IT465 - Cryptocurrencies and Blockchain Technologies

Lab - Assignment 11

Name: Chinmayi C. Ramakrishna Date: 1/10/2021

Roll No: 181IT113

1) Write the difference between centralised, decentralised and distributed system.

Feature	centralised system	Decentralised system	Distributed system
Architecture	Uses client/server architecture. Built around a single, central node which has control over the network. Client nodes are connected to this central node and submit requests to the central node.	A combination of peer-to-peer architecture & master-slave architecture. A decentralised system divides workload among various devices (nodes) in the network.	A combination of peer-to-peer network, master-slave network and n-tier architecture. All nodes are peers and work towards common goal. One nodes or some nodes become server for intermediate nodes.

			Different parts of application are distributed in different nodes
Components	Nodes Master node Communication link	Nodes Communication Link	Nodes Communication Link.
Communi-cation.	Delegation within the network is relatively simple and less cross-chatter is required within different levels of authorization	There exist many central units that create groups within the network. All members of the same group have direct communication access to each other, which means information does not need to pass through an intermediary node.	The burden of data processing is distributed across the network. All users have equal access. Decision-making requires a consensus mechanism

Scalability	Easy to add/ remove clients from main server. Vertical scalability limited due to the hardware limitation of central node.	Vertical scaling is possible. Each node can add resources to itself to increase performance.	Horizontal and vertical scaling is possible. New nodes can be added to the network to increase scalability.
Affordability	Very cost effective. When patch or update is required, only the central server needs to be updated	Not beneficial to build and operate small decentralised systems because of the low cost-benefit ratio.	Distributed networks require more resources to maintain or reconfigure. An update requires change in every node.
Consistency	Increased consistency. Its easier to standardise interactions between server and the client.	The communicating components achieve local consistency. Local consistency further guarantees global consistency.	There is no way to regulate individual nodes on the system as there are no central nodes. Difficult to make timely decisions/ large scale tasks.

3

Point of Failure	Single Point of failure. If the main server crashes, the entire network will shut down.	One central node failure causes a part of the system to fail; not the entire system	No single point of failure as resources are spread across the network
Security	Increases the risk of security breaches from cybersecurity threads such as DDOS attacks as there is only one target to compromise.	Reduces the risk of attack on a single node. Information is disseminated across network instead of passing through single point. The chances of data flow being tracked is greatly reduced.	Highly secured as they use cryptography to secure the data in the network.
Traffic control	Bottlenecks can happen when traffic spikes. The server can have a finite number of open ports to listen to.	The data load is balanced on all the nodes leading to no bottle-neck situations	The number of resources is increased. Hence traffic is distributed across the network.

Storage	Data is stored in the central/server majorly. less possibility of data back up.	Data is stored across multiple nodes in the network. Provides a well managed back-up system.	cluster of storage units. A distributed storage is used.
Examples	web services like Youtube, banking acc	Blockchain, cryptocurrency and decentralised databases	SOA-based systems Multiplayer online games.
Organisations using	Twitter, Quora, Burger King	Bitcoin, Tor network	Google search system.

Q2. What are various features of Blockchain?

1. Decentralised system

Decentralised technology gives you the power to store your assets in a network which can be an asset like contract, documents etc. With this method, the owner has direct contrd over his account via a key linked to his account, which provides owner the ability to transfer his assets to whoever he/she wants.

5

Every node in the system has equal rights. This leaves no scope for exploitation. Blockchain gives you direct control over them with your private key. Essentially, the decentralised structure is giving people their power and rights back over their assets.

Decentralisation further provides:

1. Less failure
2. User control
3. Less Prone to Breakdown
4. No Third-Party
5. Zero scams
6. Transparency
7. Authentic nature

2. Consensus

The architecture is clearly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions.

Consensus is a decision making process for the group of nodes active on the network. The nodes can come to an agreement quickly and relatively faster. When millions of nodes are validating a transaction, a consensus is absolutely necessary for a system to run smoothly. The consensus is responsible for network being trustless. Nodes trust the

algorithm they run on.

3. Increased Capacity

It increases the capacity of the whole network. This reason is that there are a lot of computers working together which in total offers a greater power that few centralised devices.

4. Better security.

Blockchain technology has better security because there is not even a single chance of shutting down the system. Added with decentralisation, cryptography lays another layer of protection for users..

