Blockchain Introduction & Consesus Mechanism and Smart contracts

Compiled from presentations by Sumi Maria Abraham & Nikhil V Chandran,
Kerala Blockchain Academy (KBA)

June 14, 2025

Abstract

These notes are compiled from the "Blockchain Introduction" and "Consensus & Smart Contracts" webinars by the IEEE Kerala Blockchain Interest Group, presented by Sumi Maria Abraham & Nikhil V Chandran. They provide a foundational understanding of blockchain technology, its core concepts, historical context, mechanisms like consensus and smart contracts, practical use cases, and educational opportunities offered by the Kerala Blockchain Academy.

Contents

1. Introduction to Blockchain

Blockchain is a foundational technology for a distributed ledger. The Kerala Blockchain Academy (KBA) is India's first Blockchain Academy, a Centre of Excellence in Blockchain at Digital University Kerala. KBA boasts significant outreach with over 40,000 students from more than 90 countries.

2. What is Blockchain? - Key Characteristics

Blockchain is fundamentally a **distributed ledger technology (DLT)** characterized by key properties:

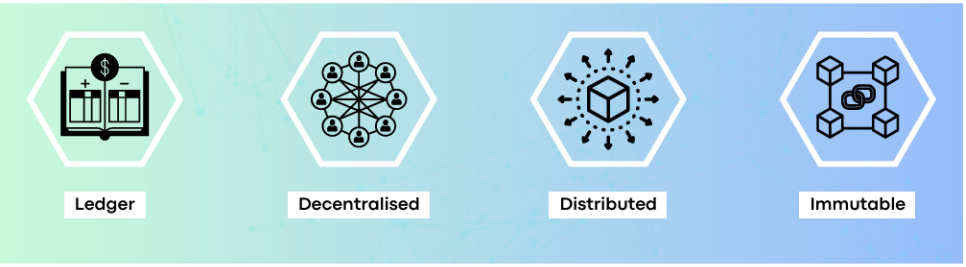

Figure 1: Core Blockchain Characteristics: Ledger, Decentralised, Distributed, Immutable (from Slide 4)

- **Ledger:** A comprehensive record of transactions.
- **Decentralised:** There is no single central authority controlling the network. Unlike a centralized ledger where a single entity manages all records and verifies transactions, a decentralized ledger distributes the record-keeping and verification among multiple participants. This removes the need for intermediaries, fostering a peer-to-peer environment.
- **Distributed:** The ledger is shared and synchronized across multiple participants or "nodes" in the network. Every participant holds a copy of the ledger.
- **Immutable:** Once data (transactions) are recorded on the blockchain, they cannot be altered or deleted. This property ensures a permanent, transparent, and tamper-proof history of all recorded events.

The shift from centralized to decentralized systems is a core principle:

The need for decentralized systems arises from challenges with centralized data control, as highlighted by various news headlines concerning data breaches and privacy issues:

2.1. Ledger Explained

A ledger is essentially a book or other collection of financial accounts. In the context of blockchain, it's a digital record of transactions.

2.1.1. Centralized Ledger

In a centralized ledger, a single entity or server maintains and controls all records. Users interact through this central point.

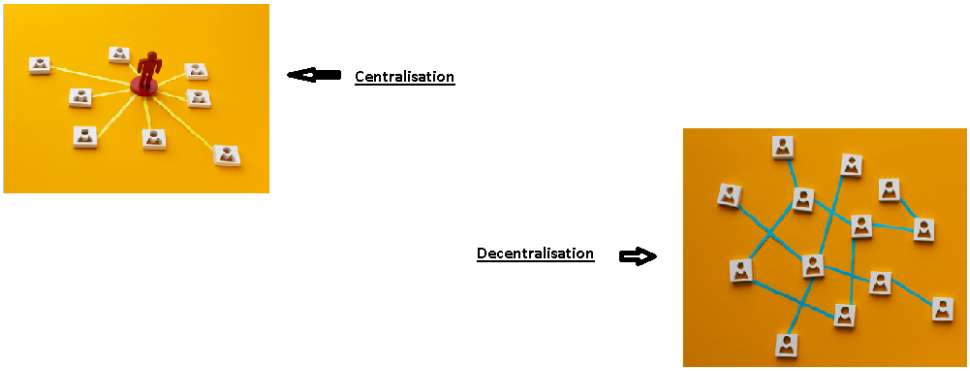

Figure 2: Centralization vs. Decentralization (from Slide 5)

Figure 3: Examples of Centralized Data Vulnerabilities (from Slide 6)

2.1.2. Decentralized Ledger

In a decentralized ledger, there is no single point of control. Records are distributed and maintained by multiple participants in the network.

3. History of Bitcoin - The First Blockchain

The concept of blockchain gained prominence with the introduction of Bitcoin.

- **2008:** An anonymous entity named Satoshi Nakamoto published a whitepaper titled "Bitcoin: A peer-to-peer electronic cash system."
- **2009:** Satoshi launched Bitcoin as an alternative to the current financial system, introducing a decentralized digital currency.
- **2010:** Laszlo Hanyecz famously bought two pizzas for 10,000 Bitcoins (BTC). As of June 2025, this amount would be equivalent to 89,706,195,282 INR, illustrating the immense growth in Bitcoin's value.

