UNIT 1

Introduction to Blockchain

CONTENTS

PART-1

Introduction to Blockchain.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.1. What do you mean by blockchain ? What are the properties/features of blockchain ?

Answer

1. Blockchain is a specific type of database.
2. Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.
3. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding).
4. The blockchain can be stored as a flat file, or in a simple database.
5. The blockchain data structure is an ordered back-linked list of blocks of transactions.
6. Blocks are linked "back", each referring to the previous block in the chain.
7. The blockchain is often visualized as a vertical stack, with blocks layered on top of each other and the first block ever serving as the foundation of the stack.
8. Blockchain is a type of Distributed Ledger Technology (DLT) in which transactions are recorded with an immutable cryptographic signature called a hash.

Properties of blockchain :

1. **Programmable :** A blockchain is programmable, *i.e.*, smart contracts.
2. **Secure :** All records are individually encrypted.
3. **Immutable :** Any validated records are irreversible and cannot be changed.
4. **Distributed :** All network participants have a copy of the ledger for complete transparency.
5. **Decentralized :** All the data is stored in a decentralized manner and no single entity has control over it.
6. **Time-stamped :** A transaction time-stamp is recorded on a block.

7. **Unanimous :** All network participants agree to the validity of each of the records.

Que 1.2. What is the motivation behind blockchain ? Explain the need for blockchain.

Answer

Motivation behind Blockchain :

1. Blockchain attempts to address the uncertainty existing in the financial transactions.
2. For example, the buyer expects fair goods for his money. The seller expects to receive the payment once he delivers the goods.
3. However, there would be a lack of trust between the parties intending to enter into the agreement.
4. Hence, a need for a third party arises that provides the trust platform for both the parties.
5. This mediating party assures the seller and buyer legitimate trade.
6. Trusting a third party however requires a lot of research and knowledge.
7. Blockchain aimed to overcome this uncertainty by implementing the applications in a secure and decentralized way.
8. Blockchain is gaining more and more acceptance and adoption, in the trustless society, precisely due to this reason.
9. Decentralization is an essential motivating factor contributing to the development and success of blockchain.
10. The decentralization is achieved by distributing the computation tasks to all the nodes.

Need for Blockchain : Need for blockchain is due to the following reasons :

1. **Faster settlements :** Traditional banking systems have time-consuming process for the settlement of transactions. But, blockchain reduced the time significantly.
2. **Security :** Cryptography functions and consensus protocols enable secured transactions in blockchain.
3. **Immutable :** Since blocks are immutable, tampering of the block is very difficult.
4. **Transparent :** Since blockchain is a decentralized system, third-party intervention is not needed at all. All stockholders of the network can participate in the network. This ensures transparency.

Que 1.3. What are different types of blockchain ?

Answer

Blockchain technologies can be divided into following three types :

A. Public blockchain :

1. Public blockchains are regarded as open source system and known as permissionless ledger and any participant can join in the network.
2. No permission is needed to join the network.
3. Participants have full rights for reading and writing into the network and have same copy of the ledger.
4. Public blockchain work seamlessly in trustless networks due to the immutable nature of the records.
5. Examples of public blockchain are Bitcoin and Ethereum.

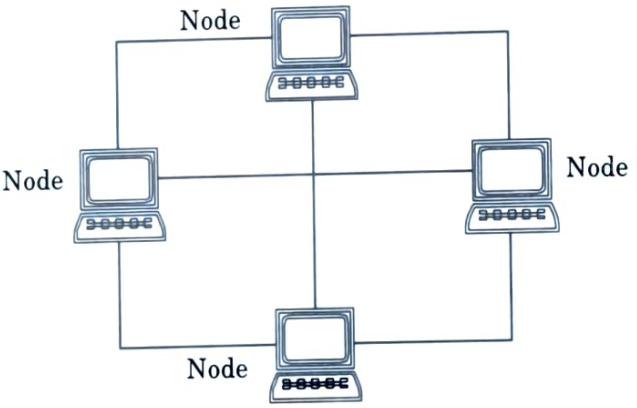

Fig. 1.3.1. Public blockchain.

B. Private blockchain :

1. They are permissioned ledger and restricts access to only selected participants of the network.
2. Each contributor in the network will have the whole record of the transactions and the associated blocks.
3. All blocks are encrypted by a private key and cannot be interpreted by anyone.
4. They are controlled only by authorized users.
5. Users can be validated with the support of identity management system.
6. Private blockchain involves trusted network and is suitable for sharing the ledger internally.
7. Examples of private blockchain are Hyperledger, Corda, and Quorum.

