

Blockchain Technology

Assignment 3

Name: Vannchannida ANG

Class: FDE C6 (Afternoon)

Answer:

1. What are the essential fields inside a blockchain transaction?

The essential fields inside a blockchain transaction are:

- Sender's address
- Recipient's address (receiver)
- Amount (how much money is being sent)
- Nonce: Transaction count of the sender)
- Fee/Gas (payment for network work)
- Digital Signature: cryptographic proof generated using the sender's private key.
 - Proves ownership
 - Ensure integrity

2. How does the network verify a transaction's authenticity (the quality of being genuine or real)?

The network verifies a transaction's authenticity through a combination of cryptography and consensus.

- Cryptography verification (digital signature):
 - Sign the transaction: Users use their unique private key to create a digital signature for the transaction, providing they authorized it.
 - Broadcast the transaction: The signed transaction is sent out to the network of participating computers (nodes)
- Node validation

-
- Check the digital signature: Each node verifies that the signature is valid by checking if it corresponds to the sender's public key. This confirms the transaction wasn't altered and was initiated by the correct person.
 - Confirm sufficient funds: Nodes also check that the sender has enough cryptocurrency in their wallet to complete the transaction.
- Consensus algorithm:
 - After passing the initial cryptographic check, the transaction is pooled with others into a mempool. Miners (in Proof of Work) or Validators then compete to bundle these transactions into a new block
 - This new block is broadcast to the entire network.
 - Agreeing on the validity of a transaction or on which version of the blockchain is the real one and immutable
 - Assures that the protocol rules are being followed and guarantees that all transactions occur in a trustworthy way.
 - Allows the creation of a blockchain system with high resistance to attack.
 -

3. Why are transaction fees necessary?

- Incentive for network validators (rewards Miners/ Stakers for work)
- Higher fees mean faster confirmation
- Fees depend on demand and complexity

4. What happens if a transaction fails?

Firstly, a transaction can fail for many reasons, including having an insufficient gas limit or an offer that is no longer valid. And if so, it gets lost in the system and is eventually forgotten. The money never leaves your wallet; it just goes back to being spendable after a short while.

5. Why is keeping your private key safe so important?

Safeguarding one's private key is paramount in the blockchain ecosystem because it represents absolute and irretrievable ownership of digital assets. Unlike a traditional

bank password, a private key cannot be reset or recovered by a central authority; the user bears sole responsibility for its security. Anyone in possession of the private key can generate the digital signatures required to authorize transactions, thereby gaining full control over the associated assets. If a private key is lost, the assets it controls become permanently inaccessible. Conversely, if a private key is stolen, the thief can irreversibly transfer all funds to their own wallet, with no recourse for the original owner. Therefore, the security of the private key is synonymous with the security of the assets themselves.