UNIT 2: BITCOIN AND CRYPTOCURRENCY

A basic crypto currency, Creation of coins, Payments and double spending, FORTH - the precursor for Bitcoin scripting, Bitcoin Scripts, Bitcoin P2P Network, Transaction in Bitcoin Network, Block Mining, Block propagation and block relay, Consensus introduction, Distributed consensus in open environments-Consensus in a Bitcoin network

---

Cryptocurrency: Definition, Coin Creation, and Double Spending Prevention

Definition:

A **cryptocurrency** is a decentralized form of digital money that uses cryptographic techniques to secure transactions, regulate new coin creation, and maintain a public, tamper-proof ledger through blockchain. Unlike traditional fiat currencies issued by governments or central banks, cryptocurrencies are created and managed by network participants through consensus protocols.

Steps in Coin Creation (Bitcoin Example):

1. **Transaction Collection:** Miners gather pending transactions from the network and place them into a candidate block.
2. **Block Formation:** The block is prepared with a header that includes the hash of the previous block, a timestamp, a nonce, and the Merkle root of all transactions.
3. **Proof of Work Puzzle:** Miners repeatedly adjust the nonce until they find a hash value below the required difficulty target (SHA-256).
4. **Block Broadcast:** The valid block is broadcast to the Bitcoin peer-to-peer network. Other nodes verify its validity before accepting it.
5. **Block Reward:** The miner receives newly created Bitcoins (block subsidy) along with transaction fees.
6. **Controlled Supply (Halving):** Every 210,000 blocks (~4 years), the block reward halves, ensuring that Bitcoin supply is capped at **21 million coins**.

Double Spending & Its Prevention:

- **The Problem:** In digital systems, copying is easy, so a malicious user might try to spend the same Bitcoin twice (double spending).
- **Bitcoin's Prevention Mechanisms:**
    - **Public Ledger:** All transactions are visible on the blockchain, making fraudulent duplication detectable.
    - **Consensus Mechanism (Proof of Work):** Only valid blocks mined with real computational effort are accepted.
    - **Longest Chain Rule:** If conflicting transactions exist, the chain with the most cumulative work (longest chain) is accepted as valid.
    - **Confirmations:** Once a transaction is buried under multiple subsequent blocks (commonly 6 confirmations), it becomes practically irreversible.

Analogy:

Think of Bitcoin like a **concert ticketing system**:

- Every ticket (Bitcoin) is uniquely numbered and recorded in a shared log (blockchain).
- When you enter the venue (make a payment), the ticket is marked as used.
- The system ensures that the same ticket cannot be used again for another entry (prevents double spending).

- New tickets (new Bitcoins) are released in controlled batches, like limited-edition passes, ensuring scarcity.

FORTH and Bitcoin Scripts
Definition:
Bitcoin uses a lightweight scripting system derived from **FORTH**, a stack-based programming language. The scripting language defines the rules for spending and unlocking Bitcoins.

Role of FORTH in Bitcoin Scripting:

- **Foundation:** FORTH inspired Bitcoin's scripting design because it is **simple, stack-based, and non-Turing complete**.
- **Stack-based Execution:** Each instruction operates on a Last-In-First-Out (LIFO) stack, making verification straightforward.
- **Security:** By being non-Turing complete (no loops or complex branching), it prevents infinite execution and ensures predictable, secure behavior.
- **Purpose in Bitcoin:**
  - Used to set spending conditions (**locking scripts**, scriptPubKey).
  - Used to provide proof that conditions are met (**unlocking scripts**, scriptSig).
- **Flexibility:** Supports advanced features such as multi-signatures, timelocks, and pay-to-script-hash (P2SH).

Example of a Bitcoin Script (P2PKH – Pay to Public Key Hash):

1. **Locking Script (scriptPubKey):**
2. OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
   - **OP_DUP:** Duplicates the top item on the stack.
   - **OP_HASH160:** Hashes the public key using SHA-256 followed by RIPEMD-160.
   - **:** The hashed public key of the recipient.
   - **OP_EQUALVERIFY:** Checks if the provided public key matches the expected hash.
   - **OP_CHECKSIG:** Verifies the digital signature.

