Lecture 9: Blockchain Mining and Security Mechanisms

Mempools: How Transactions Are Stored Before Mining

- A **mempool** (memory pool) is where **unconfirmed transactions** are stored before they are included in a block.
- Each node maintains its own **mempool**, but in an ideal network, all nodes should eventually have the same transactions in their mempools.
- Mempools can differ temporarily due to network latency and local policies.
- All nodes eventually receive the same transactions and update their mempools to reflect the confirmed state of the blockchain.
- This ensures that the network maintains consistency and integrity over time.
- Transactions with **higher fees** are given priority since miners prefer transactions that reward them the most.

CPUs vs GPUs vs ASICs: Hardware Used in Mining

Hardware	Processing Power	Energy Efficiency	Use Case
CPU (Central Processing Unit)	Low	High Power Consumption	Not suitable for modern mining
GPU (Graphics Processing Unit)	Medium	Moderate	Used for Ethereum mining before PoS transition
ASIC (Application-Specific Integrated Circuit)	Very High	Low Power Consumption	Used for Bitcoin mining

- **ASIC miners** are the most powerful and efficient but expensive.
- **GPU mining** is still used for certain cryptocurrencies, but Bitcoin mining is dominated by ASICs.

Mining Pools: Solving Blocks Collectively

- A **mining pool** is a group of miners who share computational power to solve cryptographic puzzles faster.
- Rewards are distributed among participants based on their contribution to solving the block.
- Mining pools increase the chances of **regular rewards** compared to solo mining.

51% Attack: The Major Blockchain Threat

- If a single miner or mining pool **controls more than 50%** of the network’s computing power, they can manipulate the blockchain.
- This would allow them to:
  - **Double spend** coins by reversing transactions.
  - **Prevent new transactions** from being added to the chain.
  - **Alter historical transactions**, rewriting blockchain history.
- **Prevention Measures:**
  - Decentralized mining by distributing hash power.
  - Using **Proof-of-Stake (PoS)** or hybrid consensus mechanisms.

Byzantine Fault Tolerance (BFT)

- BFT ensures a blockchain remains secure even if some nodes behave maliciously.
- It states that a network can tolerate up to **1/3 of nodes being traitors** while still functioning correctly.
- **Key concept:** If honest nodes form a majority, the system remains secure and reaches consensus.

Lecture 10: Transactions and UTXO Model

Understanding Transactions in Blockchain

- A transaction in blockchain represents the transfer of assets (e.g., Bitcoin) from one address to another.
- Transactions are digitally signed using **private keys** to ensure authenticity.

UTXO: Unspent Transaction Output Model

- **UTXO (Unspent Transaction Output)** represents the remaining balance after a transaction.
- Each transaction **consumes UTXOs** from previous transactions and creates **new UTXOs**.
- **Key Advantage:** Prevents **double spending** since each UTXO can only be spent once.

Example 1: Basic UTXO Transaction

1. Alice has **5 BTC** and wants to send **3 BTC** to Bob.
2. The transaction inputs:
   - **Alice's 5 BTC UTXO** is spent.
3. The transaction outputs:
   - **Bob receives 3 BTC** (new UTXO for Bob).
   - **Alice gets 2 BTC change** (new UTXO for Alice).

Example 2: Complex UTXO Transaction

1. Alice has two UTXOs: **2 BTC and 3 BTC**.
2. She wants to send **4 BTC** to Bob.
3. The transaction inputs:
   - Alice spends **both UTXOs (2 BTC + 3 BTC)**.
4. The transaction outputs:
   - Bob gets **4 BTC**.
   - Alice gets **1 BTC** in change.

Where Do Transaction Fees Come From?

- **Transaction Fee = Inputs - Outputs**
- Miners collect transaction fees as an incentive to include transactions in a block.
- Users can **increase fees** to get their transactions confirmed faster.

UTXO of a Miner

- Miners receive rewards in the form of **newly minted coins + transaction fees**.
- These rewards are also stored as UTXOs and can only be spent once they mature after a set number of blocks.

Summary of Key Learnings

✅ **Mempools store pending transactions before they get added to a block.**
✅ **ASIC miners dominate Bitcoin mining due to high efficiency.**
✅ **Mining pools allow miners to combine resources and increase success rates.**
✅ **A 51% attack can manipulate transactions, but decentralization prevents it.**
✅ **Byzantine Fault Tolerance ensures the system remains secure even with some malicious nodes.**
✅ **The UTXO model prevents double spending by ensuring each output can be used only once.**
✅ **Transaction fees incentivize miners to prioritize high-fee transactions.**
