**TECHNICAL ARCHITECTURE OF BITCOIN**



### 

### **1. Existing Monetary System vs. Bitcoin**

#### Existing Monetary System (Fiat Money)

* Fiat currencies (such as the US Dollar, Euro, and Yen) are created and managed by governments.
* Value is based on trust in the issuing authority.
* Central authorities establish rules, policies, and enforce transaction settlement.
* Hierarchical structure: Government > Central Bank > Banks > Users.

#### Bitcoin’s Unique Architecture

* Decentralisation: Bitcoin operates without a central authority.
* Trustless System: No need to trust any single entity.
* Byzantine Generals Problem: Solving the challenge of decision-making in a distributed network.
* Blockchain: A distributed public ledger that records all Bitcoin transactions.

### **2. Bitcoin’s Main Functions**

#### a. Transaction Verification and Recording

* New transactions are grouped into “blocks.”
* Blocks are added sequentially to the blockchain.
* Each block contains a set of verified transactions.

#### b. Consensus Mechanism

* Miners compete to solve complex mathematical puzzles (Proof of Work).
* The first miner to solve it adds a new block to the blockchain.
* Consensus ensures agreement on the state of the ledger.

#### c. Ownership Tracking

* The blockchain maintains a record of ownership for all bitcoins.
* Each transaction references previous transactions (inputs) and creates new outputs.
* Outputs have associated public keys (addresses).

### **3. Participants in the Bitcoin Network**

#### a. Miners

* Validate transactions and create new blocks.
* Incentivized by block rewards (newly minted bitcoins) and transaction fees.

#### b. Nodes

* Full nodes maintain a complete copy of the blockchain.
* Verify transactions and enforce consensus rules.
* Lightweight nodes rely on full nodes for verification.

#### c. Wallets

* Store private keys (used to sign transactions).
* Generate public keys (addresses) for receiving bitcoins.
* Different types: software wallets, hardware wallets, paper wallets.

### **Conclusion**

Bitcoin’s technical architecture enables a trustless, decentralised monetary system. By understanding its functions and roles, developers can explore opportunities within this unique ecosystem or even create their own cryptocurrencies.