THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

Date 21/03/23

Assignment 2

Q.1 Explain transactions in blockchain and UTXO and Double Spending.

⇒

Transaction :

- A blockchain's basic building block is a transaction.
- Currency is transferred from one address to another during a transaction.
- A transaction is a piece of cryptographically signed instructions issued by an externally owned account, serialized and then uploaded to a blockchain.
- On Ethereum, a transaction is a data packet that has been digitally signed using a private key and contains the instruction that, when followed, either lead to a message call or the establishment of a contract.
- Based on the output they generate, transactions may be classified into two types :

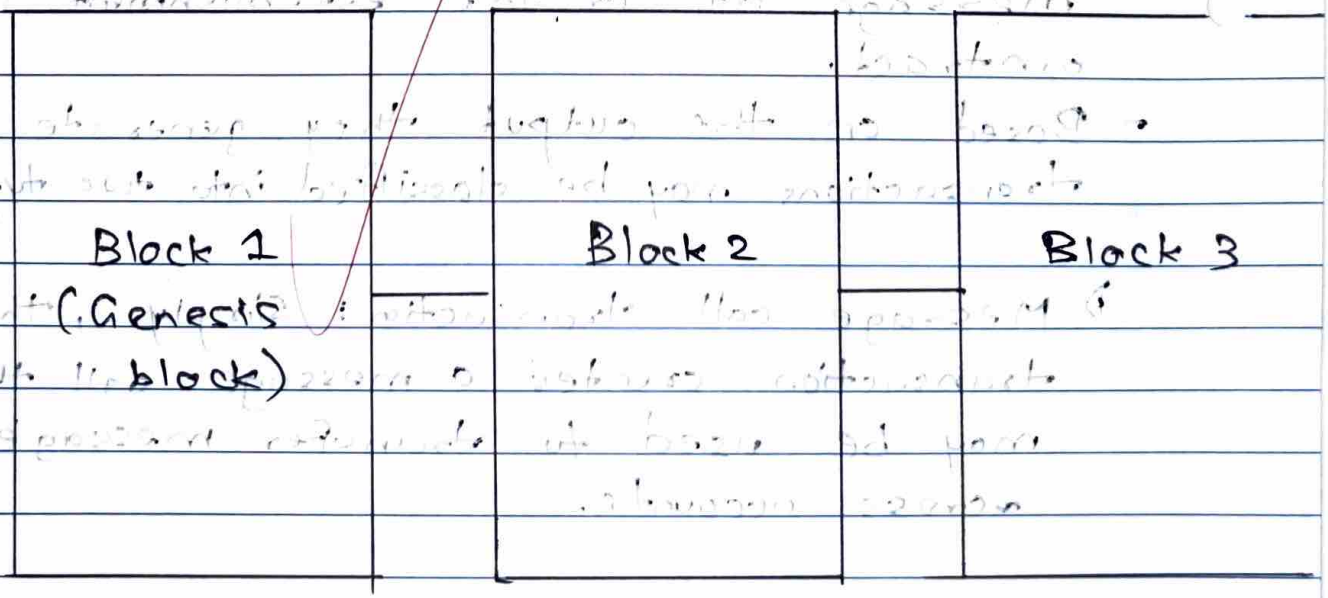
1) Message call transaction : Simply, this transaction creates a message call that may be used to transfer message across accounts.

THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

2) Contract creation transaction: As the name implies, a new contract is made as a result of these transactions. This indicates when this transaction is completed successfully, an account is created with the corresponding code.

- **Unspent Transaction Output (UTXO):**

- Blockchain is a digital, decentralized, distributed ledger.
- Blockchain utilizes a P2P (Peer-to-Peer) network, where participants present on the network are called nodes.
- The ledger stores data about transaction. It is a chain of blocks, where its most significant feature is that blocks are cryptographically linked together.



- In bitcoin, the transaction lives until it has been executed till the time another transaction is done out of that UTXO.
- It is the amount of digital currency someone has left remaining after executing a transaction.
- When a transaction is completed, the unspent output is deposited back into the database as input which can be used later for another transaction.
- UTXOs are created through the consumption of existing UTXOs. Every Bitcoin is composed of inputs and outputs.
- Inputs consumes an existing UTXO, while outputs create a new UTXO.

Double Spending :

- Although blockchain is secured, still it has some loopholes.
- Hackers or malicious users take advantage of these loopholes to perform their activities.
- Double spending means the expenditure of the same digital currency twice or more to avail the multiple services. It is a technical flow that allows users to duplicate money.