- **2025 (Estimated):** Bitcoin is estimated to consume 150 terawatt-hours (TWh) of electricity annually for its operation, which is more than the annual electricity consumption of Sweden.

4. How Blockchain Transactions Work

A blockchain transaction typically follows a multi-step process to ensure verification and secure recording on the distributed ledger.

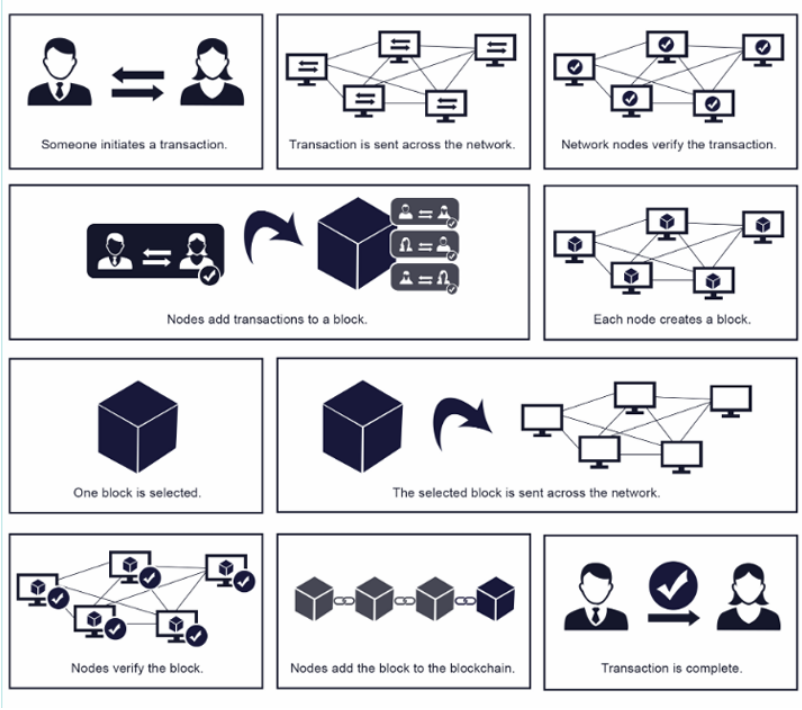

Figure 4: Blockchain Transaction Process Flow (from Slide 11)

1. **Initiation:** Someone (a user) initiates a transaction (e.g., sends cryptocurrency or data).
2. **Broadcast:** The initiated transaction is broadcast across the blockchain network to all participating nodes.
3. **Verification:** Network nodes independently verify the legitimacy and validity of the transaction according to the network's rules.
4. **Block Formation:** Verified transactions are then bundled together by nodes into a "block."
5. **Block Creation:** Each node creates its own candidate block containing these verified transactions.
6. **Block Selection (Consensus):** Through a network-specific consensus mechanism (e.g., Proof of Work, Proof of Stake), one block is selected to be added to the blockchain.
7. **Propagation:** The newly selected and verified block is broadcast across the entire network.
8. **Block Verification:** Other nodes on the network receive and verify this new block.
9. **Chain Addition:** Once verified by the network, the block is cryptographically linked to the previous block, forming an unbreakable chain.
10. **Completion:** The transaction is now permanently recorded on the immutable blockchain ledger.

5. Components of a Block

Each block in a blockchain is a data structure containing vital information that ensures its integrity and linkage within the chain.

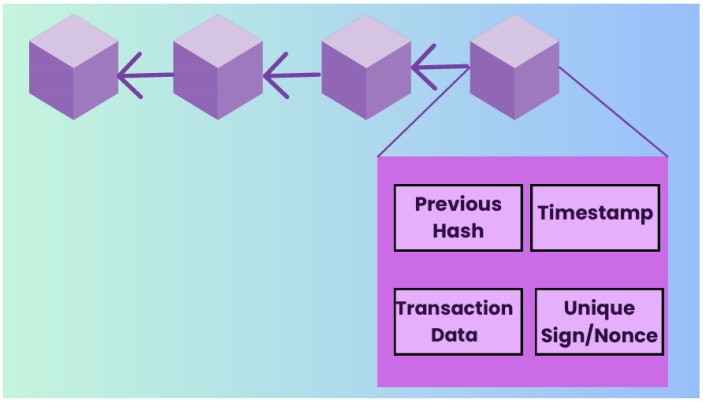

Figure 5: Simple Block Structure (from Slide 13)

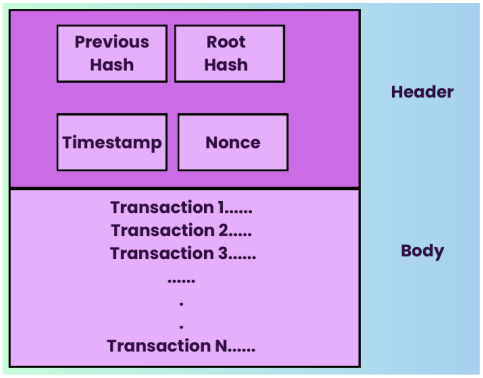

Figure 6: Detailed Block Structure (from Slide 14)