👉 This script locks the coins and requires the spender to provide a valid signature and public key.

3. **Unlocking Script (scriptSig):**
4. <Signature> <PublicKey>
   - **Signature:** Proves the spender controls the private key.
   - **Public Key:** Used to verify against the in the locking script.

Execution:
When a transaction is validated, the unlocking script and locking script are combined and executed. If all conditions are satisfied (signature is valid and public key matches the hash), the transaction is accepted.

Analogy:
Think of Bitcoin scripts as a **lock-and-key system**:

- The **locking script (scriptPubKey)** is like a padlock placed on a box of coins, specifying which key can open it.
- The **unlocking script (scriptSig)** is the actual key you provide to open the lock.
- Only the correct key (signature + public key) can unlock the padlock, ensuring that only the rightful owner spends the coins.

Bitcoin P2P Network: Architecture, Functions, and Transaction Relay

Definition:

The **Bitcoin Peer-to-Peer (P2P) network** is a decentralized communication layer that connects all nodes (computers) participating in Bitcoin. It allows nodes to exchange transactions, blocks, and consensus information without relying on any central authority or server.

Architecture of the Bitcoin P2P Network:

- **Decentralized:** No central server; all nodes are equal peers.
- **Nodes:**
  - **Full Nodes:** Store the entire blockchain and independently verify every transaction and block.
  - **Mining Nodes:** Perform Proof of Work to add blocks to the chain.
  - **Lightweight Nodes (SPV Clients):** Use block headers and Merkle proofs to verify transactions without storing the full blockchain.
- **Topology:** Nodes are connected randomly across the internet, forming a mesh-like structure where each node communicates with multiple peers.
- **Redundancy:** Multiple copies of the blockchain exist across thousands of nodes, ensuring resilience against failures or attacks.

Functions of the Bitcoin P2P Network:

1. **Transaction Relay:**
   - A user broadcasts a transaction through their wallet.
   - The transaction spreads from one node to another across the network.
   - Each node independently verifies the transaction before relaying it further.
2. **Block Relay:**
   - When a miner finds a valid block, it is broadcast to peers.
   - Each receiving node validates the block and then forwards it to its peers.
   - This ensures the blockchain stays synchronized globally.
3. **Verification:**
   - Nodes verify transactions by checking digital signatures, ensuring inputs are unspent (UTXOs), and executing scripts.
   - Blocks are checked against consensus rules (difficulty, size, structure).
4. **Security and Trust:**
   - No single point of control → censorship resistance.
   - Every node enforces the same consensus rules → ensures consistency and prevents invalid data from spreading.

How Transaction Relay and Verification Work:

- A transaction is signed and broadcast to the nearest node.
- That node validates the signature and checks that the inputs are not already spent.
- If valid, the transaction is forwarded to neighboring peers.
- The process continues until the transaction reaches miners, who may include it in a block.
- Once included in a mined block and confirmed, it becomes part of the immutable blockchain.

Analogy:
The Bitcoin P2P network works like a **rumor spreading in a town**:

- One person (the sender) tells their neighbors (nodes).
- Each neighbor first checks if the rumor makes sense (validation).
- If true, they pass it to their neighbors, and so on.
- Soon, the whole town (global network) knows the rumor (transaction).
- Just as false rumors die out quickly, invalid transactions are rejected and not spread.

Life Cycle of a Bitcoin Transaction and Its Inclusion in the Blockchain
Definition:
A Bitcoin transaction is a signed digital message that transfers ownership of Bitcoin from one participant to another. The **life cycle** of a transaction describes how it moves from creation in a wallet to permanent inclusion in the blockchain.