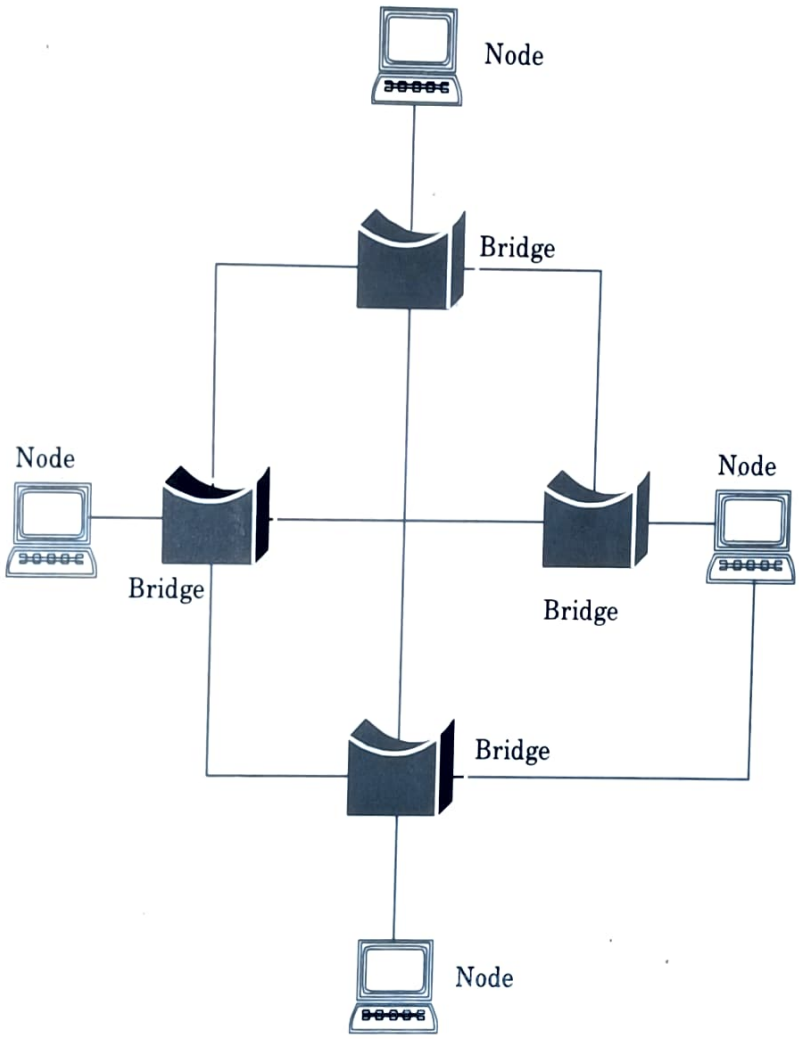

Fig. 1.3.2. Private blockchain.

C. Consortium blockchain :

1. Consortium blockchains are permissioned blockchains governed by a group of organizations rather than one entity.
2. Consortium blockchains are more decentralized than private blockchains, resulting in higher levels of security.
3. Setting up consortiums is a difficult process as it requires cooperation between a number of organizations, which presents logistical challenges as well as potential antitrust risk.
4. Also, some participating organizations may not have the needed technology or the infrastructure to implement blockchain tools.
5. Hyperledger, Corda, and R3CEV are some consortium blockchains.