- **Header:** Contains metadata about the block.
  - **Previous Hash:** A cryptographic hash of the preceding block in the chain. This is crucial for linking blocks together and enforcing the immutability of the chain. Any change in a previous block would alter its hash, invalidating subsequent blocks.
  - **Root Hash (Merkle Root):** A single hash that summarizes all the transactions included in the block's body. It is generated using a **Merkle Tree**.
  - **Timestamp:** The exact time (or approximate time) when the block was created.
  - **Nonce:** A number that "miners" (in Proof of Work) or "validators" (in Proof of Stake) adjust to find a valid hash for the block that meets specific network difficulty targets.
- **Body:** Contains the actual list of transactions that are included and validated within that particular block.

5.1. Merkle Tree

A Merkle Tree (or hash tree) is a data structure used to efficiently verify the integrity and content of large sets of data. In a blockchain, it efficiently hashes all transactions in a block into a single root hash.

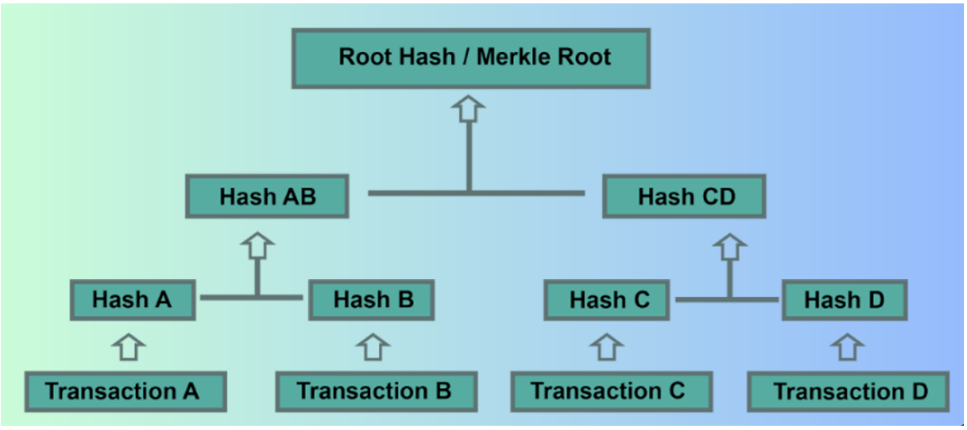

Figure 7: Merkle Tree Diagram (from Slide 15)

5.2. Blockchain Network

The blockchain network consists of multiple interconnected nodes, each maintaining a copy of the entire distributed ledger.

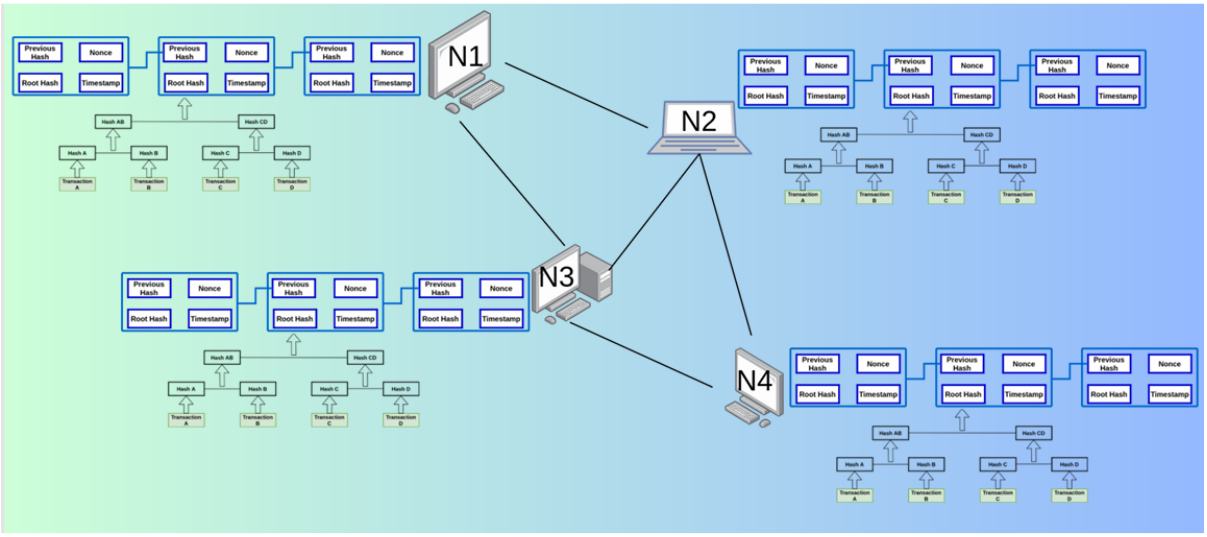

Figure 8: Blockchain Network Diagram (from Slide 16)

6. Consensus Mechanisms

Consensus mechanisms are fundamental to distributed ledger technologies. They are fault-tolerant systems used to achieve agreement on a single data value or the state of the ledger across a distributed network. They are crucial for maintaining the integrity, security, and decentralized nature of the blockchain.