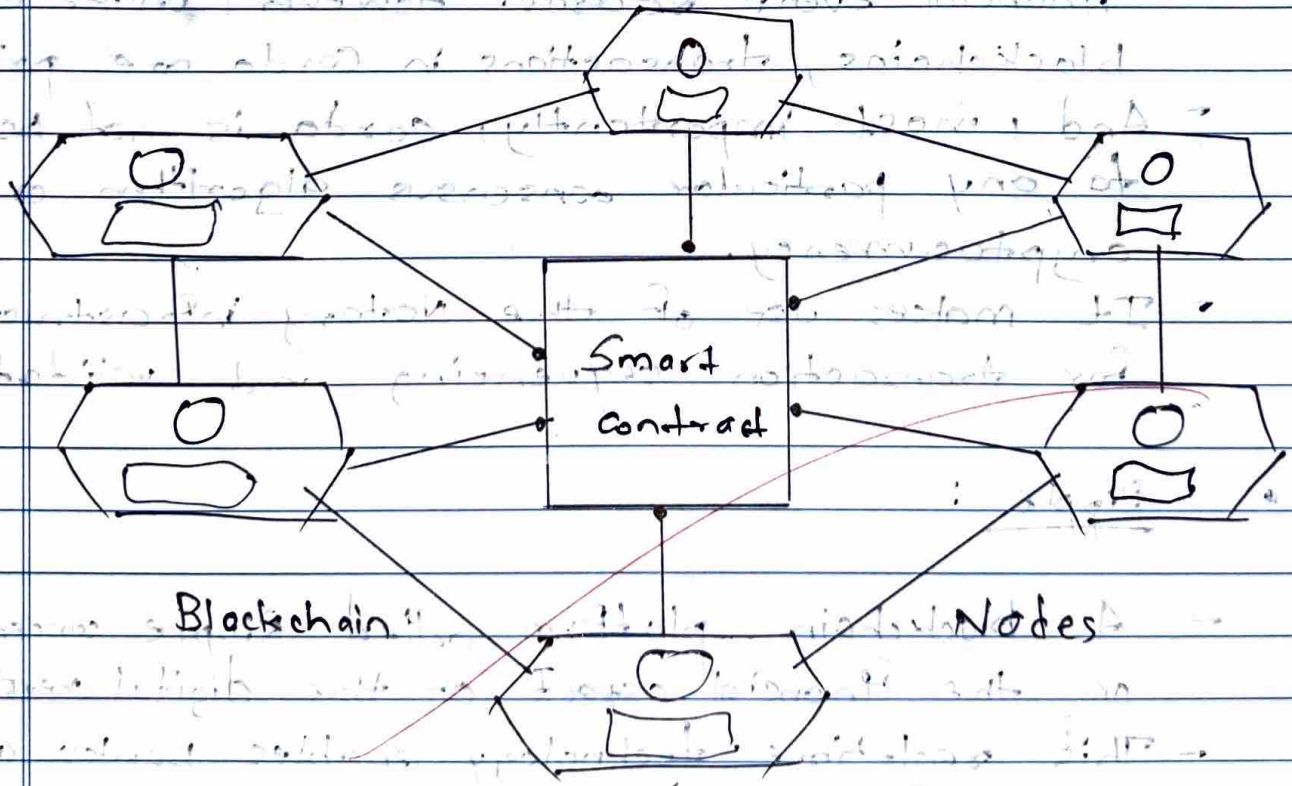
- Since digital currencies are nothing but files, a malicious users can create multiple copies of the same currency file and can use it in multiple places.
- This issue can also occur if there is an alteration in the network or copies of the currency are only used and not the original one.
- There are also double spends that allows hackers to reverse transactions so that transaction happens two times.
- By doing this, the user loses money two times one for the fake block created by the hacker and for the original block as well.
- The hacker gets incentives as well for the fake blocks that have been mined and confirmed.

Q.2 Explain in detail CORDA, Ripple and Quorum

⇒

- **Corda :**

- It is a blockchain that is open-source and uses smart contracts to let companies deal privately and directly.
- Corda is a distributed ledger technology (DLT) that R3 created specifically for enterprise use, with privacy as the guiding principle.



- The Corda protocol is built on a strong identity model, where every node's identity must be proven to have been properly on boarded by using X.509 certificate

- Corda is a custom-designed for financial industry.
- It reduces record-keeping expenses and offers development services like Corda App Consulting, User Interfaces, Regulated tokens, and others.
- The distributed apps created with Corda are known as Cordapps.
- Signing identities are only available on Corda Nodes.
- Corda enables the creation of immutable financial event records. However, unlike other blockchains, transactions in Corda are private.
- And, most importantly, Corda is not bound to any particular consensus algorithm or cryptocurrency.
- It makes use of the Notary infrastructure for transaction sequencing and validation.