Every information on the blockchain is hashed cryptographically. For this process, any input data gets through a mathematical formula/ algorithm that produces a different kind of value, but the length is always fixed.

5. Immutability

Immutability means something that can't be changed or altered. To control the blockchain anyone needs control over 51% of total market.

7

This is one of the top features of blockchain to ensure the technology is - permanent, unalterable network. Every node on the system has a copy of the digital ledger. So, without the consent from the majority of nodes, no one can add any transaction blocks to the ledger. Another fact that backs up the list of key blockchain features is that, once the transaction blocks get added on the ledger, no one can just go back and change it.

Faster settlement

It can settle money transfers at really fast speeds. This ultimately saves a lot of time and money from these institutions and provides convenience to the consumer also. This is one of the best benefits of blockchain features to this day. And with the third party away, transactions can be made with minimal fee.

Minting

It is the process of validating information, creating a new block, and recording that information into the blockchain. Proof of stake

is the mining process of controlling how blocks are created and how data is added to a block.

Q3. Write in detail about network view and structure of blockchain.

Application and Presentation Layer

Consensus Layer

Network layer

Data layer

Hardware/ Infrastructure layer

1. Infrastructure layer.

This layer comprises virtualization (creation of virtual resources). Significantly, nodes are the core of this layer. A device connected to blockchain network is a node. Nodes are decentralised and distributed.

2. Data Layer

The data structure of a blockchain can be

represented as a linked-list of blocks, where transactions are ordered. A merkle tree is a binary tree of hashes. Each block contains a hash of the merkle root with information such as the hash of previous block, timestamp, nonce, the block version number and current difficulty target. Merkle trees offer security, integrity and irrefutability for the blockchain technology.

Network layer

The network layer, also known as the P2P layer, is responsible for inter-node communication. It takes care of discovery, transactions, and block propagation. This layer can also be termed as a propagation layer. This P2P layer ensures that nodes can discover each other and can communicate, propagate and synchronize with each other to maintain a valid current state of the blockchain network.

Consensus layer

The consensus protocol is the core to the existence of blockchain platforms. As the consensus layer is responsible for validating the blocks, ordering the blocks, and ensuring

ensure everyone agrees on it, it plays a crucial role. consensus methods vary for different types of blockchain.

Application layer

This layer consists of smart contracts, chaincode, and dApps. Application layer can be further divided into two sublayers - application and execution layer. Application layer has the applications that are used by end users to interact with the blockchain network. It comprises of scripts, APIs, user interfaces, frameworks. The execution layer consists of smart contracts. This sublayer has the actual code that gets executed and rules that are executed. A transaction propagates from application layer to execution layer, however the transaction is validated and executed at the semantic layer (smart contracts and rules). Applications send instructions to the execution layer, which performs the execution of transactions and ensures the deterministic nature of the blockchai

---

Q4 write about transaction structure in detail and how a Block will be formed.

Every chain consists of multiple blocks and each block has three basic elements.

The data in the block

A 32 bit whole number called the nonce. The nonce is randomly generated when the block is generated which then generates a block header hash.

The hash is a 256-bit number wedded to the nonce. It must start with a huge number of zeroes.

when the block of a chain is created, a nonce generates a crypto graphic. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.

Miners create new blocks on the chain through a process called mining. In a block-chain every block has its own unique nonce and hash, but also refurences the hash of the previous block in the chain, so mining a block isn't easy, especially on large chains.

Miners use special software to solve this incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256, there are roughly four billion possible nonce + hash combinations that must be mined before the right one is found. When that happens miners are said to have found the "golden nonce" and their block is added to the chain.

Making a change to any block earlier in the chain requires re-mining not just the block with the change, but all of the blocks that come after. That's why its extremely difficult to manipulate blockchain technology. Miner is awarded with a reward for adding block.

Q5 Write in detail about transaction life cycle.

The transaction life cycle can be described as follows:

1) transaction is sent (broadcast) to all participating computers in the specific blockchain network.

13

2) Every verifying computer in the network checks the transaction against some validation rules that are run by each verifying computer in the network. It is very important that the verifying users are not able to deduce the type of transaction being made, hence some privacy is provided.

3) If the conditions specified in the rules have been met, transactions are stored in a block and cryptographically sealed with specialized algorithm dedicated to this process. This process is also known as mining.

4) The newly mined block is broadcast to every computer in the network. The computers check the block against some specific validation rules and propagate it to their peers if valid.