- Consensus is a fault-tolerant mechanism that is used to agree on a single data value.

6.1. Proof of Work (PoW)

Proof of Work is a widely known consensus mechanism, notably used by Bitcoin.

- **Mechanism:** Miners compete to solve a complex cryptographic puzzle, often referred to as the proof-of-work problem.
- **Process:**
  1. Transactions are bundled together into a block.
  2. Miners verify that transactions within each block are legitimate.
  3. To do so, miners must solve a mathematical puzzle by finding a "Nonce." This Nonce, when combined with the block data and hashed, must result in a hash that meets a specific difficulty target (e.g., starts with a certain number of zeros). This process requires significant computational power.
  4. The first miner to find a valid Nonce and solve the puzzle broadcasts their newly mined block to the network.
  5. Other nodes verify the solution's validity.
  6. If verified, the block is added to the public blockchain, and the successful miner receives a reward.
- **Types of Mining:** CPU mining, GPU mining, ASIC (Application-Specific Integrated Circuit) mining. ASIC mining involves specialized hardware for maximum efficiency.
- **Example:** Bitcoin.
- **Mining Incentives:** Miners receive two types of rewards:
  (1) New coins created with each new block (block reward).
  (2) Transaction fees from all the transactions included in the block.
- **Bitcoin Halving:** Approximately every four years, the block reward for mining new blocks is halved. This mechanism regulates the supply of Bitcoin to deal with inflation.

6.1.1. Limitations of Bitcoin Network (PoW)

- Was meant only for Bitcoin (simple peer-to-peer electronic cash).
- Cannot perform complex computations or execute sophisticated programs directly on its blockchain.

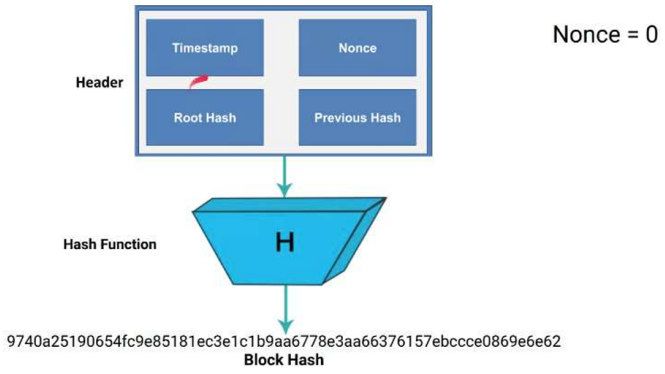

Figure 9: Proof of Work: The Hashing Puzzle (from Consensus Slide 3)

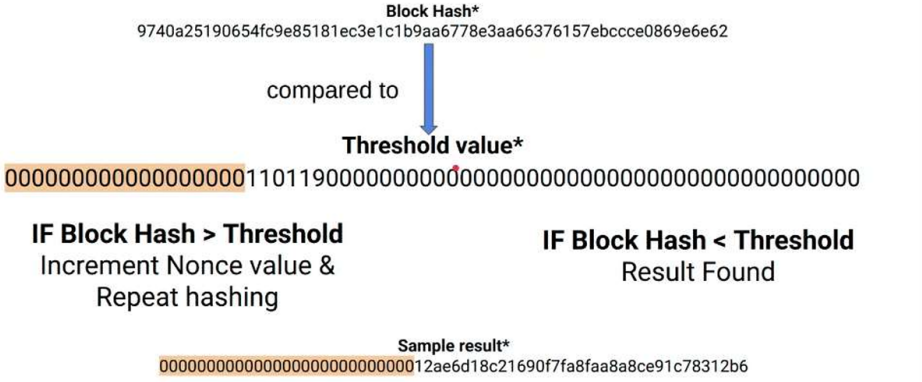

Figure 10: Proof of Work: Finding the Solution (from Consensus Slide 4)

6.2. Proof of Stake (PoS)

Proof of Stake is an alternative consensus mechanism that aims to be more energy-efficient than Proof of Work.

- **Mechanism:** Validators (instead of miners) "stake" (lock up) a certain amount of cryptocurrency as collateral to participate in the consensus process.
- **Process:**
  1. Using an election process, one node is randomly chosen to validate the next block. The size of a node's stake influences its chances of being chosen.
  2. The chosen validator checks all transactions within the proposed block.
  3. If everything seems okay, the validator node signs the block and adds it to the blockchain.
  4. The validator receives a reward, which typically consists of the transaction fees from all transactions in the validated block.
- **Trust Mechanism:** The system encourages honest behavior. If a validator validates and signs off on a fraudulent transaction, their staked cryptocurrency will be taken as a fine (slashing). As long as the potential stake loss is higher than the potential reward from

