking the integrity of large amount of data.
- The main difference from the binary three is that it basically uses hashes instead of numbers.
- The Merkle Tree is constructed by recursively hashing pairs of data until a single hash, known as the Merkle Root is obtained.
- Merkle trees allow for efficient verification of blocks, without the need to transfer and store the entire block.



Merkle tree connecting block transactions to block header merkle root

Core Blockchain Components

- **Node** : User or Computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger).
- **Transaction** : Smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain.
- **Block** : A data structure used for keeping a set of transactions which is distributed to all nodes in the network.
- **Chain** : A sequence of blocks in a specific order.
- **Miners** : Specific nodes which perform the block verification process before adding anything to the blockchain structure.
- **Consensus Algorithm** : A set of rules and arrangements to carry out blockchain operations.

Nodes

Nodes are the backbone of any blockchain network. They are the computers or devices that keep track of the blockchain ledger and ensure that all transactions are valid. Nodes verify transactions, record them on the blockchain, and help to secure the network.

How are transactions executed?

Someone is requesting a transaction → The request transaction is transmitted through a P2P network of computers called nodes → (Validation Process) → Cryptocurrency Contracts, Records → After the transaction has been verified, it is added to the group of other transactions to form a new block → A new block containing a validated transaction is permanently added to the existing blockchain and can not be changed → The transaction is complete.

Transaction Pool

Unconfirmed transactions are temporarily stored in the transaction pool, which is also known as the memory pool or mempool. This pool keeps track of transactions that are waiting to be included in the next block.

User → Blockchain → Transaction Pool

Once a transaction is selected by miner, the transaction is added to a block leading to the confirmation of the transaction.

Type of Node	Description
Full Node	❑ Stores the entire blockchain ledger. ❑ Validates all transactions and blocks independently. ❑ Maintains network security and integrity. ❑ Example: Bitcoin Core Node.
Light Node (SPV Node)	❑ Stores only block headers, not full data. ❑ Relies on full nodes for verification. ❑ Used in mobile or lightweight wallets.
Mining Node	❑ Creates new blocks by solving cryptographic puzzles (Proof of Work). ❑ Requires high computational power. ❑ Example: Bitcoin miners.
Masternode	❑ Performs special services like instant transactions or privacy functions. ❑ Requires holding a fixed collateral of cryptocurrency. ❑ Example: Dash network.
Validator Node	❑ Used in Proof of Stake (PoS) systems. ❑ Validates and proposes new blocks based on stake amount. ❑ Example: Ethereum 2.0, Cardano.
Archival Node	❑ Stores the complete blockchain history including all past states. ❑ Used for research, analytics, and data recovery. ❑ Not directly involved in consensus.

Mining

The blockchain network temporarily holds transactions in the transaction pool until miners incorporate them into a block. This process plays a vital role in maintaining the integrity and security of the blockchain.

Transactions Pool → Miner/Validator → Find Valid Nonce (The block will be transferred to all nodes after a valid nonce value is found) → Miners will start working on the last block that was added.

A consensus mechanism is the core process in a blockchain network that ensures all nodes agree on a single, valid version of the ledger - even though no central authority exists. It's what makes a blockchain trustless, secure, and synchronized across all participants.

- ❑ Proof of Work (PoW)
- ❑ Proof of Stake (PoS)
- ❑ Proof of History (PoH)
- ❑ Proof of Capacity (PoC)
- ❑ Proof of Activity (PoA)
- ❑ Proof of Burn (PoB)
- ❑ Proof of Authority (PoA)
- ❑ Delegated Proof of Stake (DPoS)

Blockchain Transaction Type

- Public Transactions : Public transactions are stored in the transaction pool for some time and are awaiting confirmation.

The process: User → Transaction Pool → Miner/Validator → Nonce (transaction published) → Added to Blockchain

- Private Transactions : Private Transactions are sent directly to the processing/verification device, without being saved to the transaction pool.

The Process: User → Miner/Validator

Web3 Ecosystem

By JKonChain

Blockchain Layer (Base Layer / Layer 1)

These are foundational decentralized networks that store data and execute transactions. Examples: Bitcoin, Ethereum, Solana, Polkadot, Binance Smart Chain, Avalanche.

Responsible for:

- ❑ Security
- ❑ Transaction Validation
- ❑ Consensus Mechanism
- ❑ Smart Contract Execution (for some chains)

Protocol Layer (Layer 1/ Layer 2)

These define rules for communication, interoperability, and scaling. Includes:

- ❑ Layer 2 Networks (Polygon, Optimism, Arbitrum) – Improve speed & reduce gas fees
- ❑ Cross-Chain Protocols (Cosmos IBC, Polkadot XCMP, Wormhole) – Enable chain-to-chain interaction
- ❑ Storage Protocols (IPFS, Filecoin, Arweave) – Decentralized file hosting
- ❑ Compute Protocols (Golem, Akash) – Decentralized cloud computing

Smart Contract Layer

Self-executing contracts with predefined logic.
Enable creation of:

- ❑ DeFi platforms
- ❑ NFTs
- ❑ DAOs
- ❑ Dapps

Main languages: Solidity, Rust, Vyper, Move

Application Layer (DApps)

Decentralized applications built on smart contracts.
Examples:

- ❑ DeFi : Uniswap, Aave, MakerDAO
- ❑ NFT Platforms : OpenSea, Rarible
- ❑ Gaming/Metaverse : Decentraland, Axie Infinity
- ❑ Identity : ENS, Lens Protocol
- ❑ SocialFi : Farcaster, BaseApp

Wallets & Identity Layer

Web3 Wallets: Metamask, Phantom, Ledger
Purpose:

- ❑ Store private keys
- ❑ Interact with DApps
- ❑ Manage crypto assets
- ❑ Provide digital identity

Decentralized Identity (DID) systems provide control over identity without central authorities.

Infrastructure & Tools

These power development, monitoring, and user interactions. Includes:

- ❑ Node Providers: Infura, Alchemy, QuickNode
- ❑ Indexing Protocols: The Graph
- ❑ Oracles: Chainlink, Band Protocol
- ❑ Dev Tools: Hardhat, Foundry, Truffle
- ❑ Bridges: LayerZero, Polygon Bridge

Token Economy Layer

Tokens enable ownership, governance, and value creation. Types:

- Utility Tokens : Used inside the platform
- Governance Tokens : Voting and decision-making
- Security Tokens : Represent financial assets
- Stablecoins : Pegged to fiat
- NFTs : Unique digital assets

Governance (DAO Ecosystem)

DAOs are decentralized autonomous organizations governed by token holders. Enable transparent, on-chain decision-making.

- Examples: MakerDAO, Uniswap DAO, Aave DAO

Core Components of Web3

Component	Description	Key Functions	Examples
Blockchain Networks (Layer 1)	Decentralized, distributed ledgers that record transactions securely without central control.	❑ Transaction validation ❑ Consensus execution ❑ Network security ❑ Immutable record keeping	Bitcoin, Ethereum, Solana, Polkadot, BNB Chain, Avalanche
Smart Contracts	Self-executing code that runs on a blockchain with pre-defined rules and automation.	❑ Automate agreements ❑ Execute logic trustless ❑ Power DApps, DeFi, NFTs	Solidity (Ethereum), Rust (Solana), Move (Aptos/Sui), Vyper
Decentralized Storage	Storage systems that distribute files across a peer-to-peer network instead of a central server.	❑ Secure file hosting ❑ Censorship resistance ❑ Persistent and tamper-proof storage	IPFS, Filecoin, Arweave
Cryptographic Tokens	Digital assets representing value, ownership, or rights on a blockchain.	❑ Value transfer ❑ Incentives for participation ❑ Governance rights ❑ Ownership of digital items (NFTs)	ETH, SOL, MATIC, USDT, USDC, BNB, NFTs

Core Components of Web3

Component	Description	Key Functions	Examples
Web3 Wallets (Identity Layer)	Applications that store private keys, manage assets, and serve as digital identity to interact with Web3.	❑ Send/receive crypto ❑ Connect to Dapps ❑ Sign transactions ❑ On-chain identity management	MetaMask, Phantom, Ledger, Trust Wallet
Decentralized Applications (DApps)	Applications running on smart contracts without centralized servers or intermediaries.	❑ DeFi services ❑ NFT marketplaces ❑ Gaming/Metaverse apps ❑ Social networks	Uniswap, Aave, OpenSea, Axie Infinity, Lens Protocol
Oracles	Systems that provide external data to blockchains, enabling smart contracts to interact with real-world information.	❑ Price feeds ❑ Weather data ❑ Randomness ❑ Cross-chain messaging	Chainlink, Band Protocol, Pyth
Interoperability Protocols	Protocols that enable communication and asset transfer between different blockchains.	❑ Cross-chain transfers ❑ Messaging ❑ Shared security	Cosmos IBC, Polkadot XCMP, LayerZero, Wormhole

Core Components of Web3

Component	Description	Key Functions	Examples
Layer 2 Scaling Solutions	Technologies built on top of Layer 1 blockchains to increase speed and reduce transaction fees.	❑ Faster processing ❑ Higher throughput ❑ Lower gas fees	Optimism, Arbitrum, Polygon, zkSync, StarkNet
Governance & DAOs	Community-driven decision-making frameworks using smart contracts and governance tokens.	❑ Voting on upgrades ❑ Treasury management ❑ Protocol direction	MakerDAO, Uniswap DAO, Aave DAO
Developer Infrastructure & Tools	Tools and services that simplify building, testing, deploying, and monitoring Web3 applications.	❑ Node access ❑ Indexing ❑ Smart contract development ❑ Analytics	Infura, Alchemy, The Graph, Hardhat, Foundry, Truffle
Token Economy & Incentives	Economic models that govern how tokens are used for utility, governance, staking, rewards, and security.	❑ Incentivize Network participants ❑ Reward Validators ❑ Enable Governance ❑ Build digital economies	Staking rewards, governance tokens, gas tokens, yield farming

Thank You

Web3Assam Winter Cohort 2025

By JKonChain