- **Ripple :**

- A blockchain platform called Ripple concentrates on the financial aspect of the digital revolution.
- This real-time technology enables banks and other financial institutions to transmit payment transactions across the globe in real time.
- Ripple is an open-source person-to-person payment network that allows anyone in the world to send money to anyone

elese for free.
- For banks and payment processors, Ripple Labs aims to make it simple and affordable to send money abroad.
- There is a big problem when your want to send money from one country to another country.
- Sometimes it takes days and it is usually expensive, and in some countries you even have to do illegal things to make it happen.
- Ripple's primary goal is to eliminate the need for older system such as Western Union or Swift.
- Ripple is a distributed payment protocol.
- Ripple is emerging as the next promising virtual currency.

- **Quorum :**

- A distributed ledger protocol called Quorum is based on Ethereum.
- As Quorum only modifies Ethereum's core slightly, it is intended to grow and change alongside Ethereum.
- It is a JP Morgan's Enterprise focused blockchain which is open source.
- Quorum is a free and open source blockchain protocol designed specifically for use in a private blockchain network, in which multiple

members each own a portion of the network.

- It is a software of the very well-known public Ethereum blockchain.
- Quorum is Ethereum blockchain aimed specifically at the finance sector.
- It is created solely to provide privacy for private transactions between nodes.
- The main feature of Quorum is privacy. Transactions and smart contracts on the blockchain can be private.
- Quorum features multiple voting based consensus mechanisms that do away with the current proof-of-work consensus algorithm used by public Ethereum blockchain.
- Quorum can be run with two different privacy options, Tessera and Constellation, which are used by Quorum to encrypt and data among nodes.
- Transactions on the Quorum network don't cost Ether. Voting is the primary method of transaction verification, a mechanism for agreement.

Q.3 Explain 0, 1 and 6 confirmation transaction.

⇒

In the context of blockchain technology, the terms "0 confirmation", "1 confirmation" and "6 confirmation" refers to the number of blocks that have been mined on top of a given transaction's block in a blockchain.

0 transaction

- A 0 transaction is one that has been broadcasted to the network but has not yet been included in a block.
- This means the transaction is still in the mempool where transaction's are stored while waiting to be included in block by miners.
- Status: Pending, not yet confirmed by the blockchain.
- Risk: The transaction can still be canceled or replaced by the sender, making it susceptible to a "double-spend-attack" where the sender tries to use the same funds in another transaction.
- Use: Merchants or individuals usually avoid accepting 0 confirmation transaction for large payments because they are not secure.

1 Confirmation Transaction :

- A 1 confirmation transaction has been included in a block, meaning that one block has been mined containing the transaction, and it is officially part of the blockchain.
- Status : The transaction is confirmed and recorded in the blockchain, but only one block has been mined after the transaction.
- Risk : Although it is more secure than 0 confirmation transaction, a 1 confirmation transaction could theoretically still be reversed if a malicious miner reorganizes the blockchain by creating a longer competing chain.
- Use : Some businesses or individuals may accept transactions with 1 confirmation for smaller or lower-risk transactions because the chances of a reversal are low, but not negligible.

6 confirmation Transaction :

- A 6 confirmation transaction has been confirmed by the network and included in a block, and five additional blocks have been mined on top of it.

- Status: Very secure. The transaction is now deeply embedded in the blockchain and the probability of it being reversed is extremely low.
- Risks: The risk of reversal at this point is practically negligible because altering a transaction this deep in the chain would require an attacker to recognize the six blocks.
- Use: Most exchanges, merchants and businesses consider 6 confirmations as the gold standards for security, especially for high-value transactions. Once a transaction has six confirmations, it is generally considered irreversible.

Q.4: What is smart contract? How crowd funding platforms can be managed using smart contracts?

⇒ Smart Contract:

- The smart contract is the software program implementing a set of rules or conditions and operates on the top of a blockchain.
- These set of rules are used by different parties to that smart contract to transfer the digital assets between them.
- Based on set of rules implemented in smart contracts, different parties to the smart contracts agree to interact with each other.
- This agreement automatically gets executed after fulfilling the predefined rules.
- The smart contracts code execute, validate and ensure the transaction or agreement.
- Hence, they are fully automated and it is possible to automate the records of real-life agreements related to purchase and sale of assets.
- A smart contract implements security coding of the blockchain and include details and permissions that require a precise sequence of events to happen to trigger agreement of the terms stated in the smart contract.

- **How Crowdfunding Platforms can be managed using smart contracts :**

- Crowdfunding platforms can be greatly enhanced using smart contracts to automate the process of collecting and distributing funds while ensuring transparency and security.

1) **Decentralized Fund Collection**

⇒ Smart contracts can be programmed to accept funds from investors or backers of a crowdfunding project.
- Contributors send funds directly to the smart contract, eliminating the need for intermediaries like traditional crowdfunding platforms.
- A goal amount can be set in the smart contract

2) **Conditional based Fund Release**

⇒ IF the fund raising goal is met by a specific deadline, the smart contract automatically releases the funds to the project creator.
- IF the goal is not met, the smart contract automatically refunds the contributors, ensuring transparency and reducing the risk of fraud.

30/09/24