5) Each verifying node in the network receiving new blocks validates it against some rules and adds it to their memory of the longest chain.

6) Now, the transaction is part of the blockchain and can't be altered in any way. The verification happens without human intervention. It is less prone to human error. Also, blockchain - powered scheme operates without any trusted third parties and is highly transparent for every user.

8)6. Explain in detail about blockchain architecture

A blockchain is an open financial ledger or record in which every transaction is authenticated and authorised. A blockchain is designed as a decentralised network of millions of computers, commonly referred to as nodes. Its a distributed database architecture in which each node plays the role of a network administrator who voluntarily joins the network. Since there's no centralised information in a blockchain architecture, a blockchain is literally impossible to hack. The blockchain architecture supports a growing list of ordered records known as blocks. Each block maintains a timestamp and a link to the previous block.

Components of blockchain architecture

Node - a computer in the blockchain architecture (each node has an independent copy of the entire blockchain ledger.

Transaction - A data record verified by blockchain participants that serves as an almost immutable confirmation of the authenticity of a financial transaction or contract.

15

Block - A sealed data that contains: hash code identifying a block, previous block's hash code from the previous block in the sequence of blocks and a set of timestamped transactions.

Chain - a ordered sequence of blocks.

Miners - Nodes that validate blocks before adding them to the blockchain structure.

Consensus - a set of rules and agreements for performing blockchain operations.

The blockchain architecture has many business benefits:

Cryptography
Provenance
Decentralization
Anonymity
Transparency

Types of blockchain architecture

Public blockchain architecture:-

A public blockchain architecture operates on the basis of proof of work (PoW) consensus algorithms and uses appropriate protocols. A public blockchain doesn't need any permission.

as it is open source.

Private blockchain architecture

A private blockchain architecture allows only a certain group of participants to access information. Such blockchain architectures are built by organisations with the aim of increasing the overall benefit or efficiency.

Consortium blockchain architecture

There is also a consortium, or public permissioned, blockchain architecture. In this type of blockchain architecture, anyone can connect to and view the blockchain, but a participant can add information or connect a node only with the permission of other participants. Such blockchains are built by organizations in order to increase trust among customers, consumers and society.

Q7 write about smart contracts in detail.

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met and verified. They typically are used to automate the execution of an agreement so that all

participants can be immediately certain of the output, without any intermediary's involvement or time loss.

Smart contracts work by following simple "if/when...then..." statements that are written into code on a blockchain. These actions could include releasing funds to appropriate parties, sending notifications, generating a ticket etc. The blockchain is then updated and transaction is completed.

To ensure that the task is completed satisfactorily, stipulations can be added to a smart contract as many times as possible. To establish the terms, participants must determine how transactions and their data are represented on a blockchain, agree on the "if/when...then..." rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes.

Smart contracts can be programmed by developers, although increasingly organisations using blockchains are offering interfaces, templates and other tools online to make smart contract creation easier.

Benefits of smart contracts

Speed, Efficiency and accuracy

A contract is automatically executed once a condition is met. Using digital and automated contracts reduces the risk of errors when filling out documents by hand and the time spent on resolving them.

Trust and Transparency

Since no third party is involved and encryption is used to store transactions, one doesn't need to worry about their information being manipulated.

Security

Blockchain transactions are supported by cryptographic records making them very difficult to hack. Additionally, since a distributed ledger is used, hackers need to alter every record to alter one.

Saving

By removing intermediaries from transaction, smart contracts will reduce the time and fees associated with them.

Some examples of smart contracts

Health insurance

Smart contracts can be used daily in health insurance and could reduce many inefficiences in the current systems. If patients use smart contracts to buy their insurance, all details of their policy will be automatically secured in their patient profile. This is then stored on the blockchain - a safe and secure ledger which is less prone to hackers than a traditional database.

Elections

In the Brazilian elections, there is an electronic ballot box responsible to counting the voting in each electoral college that allows the electors to type the candidate number. There is a remote control normally operated by a poll worker which requires the entry of elector identification number to verify if the same elector has voted earlier. This verification is important to ensure the elector cannot vote more than one time in the same election.

Trade finances

Financial documents linked and accessible through blockchain are surveied and approved in real time, reducing the time it takes to initiate shipment. As contract terms are met, status is updated on blockchain in real time, reducing the time and head count required to monitor the delivery of goods. Contract terms executed via smart contracts eliminate the need for correspondent banks and additional transaction fees.