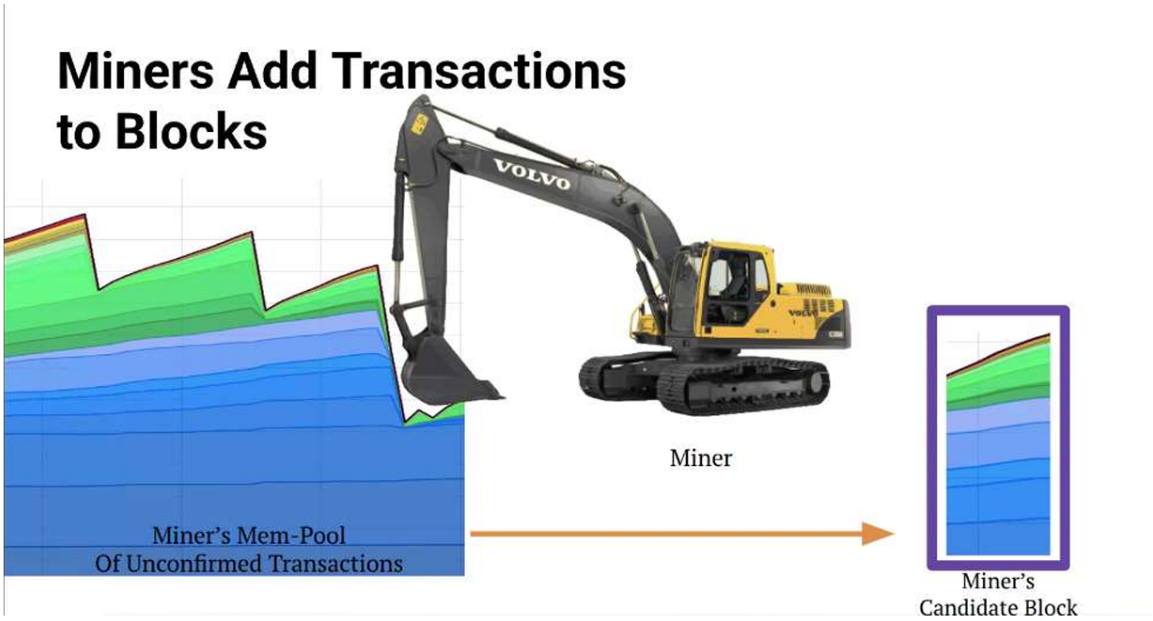

Figure 11: Miners Adding Transactions to Blocks (from Consensus Slide 7)

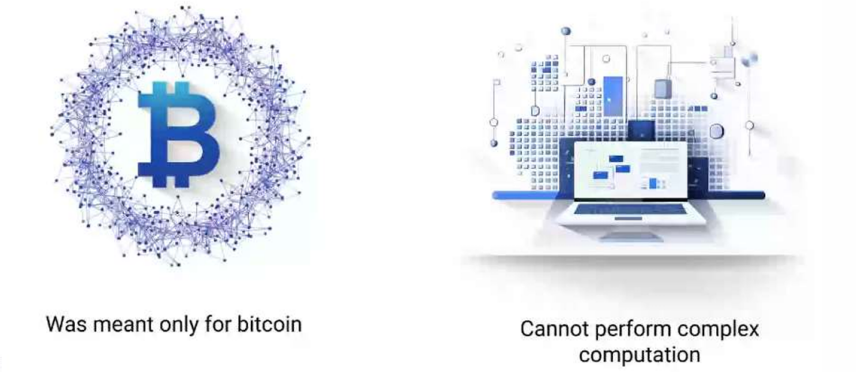

Figure 12: Bitcoin Network Limitations (from Consensus Slide 9)

dishonesty, the validator is incentivized to act truthfully. When a node stops being a validator, their stake and earned transaction fees are released after a certain period.

- **Example:** Ethereum (which transitioned from PoW to PoS). In Ethereum, consensus operates in 'Epochs' (a fixed number of blocks), divided into 'Slots'. A 'Block Proposer' is chosen for each slot, and a 'Validator Committee' verifies the proposed block.

7. Smart Contracts

A **smart contract** is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. As defined by Nick Szabo, it is "A set of promises, specified in digital form, including protocols within which the parties perform on