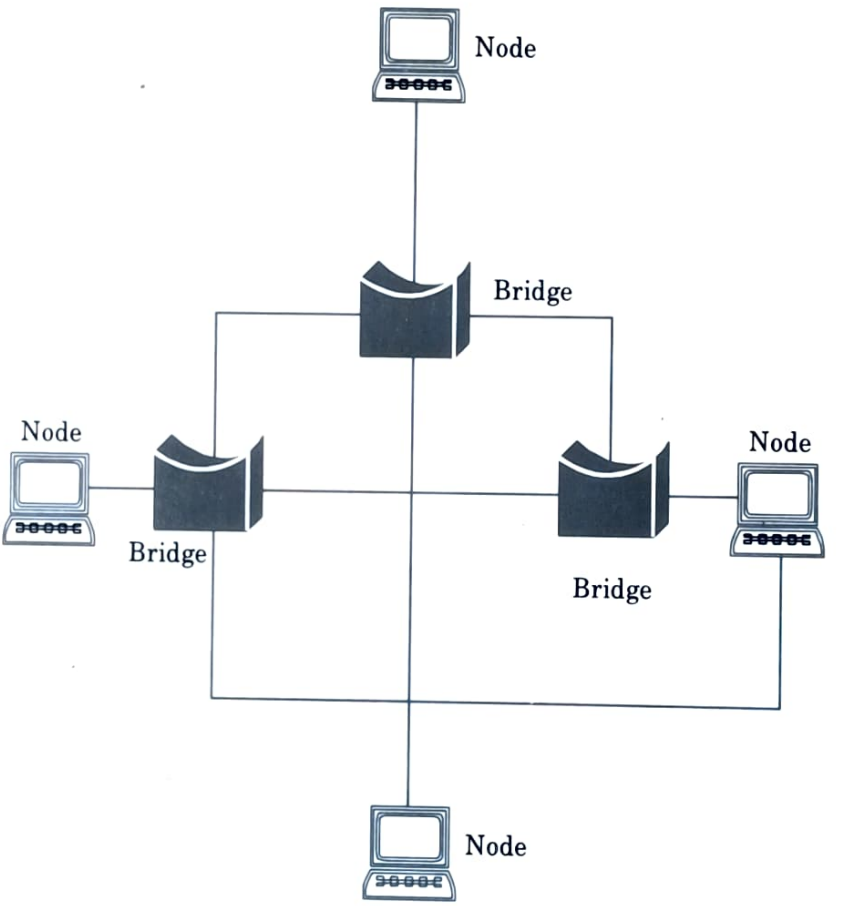

Fig. 1.3.3. Consortium blockchain.

Que 1.4. **List the advantages and disadvantages of public, private and consortium blockchain.**

Answer

A. Advantages and disadvantages of public blockchain :

Advantages :

1. Public blockchains are completely independent of organizations, so if the organization that started it ceases to exist the public blockchain will still be able to run.
2. Public blockchains have high level of network's transparency.
3. Public blockchains are mostly secure, as long as the users follow security protocols and methods fastidiously.

Disadvantages :

1. The network can be slow, and companies can't restrict access or use.

2. If hackers gain 51% or more of the computing power of a public blockchain network, they can unilaterally alter it.
3. Public blockchains don't scale well. The network slows down as more nodes join the network.

B. Advantages and disadvantages of private blockchain :

Advantages :

1. In private blockchain the controlling organization sets permission levels, security, authorizations and accessibility.
2. Private blockchains are fast and can process transactions more quickly than public blockchains.
3. Private blockchains can support and process a lot of higher transactions.

Disadvantages :

1. Private blockchains aren't true blockchains, since the core philosophy of blockchain is decentralization.
2. It's difficult to fully trust the information, since centralized nodes determine what is valid.
3. The source code from private blockchains is often proprietary and closed. Users can't independently audit it, which can lead to less security.

C. Advantages and disadvantages of consortium blockchain :

Advantages :

1. A consortium blockchain tends to be more secure, scalable and efficient than a public blockchain network.
2. Like private blockchain, it also offers access controls.

Disadvantages :

1. Consortium blockchain is less transparent than public blockchain.
2. It can be compromised if a member node is breached.
3. Consortium blockchain's own regulations can impair the network's functionality.

Que 1.5. Explain the major elements of the blockchain ecosystem in detail. **AKTU 2020-21, 2021-22; Marks 07**

Answer

Following are four main elements/components in a complete blockchain ecosystem :

A. Network of nodes :

1. All nodes are connected together to form a network that validates and maintains all the transactions.
2. Consensus protocol is used to validate each transaction.

3. When the transactions are validated, they are recorded in the blockchain.
4. This process of recording the transactions into the blockchain is known as mining of the blocks.
5. Block in blockchain can have zero or multiple number of transactions.

B. Distributed database :

1. Blockchain is a network and a database. It stores the data generated by the network.
2. Unlike central databases, blockchain resides in every node of the blockchain network.
3. So, the copy of the blockchain is with every node.
4. Each block will have list of transactions, timestamp, and information about the previous block.
5. This linkage to the previous block makes blockchain immutable.
6. If data in a block are tampered, then the hash of the block changes, which will make all blocks after the tampered block invalid.

C. Shared ledger :

1. The ledger is shared among all nodes.
2. If an attacker tries to tamper with the blockchain, then the attacker needs to make the change in every single node in the network.
3. This makes attacking difficult.
4. To tamper the blockchain, the attacker needs the control of at least 51% of the nodes in the network.