Life Cycle of a Bitcoin Transaction:

1. **Creation:**
    - A user initiates a payment using a Bitcoin wallet.
    - Inputs (previous unspent transaction outputs, UTXOs) and outputs (recipient addresses) are defined.
    - The sender signs the transaction with their private key.
2. **Broadcast:**
    - The signed transaction is broadcast to the nearest node in the Bitcoin P2P network.
    - That node verifies the format and forwards it to peers.
3. **Validation by Nodes:**
    - Each node checks:
        - **Digital Signatures** → Is the spender authorized?
        - **Inputs** → Are the coins unspent (UTXO check)?
        - **Scripts** → Do the locking/unlocking conditions match?
        - **Consensus Rules** → Is the transaction valid under Bitcoin protocol?
4. **Mempool Storage:**
    - Valid transactions are stored in the **mempool** (memory pool), waiting for miners to include them in a block.
    - Invalid transactions are discarded and not relayed further.
5. **Selection by Miners:**
    - Miners pick transactions from the mempool, prioritizing those with higher transaction fees.
    - Transactions are bundled into a candidate block.
6. **Mining and Block Creation:**
    - Miners perform Proof of Work by finding a nonce that produces a block hash below the difficulty target.
    - When a miner succeeds, the new block (containing the transaction) is broadcast to the network.

How a Transaction Becomes Part of the Blockchain:

1. **Block Validation:** Other nodes verify the new block's integrity (hash, difficulty, block structure).
2. **Chain Extension:** If valid, the block is appended to the blockchain, extending the ledger.
3. **Confirmations:** Each new block added after it counts as one confirmation.

- After ~6 confirmations, a transaction is considered practically irreversible.

4. **Finality:** The transaction is now a permanent part of Bitcoin's immutable history.

Important Aspects:

- Transactions with low fees may remain in the mempool for a long time.
- Double-spend attempts are rejected if inputs are already spent.
- Nodes maintain consistency by always following the **longest valid chain**.

Analogy:

The life cycle of a Bitcoin transaction is like sending a **registered parcel** through a courier service:

- You prepare and sign the package (transaction creation).
- You drop it at the local branch (broadcast to the network).
- Staff verify the address and postage (validation by nodes).
- It waits in a sorting center (mempool).
- A delivery truck picks it up (miner selects it).
- It is logged into the central system and delivered (block inclusion).
- Once delivered and signed for (confirmations), the parcel's delivery record becomes permanent.

Block Mining and Nonce Discovery in Bitcoin

Definition:

Block mining is the process by which Bitcoin transactions are validated and permanently recorded on the blockchain. It involves solving a **Proof of Work (PoW)** puzzle, where miners repeatedly adjust a variable called the **nonce** to produce a valid block hash that meets the network's difficulty target.

Process of Block Mining:

1. **Transaction Collection:**
   - Miners gather pending transactions from the mempool.
   - Transactions with higher fees are prioritized.
2. **Block Formation:**
   - Transactions are bundled into a candidate block.
   - The block header includes:
     - Previous block hash,
     - Merkle root (hash of all transactions),
     - Timestamp,
     - Difficulty target,
     - Nonce (a random number miners can change).
3. **Proof of Work Puzzle:**
   - Miners compute the hash of the block header using SHA-256.
   - They repeatedly change the **nonce** and re-hash until the output hash is below the difficulty target (a hash with a required number of leading zeros).
4. **Block Discovery:**
   - Once a valid nonce is found, the block is broadcast to the network.
   - Other nodes verify it; if valid, the block is added to the blockchain.
5. **Reward:**
   - The miner receives the **block subsidy** (new Bitcoins created) + **transaction fees**.

- Block subsidy halves every ~4 years (halving event).

Importance of Nonce Discovery:

- **Ensures Security:** Makes altering past blocks computationally infeasible, since attackers must redo the work for all subsequent blocks.
- **Maintains Fairness:** Mining is like a lottery-every miner has a fair chance, but success depends on computational effort.
- **Controls Block Time:** Difficulty adjustment ensures that blocks are mined approximately every 10 minutes.
- **Prevents Spam:** High energy and resource costs deter malicious actors from flooding the system with fake transactions.

