CS6290 Privacy-enhancing Technologies
Tutorial 2

Question 1: The Longest Chain Rule

Q1-a: In the proof-of work system, an attacker should modify all the blocks after the block he attack in to prevent being blocked by the system. If the chain is longer, the attacker's workload will be larger. So that the probability of an attacker's attack success decreases over time?

Answer: The answer is **Yes**. In a Proof-of-Work (PoW) system, the security of the blockchain is based on the *computational effort* needed to add blocks to the chain. If someone wants to attack the blockchain (for example, by changing a transaction in an earlier block), they can't just change that one block. Why? Because each block is linked to the one before it, and if you change one block, all the blocks after it become invalid. So, the attacker would have to **redo** the computational work (or "mining") for that block and all the blocks after it to make their new version of the blockchain the longest and most valid.

This ties directly into the **longest chain rule**, which states that the blockchain with the most cumulative computational work (or equivalently, the longest valid chain) is treated as the legitimate chain by the network. For an attack to succeed, the attacker must not only rewrite the target block but also extend their version of the chain so that it becomes longer than the honest chain. As miners in the network continue to add blocks to the legitimate chain, the attacker falls further behind, making it increasingly difficult for them to overtake the honest chain.

Now, heres the tricky part for the attacker: while theyre trying to catch up, the rest of the network is still mining new blocks and extending the chain. The longer the chain gets, the more computational work the attacker has to do to catch up and overtake it. Because of the longest chain rule, the network will only accept the attackers chain if it is the longest, meaning it has the most computational effort behind it. This means the longer the chain grows, the harder it becomes for the attacker to succeed, as they need exponentially more resources to match and surpass the honest miners.

Q1-b:

If during the time, old blocks are compacted by stubbing off branches of the tree, the chain will be shorter and the system will not be as safe as before?

Answser: Compacting old blocks by stubbing off branches of the Merkle tree does not make the Bitcoin system less safe. This process involves removing unnecessary transaction data from old blocks while retaining the Merkle root. The Merkle root is a cryptographic hash that encapsulates the integrity of all transactions in the block, meaning that as long as the Merkle root remains intact, the blocks validity and the security of the blockchain are preserved.

The reason this does not compromise safety is that the Merkle root is included in the block header, which is part of the cryptographic chain of blocks. Any attempt to alter past transactions would require recomputing the Merkle root and invalidating the

cryptographic link to subsequent blocks. This process is computationally infeasible due to Bitcoins proof-of-work consensus mechanism. Compacting old blocks improves storage efficiency without affecting the trustworthiness or security of the system, as the essential cryptographic proofs remain intact.

Question 2: The Routine Escrow Mechanism

Q2-a: What is the meaning of "routine escrow mechanisms" in the Bitcoin paper?

Answer: "*Escrow* is a legal concept describing a financial agreement where assets or money are held by a neutral third party on behalf of two other parties that are in the process of completing a transaction."[1] Think about this example: we buyers need to ensure that we can get what we have paid. Or, we could get our money back.

Q2-b: Can Bitcoin achieve "routine escrow mechanisms"?

Answer: In the blockchain context, such routine escrow mechanisms can be achieved through its **scripting language** (i.e., *smart contract*, which we will learn later in this course). For those interested, please see more explanations on this page.

Question 3: Transaction Broadcasting

In the network section of the Bitcoin paper, it is stated at the very beginning that new transactions are broadcast to all nodes. However, later in the section, it is mentioned that new transaction broadcasts do not necessarily need to reach all nodes. Why?

Answer: At the beginning of the network section in the Bitcoin paper, it is stated that new transactions are broadcast to all nodes. This reflects the idealized design principle of the Bitcoin network, where the goal is for every transaction to propagate widely, ensuring that all nodes have access to the same set of transactions. This broad dissemination supports the systems decentralized consensus, as nodes need to verify and include transactions in blocks, and consistent information helps prevent issues like double-spending.

For statement about transaction broadcasting in the last part, it acknowledges practical realities of a decentralized network, where redundancy and block propagation mechanisms compensate for incomplete dissemination. Transactions that do not directly reach all nodes are included in mined blocks, which are then broadcast to the network, ensuring eventual consistency. This design balances efficiency with resilience, as the system can tolerate missed broadcasts without compromising security or integrity.

[1] https://www.investopedia.com/terms/e/escrow.asp