D. Cryptography :

1. Data in blockchain are cryptographically hashed.
2. Hash function is a one-way function *i.e.*, hash can be generated from the plain text, but deriving the plain text from the hash is extremely difficult.
3. Thus, tracking of information and unauthorized tampering of data cannot be done.

Que 1.6. How does a blockchain work ?

Answer

The following steps are involved in the working of blockchain :

1. Users initiate a transaction in the network. The transaction could be contracts, cryptocurrency or records of other information.
2. The request for the transaction has to be represented as block in the network.

3. The block is created first and then disseminated to the participants of the network.
4. All participants analyze the received block from the network and validate that block.
5. The block validation is done with the support of consensus algorithm.
6. Members of the network validate the block for attaching the block to the network.
7. The new block is attached to the network and transaction gets completed.
8. Block added with the consent of members of the network becomes permanent and immutable.

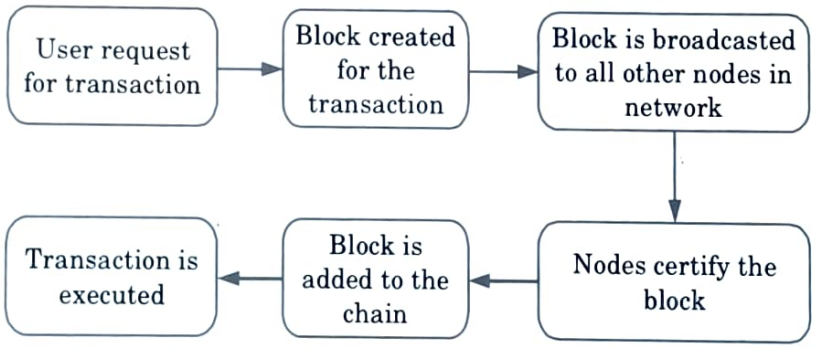

Fig. 1.6.1. Working of blockchain.

Que 1.7. What is a blockchain database ?

Answer

1. A blockchain database utilizes blockchain technology to create an immutable ledger of transactions.
2. Blockchain technology relies on peer-to-peer decentralized transactions meaning that it is a distributed ledger.
3. This offers greater security and removes the need for any single controlling entity that retains administration rights over the database.
4. The data structure involves data being recorded in blocks.
5. As each new block or transaction is recorded, it is added to the previous one to form a chain of data records or a blockchain.
6. As a result, a blockchain contains every transaction recorded since the ledger was started.
7. The technology relies on a consensus algorithm that requires a majority of the nodes on the network to validate any new transactions.
8. This makes any unauthorized modifications or any attempts to tamper with the data extremely difficult.
9. A blockchain as a database can contain any information.
10. Blockchains are not really good at storing vast amounts of data due to network limitations and cost.

Que 1.8. **What is a blockchain database ? How does a blockchain work ?** **AKTU 2019-20, Marks 07**

Answer

Blockchain database : Refer Q. 1.7, Page 1–9P , Unit-1.

Blockchain working : Refer Q. 1.6, Page 1–8P, Unit-1.

Que 1.9. **Blockchain is a distributed database. How is it different from a traditional database ?** **AKTU 2019-20, Marks 07**

OR

What is the difference between blockchain and database ? **AKTU 2020-21, Marks 07**

OR

Name organizations that can use blockchain technology. What is the difference between blockchain and database ? **AKTU 2021-22, Marks 07**

Answer

S. No.	Blockchain	Database
1.	Blockchain is decentralized because there is no admin or in-charge.	The database is centralized because it has admins and in-charge.
2.	Blockchain is permissionless because anyone can access it.	The database required permission because it can be accessed only by entities who have rights to access.
3.	Blockchains are slow.	Databases are fast.
4.	It has a history of records and ownership of digital records.	It has no history of records and ownership of records.
5.	Blockchain is fully confidential.	The database is not fully confidential.
6.	Blockchain has only Insert operation.	The database has Create, Read, Update, and Delete operation.
7.	It is a fully robust technology.	It is not entirely robust technology.
8.	Disintermediation is allowed with blockchain.	Disintermediation is not allowed with the database.

9.	Anyone with the right proof of work can write on the blockchain.	Only entities entitled to read or write can do so.
10.	Blockchain is not recursive. Here, we cannot go back to repeat a task on any record.	The database is recursive. Here, we can go back to repeat a task on a particular record.