Analogy:

Block mining is like a **lock-and-key puzzle competition**:

- Thousands of miners are trying different keys (nonces) to open a vault (valid block hash).
- Only one key works, and the miner who finds it first gets the treasure inside (block reward).
- Once the vault is opened, everyone can verify the solution, and the vault is sealed forever into history (blockchain immutability).

Block Propagation and Relay in the Bitcoin Network

Definition:

Block propagation (or block relay) is the process by which a newly mined block is distributed from the miner that discovered it to all other nodes in the Bitcoin peer-to-peer network. This ensures that the blockchain remains synchronized and consistent across the entire network.

Process of Block Propagation:

1. **Block Discovery:**
   - A miner successfully finds a valid nonce and creates a new block.
2. **Initial Broadcast:**
   - The miner broadcasts the block to its directly connected peers in the P2P network.
3. **Validation by Receiving Nodes:**
   - Each receiving node performs verification checks:
     - Block structure and header are valid.
     - Proof of Work meets the difficulty target.
     - All transactions inside are valid and not double spent.
4. **Further Relay:**
   - If valid, the node forwards the block to its own peers.
   - Invalid blocks are discarded and not relayed.
5. **Global Synchronization:**
   - The process repeats until all nodes in the network have received, validated, and updated their copy of the blockchain.

Challenges in Block Relay:

- **Network Latency:** Blocks may take seconds to propagate across the globe, creating temporary inconsistencies.

- **Block Size:** Larger blocks take more time and bandwidth to transmit, slowing propagation.
- **Orphan Blocks:** If two miners solve a block at nearly the same time, some nodes may temporarily follow different versions. Eventually, the longest valid chain survives, and the other block becomes an orphan.
- **Bandwidth Load:** The network must handle thousands of nodes exchanging large amounts of data, which can cause bottlenecks.
- **Propagation Delay Attacks:** Malicious nodes may attempt to slow block relay, causing inefficiencies or forks.

Importance of Efficient Propagation:

- Ensures all nodes converge on the same blockchain state.
- Reduces the risk of forks and orphan blocks.
- Maintains fairness by minimizing the advantage of miners who discover blocks earlier.

Analogy:

Block propagation is like **breaking news spreading through social media**:

- A journalist (miner) first posts the news (new block).
- Followers (peer nodes) check the credibility before sharing.
- If valid, it spreads rapidly through retweets and shares (relay).
- Sometimes two journalists post slightly different versions at the same time (competing blocks), but eventually, the community accepts the most widely shared version (longest chain).

Consensus in Blockchain and Distributed Consensus in Bitcoin

Definition of Consensus in Blockchain:

Consensus is the mechanism by which nodes in a decentralized blockchain network agree on the validity of transactions and the single, consistent version of the ledger. Since there is no central authority in blockchain, consensus protocols are essential for maintaining trust, security, and synchronization among participants.

Why Consensus is Needed:

- To prevent **double spending**.
- To ensure all nodes share the same transaction history.
- To protect the system from malicious actors.
- To maintain decentralization without requiring trust in a central party.

How Distributed Consensus is Achieved in Bitcoin:

1. **Proof of Work (PoW):**
    - Miners solve complex computational puzzles to propose new blocks.
    - The puzzle (finding a valid hash) ensures that block creation requires real-world resources (electricity + hardware).
    - This makes attacks costly and impractical.
2. **Independent Validation:**
    - Every node independently verifies blocks and transactions against Bitcoin's rules (valid signatures, unspent inputs, correct block structure, difficulty target, etc.).
3. **Longest Chain Rule:**
    - If competing chains exist (e.g., two miners mine blocks simultaneously), nodes accept the chain with the most accumulated computational work.

- This ensures the network converges on a single, agreed history.

