CS6290 Privacy-enhancing Technologies
Tutorial 3

In this tutorial, we continue to revisit the original Bitcoin whitepaper [Nak08]. We have prepared some questions for you. Note that the goal is not to memorize answers but to **connect** technical details to Bitcoins core principles (decentralization, censorship resistance, trust minimization).

Question 1: What is a "Coin" in Bitcoin?

If Bitcoin doesnt track coins directly, how does it prevent users from double-spending the same BTC?

(**Hint:** Bitcoin uses transaction outputs (UTXOs) instead of physical coins (Section 2); How nodes verify UTXO validity? (Section 5))

Question 2: Double-Spending and Consensus

Why is the order of transactions more important than validating individual transactions to prevent double-spending?

(**Hint:** How Bitcoin timestamps transactions via blocks (Section 2)?; Think about how conflicting transactions are resolved.)

Question 3: Proof-of-Work vs. Alternatives

Why does Bitcoin use computational work (PoW) instead of one IP address, one vote for consensus?

(**Hint:** Consider the problem of Sybil attacks (Section 4); What makes PoW expensive to fake, and why is this cost critical for security?)

Question 4: Miner Incentives and Long-Term Security

If block rewards decrease over time, why would miners continue to secure the network?

(**Hint:** Consider the problem of Sybil attacks (Section 4); What makes PoW "expensive" to fake, and why is this cost critical for security?)

Question 5: Merkle Trees and Efficiency

How do Merkle trees allow lightweight clients (like mobile wallets) to verify transactions without storing the entire blockchain?

(**Hint:** How Merkle roots summarize all transactions in a block? (Section 7); How does this design enable secure, partial verification (e.g., checking if a transaction is included in a block)?)

References

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008. Accessed: 2025-01-24.