Theoretical Part

1. Blockchain Basics

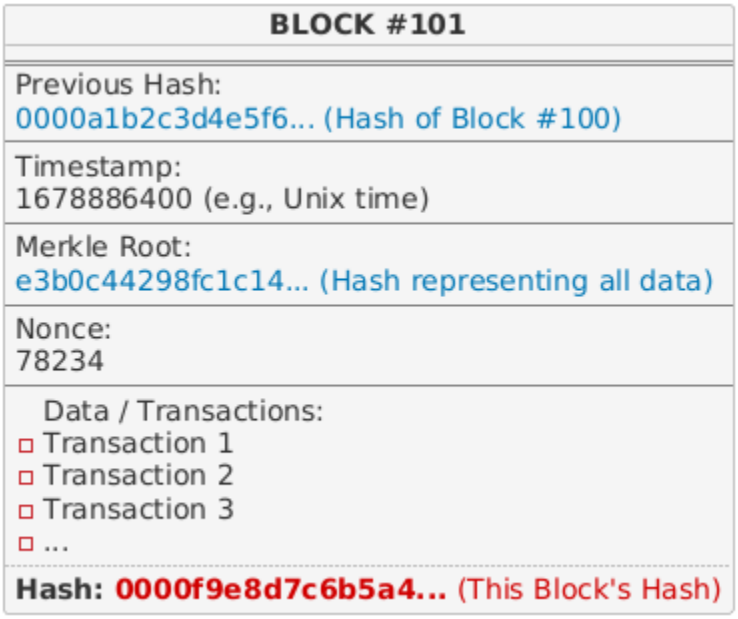
A blockchain is an immutable and decentralized digital ledger that is specifically created to record transactions openly and securely. It consists of a growing chain of "blocks", with each block having a number of transactions, a timestamp, and a hash of the preceding block. The hash is used to link the blocks, creating a chronological and immutable chain. Because the ledger is spread across a network of computers, no one company or person controls it, and thus it is highly resistant to tampering or censorship. All the participants in the network and all participants have a copy of the ledger, and new blocks are added only after the participants in the network agree, thus ensuring the validity and integrity of the entire chain.

List 2 real-life use cases:

1. **Supply Chain Management:** Blockchain technology allows for an immutable and secure history of a product's journey from source to end user. Each step, from growing to processing, shipping, and ultimate delivery, can be logged as a transaction on the blockchain network. This feature can be employed to authenticate the authenticity of products (e.g., high-end products and organic products), prevent counterfeiting, improve traceability of products in product recalls, and impose accountability on all such stakeholders (producers, shippers, retailers).
2. **Digital Identity:** Blockchain technology allows for self-sovereign identity, where one is fully in control of his or her own information. Instead of being reliant on centralized players like Google or government bureaucracies, a person's identity credentials—birth certificates, driver's licenses, and diplomas—can be safely stored on a blockchain. This allows individuals to selectively disclose specific, verifiable details of their identity to third parties without transmitting irrelevant data, enhancing security and privacy.

2. Block Anatomy

Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.



Briefly explain with an example how the Merkle root helps verify data integrity.

A Merkle root is a single hash containing all the transactions contained in a block, created by hashing pairs of transaction hashes together over and over again until only one hash is left.

For example, take a block with four transactions, i.e., TX1, TX2, TX3, and TX4.
First, each transaction is hashed separately, where H1 = hash(TX1), H2 = hash(TX2), H3 = hash(TX3), and H4 = hash(TX4).
Then, we hash pairs of these hashes: H12 = hash(H1 + H2) and H34 = hash(H3 + H4).
Lastly, we compute the hash of the resulting pair to obtain the Merkle root: Merkle Root = hash(H12 + H34).

The Merkle Root is stored in the block header. If the attacker was to alter even a single character in TX3, the corresponding value of H3 would see a drastic change. This would cascade upwards, thus changing H34 and finally leading to a vastly different Merkle Root. The integrity of the data can be simply checked by re-computing the Merkle root and comparing with the value stored in the block header. If there is a mismatch, it would mean that the data has been tampered with.

3. Consensus Conceptualization

What is Proof of Work and why does it require energy?

Proof of Work (PoW) is a consensus mechanism where nodes in the network, called "miners," compete to solve a difficult math puzzle. The victor of the competition, the first miner to solve it, has the privilege of adding the next block of transactions to the blockchain and is rewarded in cryptocurrency. The puzzle is to have the miners make an educated guess at a number (a "nonce") that, when combined with the data of the block and hashed, produces a value that meets a specified difficulty level (e.g., a hash that starts with some number of zeros). This is a power-consuming operation, since the solution to the puzzle is more or less a brute-force endeavor; there is no other option than to take trillions of guesses per second, which requires the use of high-speed, custom-made computing equipment (e.g., ASICs) that burn enormous amounts of electrical power.

What is Proof of Stake and how does it differ?

Proof of Stake (PoS) is another consensus algorithm in which groups or individuals, known as "validators," are chosen to construct new blocks based on the amount of cryptocurrency they own and are willing to "stake" or offer as collateral. The network conducts a random selection process to choose a validator who will propose the next block, whose chances of selection are usually directly related to the size of their stake. This algorithm is the opposite of Proof of Work (PoW) since it replaces economic competition with computational competition. Instead of using energy to verify their work, validators risk their own capital. On being guilty of malicious actions, their stake can be subject to "slashing" (i.e., seizure), thus encouraging honest behavior and making the system over 99% more energy-efficient compared to PoW.

What is Delegated Proof of Stake and how are validators selected?

Delegators' Proof of Stake (DPoS) is a Proof of Stake (PoS) alternative designed to improve both transaction speed and operation efficiency. Token holders do not directly validate blocks in a DPoS system but instead vote for a fixed, limited number of "delegates" (or "witnesses") from their balances. The chosen delegates are only tasked with creating and validating new blocks for the network. The validators (delegates) are voted for by an ongoing on-chain election. The user holding more tokens has more voting power. This configuration creates a representative democracy, where a few

trusted and high-capacity nodes secure the network, allowing for faster consensus and greater throughput compared to traditional PoS or Proof of Work (PoW).