4. **Finality through Confirmations:**
   - A transaction becomes increasingly secure as more blocks are added on top of it.
   - After ~6 confirmations, the probability of reversal becomes negligible.

Security Against Attacks:

- An attacker would need to control **>50% of global mining power** to outpace honest miners and rewrite history (a "51% attack").
- Due to enormous computational and energy costs, such an attack is practically infeasible for Bitcoin.

Analogy:

Consensus in Bitcoin works like a **democratic election in a global classroom**:

- Every student (node) checks and votes independently on whether the assignment (block) is correct.
- Sometimes two versions circulate, but the version with the **most votes and effort** becomes the official record (longest chain).
- Just like majority agreement ensures fairness in a class, consensus ensures fairness and trust in Bitcoin.

Transaction Validation in Bitcoin and Double Spend Detection

Definition:

Transaction validation in Bitcoin is the process by which nodes verify the authenticity, correctness, and legitimacy of a transaction before it is accepted into the mempool and later added to the blockchain. This ensures that only valid transactions become part of the ledger and prevents fraudulent activities like double spending.

Stages of Transaction Validation in Bitcoin:

1. **Syntax & Structure Check:**
   - The transaction must be properly formatted.
   - Inputs, outputs, and digital signatures must follow Bitcoin's standard rules.
2. **Digital Signature Verification:**
   - Each input must include a valid digital signature created using the sender's private key.
   - Ensures the spender is authorized to use those coins.
3. **UTXO (Unspent Transaction Output) Check:**
   - Inputs must refer to **unspent outputs** from previous transactions.
   - Prevents reusing coins that have already been spent.
4. **Script Execution:**
   - The unlocking script (scriptSig) is executed with the locking script (scriptPubKey).
   - If the conditions are satisfied, the coins are unlocked.
5. **Consensus Rule Checks:**
   - Transaction size limits,
   - Fee requirements,
   - No creation of extra coins beyond rewards,
   - Block size and weight rules when included in a block.
6. **Inclusion in Mempool:**
   - If all checks are passed, the transaction enters the mempool, waiting for miners to pick it up.

Detection of Malicious Double Spends:

- **Definition of Double Spending:** An attempt to use the same Bitcoin twice in two conflicting transactions.

How Bitcoin Detects and Prevents It:

1. **UTXO Model:**
    - Each input must point to an unspent output. If one transaction spends it, the other becomes invalid.
2. **Mempool Rejection:**
    - If two conflicting transactions are broadcast, nodes will only keep the first one seen in the mempool and reject the duplicate.
3. **Consensus & Longest Chain Rule:**
    - If conflicting transactions appear in competing blocks, only the block in the longest chain survives.
    - The double-spend in the discarded block is automatically rejected.
4. **Confirmations:**
    - The more confirmations a transaction has, the harder it is to reverse. After ~6 confirmations, the probability of a double-spend succeeding is practically zero.

Analogy:

Transaction validation is like **bank cheque processing**:

- The bank checks the cheque's format, verifies the signature, ensures the account has sufficient balance, and cross-checks against fraudulent duplicates.
- Similarly, Bitcoin validates structure, signatures, and unspent balances, rejecting attempts to "cash" the same cheque twice (double spend).

Centralized vs Decentralized Consensus and Trust in Bitcoin

Definition:

Consensus is the process of achieving agreement on the validity of transactions and the state of the ledger. In centralized systems, a single authority decides; in decentralized systems like Bitcoin, agreement emerges collectively through consensus protocols.

Centralized vs Decentralized Consensus:

Aspect	Centralized Consensus (e.g., Banks)	Decentralized Consensus (e.g., Bitcoin)
Decision Authority	A single central entity (bank, government)	Collective agreement among many nodes
Trust Model	Trust placed in the central authority	Trust placed in math, cryptography, and protocol
Speed	Fast (single authority decides immediately)	Slower (network must validate globally)
Transparency	Limited (closed ledgers)	High (public blockchain visible to all)
Security	Vulnerable to corruption or single-point failure	Highly secure but requires large resources to attack
Scalability	Easier to scale with central servers	Harder to scale due to global consensus
Examples	Central banks, Visa, PayPal	Bitcoin, Ethereum

How Bitcoin Ensures Trust Without a Central Authority:

1. **Proof of Work (PoW):**

- Blocks are only accepted if miners show proof of computational effort, making fraud costly and impractical.