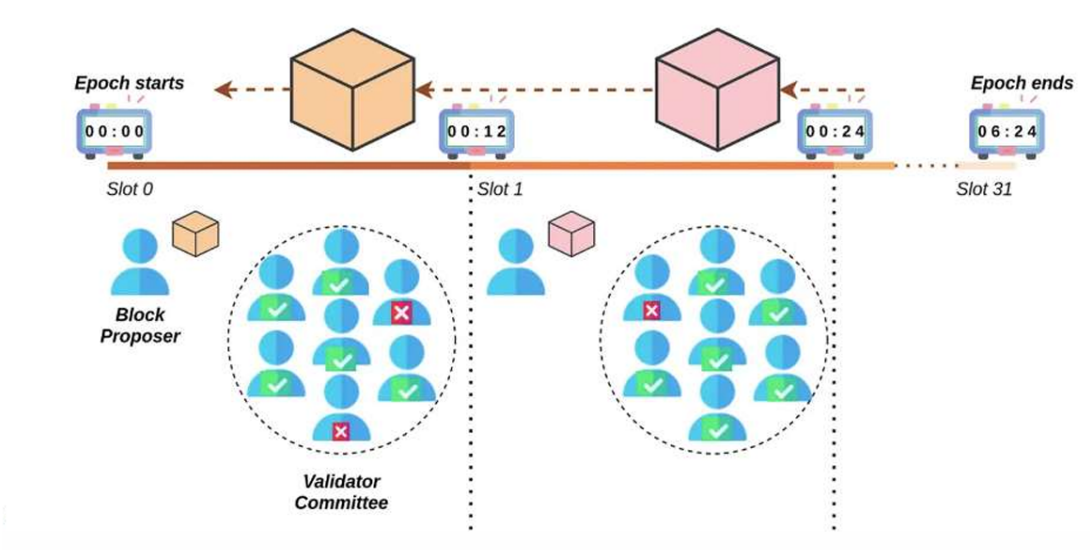

Figure 13: Consensus in Ethereum: Proof of Stake (from Consensus Slide 14)

these promises."

Figure 14: Traditional Contract vs. Smart Contract Flow (from Consensus Slide 16)

7.1. How Smart Contracts Work

Smart contracts automate the execution of an agreement when predefined conditions are met, largely eliminating the need for third parties.

1 **Pre-programmed Contracts:** A line of code is established by all counterparties, defining the rules, terms, and conditions of the agreement.

2 **Chain of Events:** If the events specified by the pre-defined conditions occur (as detected by the network), the code automatically executes.

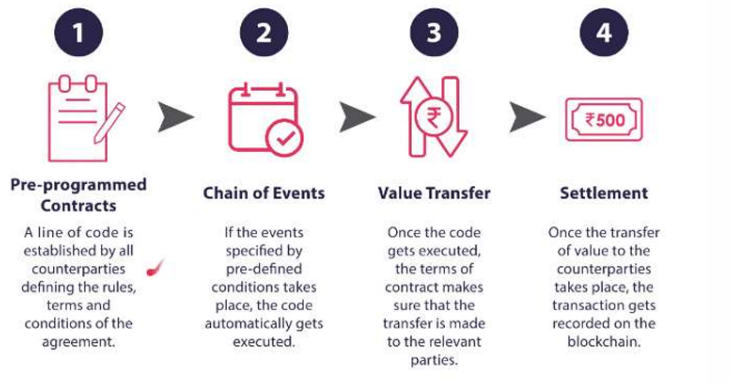

Figure 15: How Smart Contracts Work (from Consensus Slide 17)

3 **Value Transfer:** Once the code gets executed, the terms of the contract ensure that any defined value transfer (e.g., funds, data) is made to the relevant parties.

4 **Settlement:** Once the transfer of value takes place, the transaction gets recorded on the blockchain, making it trackable and irreversible.

7.2. Benefits of Smart Contracts

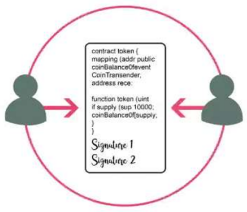

Figure 16: Smart Contract Benefits (from Consensus Slide 18)

- **Self-executing:** Automatically execute when predefined conditions are met.
- **Tamper-resistant:** Once deployed on the blockchain, their code cannot be altered.
- **Reduces malicious or accidental events:** Code-based execution minimizes human error, manipulation, and malicious intent.
- **Deterministic:** Outcomes are predictable and consistent based on the logic embedded in the code.

- **Provides transparency:** The code and execution are visible and verifiable on the public blockchain.
- **Reduced intermediaries:** Eliminates the need for third-party arbiters, leading to reduced costs and faster transactions.
- **Better trust among anonymous entities:** Trust is built into the cryptographic security and verifiable code of the contract, rather than relying on known parties.

7.3. Programmable Blockchains (e.g., Ethereum)

Bitcoin's initial design was limited to simple currency transactions. **Ethereum** introduced a "programmable blockchain," which is a modular, stateful, Turing-complete contract scripting system. This innovation enabled the creation of more complex applications beyond simple value transfers.