2. **Independent Validation:**
   - Every node verifies transactions and blocks independently (signatures, UTXOs, rules).
   - No need to trust a third party-each participant checks for themselves.
3. **Public Ledger Transparency:**
   - All transactions are publicly recorded on the blockchain.
   - Anyone can audit the system, ensuring accountability.
4. **Longest Chain Rule:**
   - The chain with the most accumulated PoW is considered valid.
   - Ensures consistency even if temporary forks occur.
5. **Immutability & Confirmations:**
   - Once included in a block and buried under more confirmations, reversing a transaction becomes practically impossible.

Analogy:

- A **centralized consensus** is like a **school teacher grading everyone's papers**-the decision is fast, but you must trust the teacher's fairness.
- A **decentralized consensus** is like a **peer review system** where all students check each other's work. It takes longer, but errors and fraud are nearly impossible to slip through because everyone verifies independently.

Block Mining in Bitcoin and Incentive Mechanism for Miners

Definition:

Block mining is the process of validating Bitcoin transactions and adding them to the blockchain through **Proof of Work (PoW)**. Miners compete to solve a mathematical puzzle by finding a nonce that generates a valid block hash. As a reward for securing the network, miners receive newly minted Bitcoins and transaction fees.

Process of Block Mining (with Example):

1. **Transaction Collection:**
   - Pending transactions from the mempool are gathered by miners.
   - Transactions with higher fees are prioritized.
2. **Block Formation:**
   - Miners create a candidate block with:
     - A list of transactions,
     - Previous block hash,
     - Merkle root,
     - Timestamp,
     - Difficulty target,
     - Nonce (variable number).
3. **Proof of Work Puzzle:**
   - The block header is hashed using SHA-256.
   - Miners try billions of nonce values until the hash produced is below the network's difficulty target.
4. **Block Broadcast and Validation:**
   - Once a valid nonce is found, the miner broadcasts the block.

- Other nodes validate it before adding it to their copy of the blockchain.

Example:

- Suppose the network requires a hash starting with **"0000"**.
- Miner A hashes the block header with nonce 10002 → output starts with **"7d4c"** → invalid.
- Miner B hashes with nonce 23489 → output starts with **"0000af"** → valid.
- Miner B wins the race, broadcasts the block, and earns the block reward.

Incentive Mechanism for Miners:

1. **Block Subsidy (New Coins):**
   - Each mined block rewards the miner with new Bitcoins (currently 6.25 BTC).
   - This amount halves every 210,000 blocks (~4 years) in an event called the **halving**, ensuring scarcity.
2. **Transaction Fees:**
   - Users attach fees to transactions to incentivize miners to include them quickly.
   - As block subsidy decreases over time, transaction fees will become the primary incentive.
3. **Security Incentive:**
   - High rewards motivate miners to act honestly.
   - Dishonest behavior (e.g., double spending, invalid blocks) wastes computational resources and provides no reward.
4. **Long-Term Sustainability:**
   - By 2140, all 21 million Bitcoins will have been mined.
   - After that, miners will be incentivized purely through transaction fees.

Importance of Incentives:

- Keeps miners actively securing the network.
- Distributes new coins into circulation fairly.
- Ensures continuous participation even after subsidies end.

Analogy:

Mining in Bitcoin is like a **global lottery system**:

- Miners buy tickets by burning electricity and computational power.
- The first miner to pick the winning ticket (valid nonce) wins the prize (block reward + fees).
- Just like lotteries prevent cheating by requiring everyone to follow the same rules, Bitcoin mining ensures fairness and trust in the system.