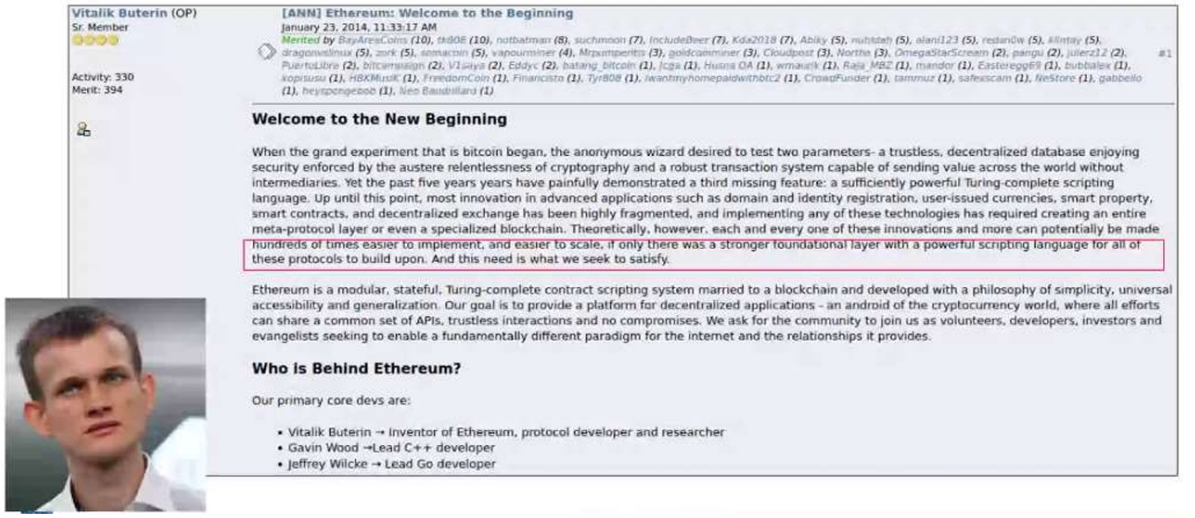

Figure 17: Vitalik Buterin and the Ethereum Announcement (from Consensus Slide 11)

7.4. Decentralized Applications (DApps)

DApps are applications built on top of decentralized networks like Ethereum.

- **Characteristics:** Distributed and shared control among network participants, open and transparent code, and code reusability.
- **Difference from Traditional Apps:** Unlike centralized applications that rely on a central server for data storage and processing, DApps distribute data storage and communication across a blockchain. This makes them more resilient, censorship-resistant, and transparent.

7.5. Smart Contract Use Case: Flight Delay Insurance

A smart contract can automate flight delay insurance:

- A smart contract is created based on the terms and conditions (e.g., compensation for delays exceeding two hours).

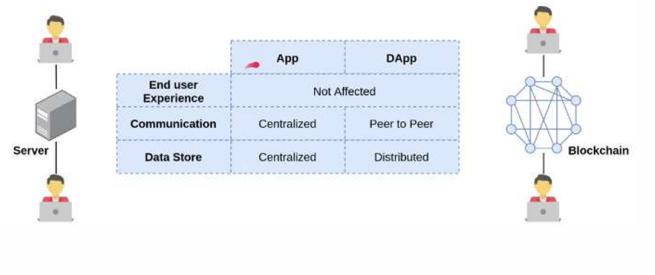

Figure 18: Decentralized Applications (DApps) Comparison (from Consensus Slide 15)

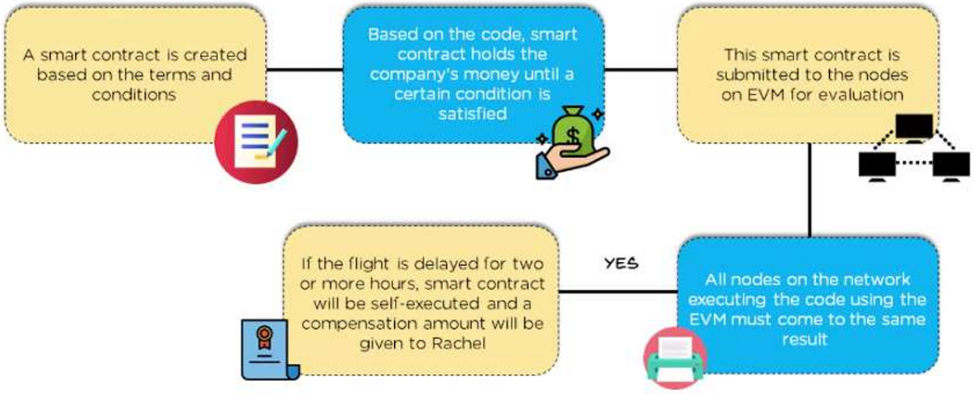

Figure 19: Flight Delay Insurance Smart Contract Use Case (from Consensus Slide 19)

- Based on the code, the smart contract holds the company's money until a certain condition is satisfied.
- This smart contract is submitted to the nodes on the Ethereum Virtual Machine (EVM) for evaluation.
- If the flight is delayed for two or more hours (verified by an external data feed/oracle), the smart contract automatically self-executes, and the compensation is given to the policyholder.
- All nodes on the network executing the code using the EVM must come to the same result, ensuring integrity.

8. Blockchain Variants

Blockchains can be categorized based on their access and participation rules, primarily into permission-less and permissioned variants.

8.1. Permission-less Blockchains (Public Blockchains)

- **Access:** Anyone can join the network, participate in consensus, and read/write transactions without any prior authorization.
- **Identity:** Participants typically operate under pseudonymous identities, not requiring real-world identification.
- **Consensus:** Commonly utilize resource-intensive consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS).
- **Examples:** Bitcoin, Ethereum.

8.2. Permissioned Blockchains (Private/Consortium Blockchains)

- **Access:** Only a restricted and pre-approved set of users have the rights to validate block transactions, create new blocks, or participate in the network.
- **Identity:** Participants are usually known and vetted entities.
- **Consensus:** Often employ more efficient consensus mechanisms suitable for closed environments, such as Paxos, Raft, or PBFT (Practical Byzantine Fault Tolerance), where only approved actors participate.
- **Examples:** Hyperledger Fabric, Corda.
- **Sub-types:** Can include private hybrid and consortium networks, allowing for different levels of decentralization and access control.

9. When to Use a Blockchain?

Blockchain technology is particularly beneficial in specific scenarios where its core properties provide significant advantages.

Consider implementing blockchain technology when:

- There is **no central authority** or trusted intermediary available or desired to manage a system, or when trust needs to be established between mutually untrusted parties.
- You need to **share data across multiple companies** or entities in a secure, transparent, and auditable manner.
- **Transactions should be visible to multiple members** of a network, ensuring transparency and accountability among all participants.
- A **permanent, immutable history** of transactions or data is required, where records cannot be altered or deleted once committed.

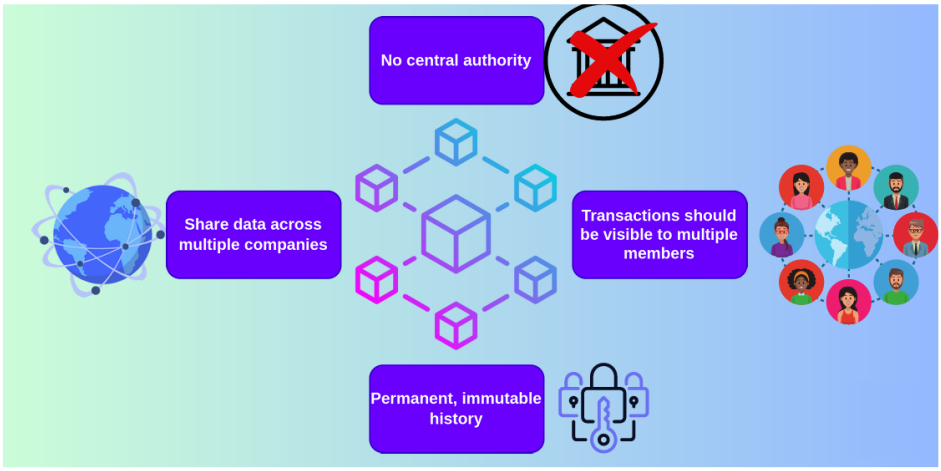

Figure 20: Conditions for Blockchain Adoption (from Slide 21)

10. Blockchain Use Cases

Blockchain technology has found extensive applications across various industries, disrupting traditional models and introducing new efficiencies and trust.

- **Cryptocurrency:** Digital currencies like Bitcoin and Ethereum for decentralized financial transactions.
- **Trade Finance:** Streamlining international trade processes, letters of credit, and supply chain finance through transparency and automation.
- **Banking:** Improving cross-border payments, settlements, interbank reconciliation, and secure record-keeping.
- **Crowd Funding:** Decentralized platforms for fundraising that bypass traditional intermediaries.
- **Insurance:** Enhancing transparency in claims processing, fraud detection, and managing policy records.
- **Legal:** Enabling digital contracts, protecting intellectual property rights, and providing immutable legal record-keeping.
- **Shared Economy:** Facilitating decentralized platforms for services like ride-sharing or asset sharing without central aggregators.
- **Real Estate:** Streamlining property titles, land registries, property transfers, and fractional ownership.
- **Internet of Things (IoT):** Securing data exchange between IoT devices, enabling automated payments, and device management.
- **Supply Chain:** Enhancing transparency, traceability, and integrity of goods from origin to consumer, reducing fraud and inefficiencies.

- **Storage:** Decentralized data storage solutions that offer enhanced security and censorship resistance.
- **Healthcare:** Securely sharing patient records, managing drug authenticity, and verifiable tracking of medical supplies.

11. Job Opportunities in Blockchain

The rapidly growing blockchain industry offers a wide array of career opportunities.
Key roles include:

- Blockchain Developer
- Smart Contract Auditor
- Blockchain Analyst
- Blockchain Architect
- Blockchain Quality Engineer
- Blockchain Consultant
- Research & Development roles
- Community Manager
- ...and many more emerging positions.

12. Blockchain Learning with Kerala Blockchain Academy

KBA provides comprehensive educational pathways for individuals interested in blockchain technology.

Figure 21: KBA QR Code

12.1. Training Programs

- Certified Blockchain Associate
- Certified Ethereum Developer
- Certified Hyperledger Fabric Developer
- Developer Essentials for Blockchain

12.2. Internships

- Certified Blockchain Architect
- Blockchain Internship Program

12.3. Educational Programs (Self-paced, Free)

- Blockchain Fundamentals
- Ethereum Fundamentals
- Hyperledger Fabric Fundamentals (JavaScript)
- Hyperledger Fabric Fundamentals (Golang)
- Corda Fundamentals

12.4. KBA Innovation Club (KBAIC)

- KBAIC is a novel initiative by Kerala Blockchain Academy (KBA) to help students from academic institutions across the country to explore deep into the potential of the blockchain technology.
- KBAIC provides an opportunity to work closely with experts and experiment the latest advancements in this domain.
- This will also help students to build their career in the disruptive world of blockchain.

13. IEEE Kerala Blockchain Group

Join the interest group using the link

Contact and Thank You

Website: kba.ai
Email: kba.admin@duk.ac.in
Phone: +91 6238210114
Medium: kbaiiitmk.medium.com
YouTube: @KeralaBlockchainAcademy

Thank you!