Following are the organizations that use blockchain technology :

1. **Bank and Finance :** HSBC, Barclays, VISA.
2. **Supply Chain :** Walmart, Unilever.
3. **Healthcare :** Pfizer, Change Healthcare, CDC.
4. **Insurance :** MetLife, AIG.
5. **Energy :** Siemens, Shell.
6. **Travel :** Etihad Airways, Singapore Airlines, British Airways.

Que 1.10. What are the advantages / benefits of blockchain ? Explain in detail.

Answer

Following are the advantages / benefits of blockchain :

1. **Accuracy of the chain :** Transactions on the blockchain network are approved by a network of thousands of computers. This removes almost all human involvement in the verification process, resulting in less human error and an accurate record of information.
2. **Cost reductions :** Blockchain eliminates the need for third-party verification and, with it, their associated costs.
3. **Decentralization :** Blockchain does not store any of its information in a central location. Instead, the information is copied and spread across a network of computers. Whenever a new block is added, every computer on the network updates its blockchain to reflect the change.
4. **Efficient transactions :** Blockchain works 24 hours a day, seven days a week, and 365 days a year. Transactions can be completed in as little as ten minutes and can be considered secure after just a few hours.
5. **Secure transactions :** Once a transaction is recorded, its authenticity must be verified by the blockchain network. After a computer has validated the transaction, it is added to the blockchain block. Each block on the blockchain contains its own unique hash, along with the unique hash of the block before it.
6. **Transparency :** Most blockchains are entirely open-source software. This means that anyone and everyone can view its code. This makes blockchain more transparent.

Que 1.11. What are the limitations of blockchain ? Explain in detail. **AKTU 2020-21, Marks 07**

OR

Mention various limitations of blockchaining in detail with proper representation. **AKTU 2021-22, Marks 07**

Answer

Following are the limitations/disadvantages of blockchain :

1. **Scalability is an issue :** Blockchains are not scalable as their counterpart centralized system. Due to this there is problem of network congestion. The more people or nodes join the network, the chances of slowing down is more.
2. **Consume too much energy :** Bitcoin incentivizes the miner's to solve complex mathematical problems. The high energy consumption is what makes these complex mathematical problems not so ideal for the real-world. Every time the ledger is updated with a new transaction, the miners need to solve the problems which means spending a lot of energy.
3. **Data is immutable :** Data immutability has always been one of the biggest disadvantages of the blockchain. For example, you have processed payment and need to go back and make an amendment to change that payment, you cannot do that.
4. **Blockchains are inefficient :** There are multiple blockchain technologies which have a lot of inefficiencies within the system. This is one of the big disadvantages of blockchain. For example, the blockchain technology used by Bitcoin is not efficient in data storage.
5. **Not completely secure :** Blockchain technology is more secure than other platforms. However, this doesn't mean that it is completely secure. There are different ways the blockchain network can be compromised like 51% attack, double-spending, DDoS's attack, cryptographic cracking, etc.
6. **Cost of implementation :** The underlying cost of implementing blockchain technology is huge. Even though most of the blockchain solutions are open source, they require a lot of investment from the organization that is willing to pursue it.
7. **Expertise knowledge :** Implementing and managing a blockchain project is hard. Business's need to hire multiple experts in the blockchain field that leads to the problem and hence it is counted as one of the disadvantages of blockchain.

PART-2

Digital Money to Distributed Ledgers.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.12. What is digital money ?

Answer

1. Digital money (or digital currency) refers to any means of payment that exists in a purely electronic form.
2. Digital money is not a physically tangible asset like cash.
3. It is accounted for and transferred using online systems.
4. One well-known form of digital money is the cryptocurrency Bitcoin.
5. Digital money can also represent fiat currencies, such as rupees or dollars.
6. Digital money is exchanged using technologies such as smartphones, credit cards, and online cryptocurrency exchanges.
7. In some cases, it can be converted into physical cash through the use of an ATM.
8. Digital money is susceptible to hacks and can compromise user privacy.

Que 1.13. What are distributed ledgers ?

Answer

1. A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions, or geographies, accessible by multiple people.
2. It allows transactions to have public "witnesses."
3. The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it.
4. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes.
5. A distributed ledger is different from centralized ledger, which is the type of ledger that most companies use.
6. A centralized ledger is more prone to cyber attacks and fraud, as it has a single point of failure.
7. Distributed ledgers use the same technology that is used by blockchain.
8. Blockchain is a type of distributed ledger used by bitcoin.
9. Bitcoin is a virtual currency that can be used for payments with transaction fees less than conventional online payment methods.

10. Ethereum is also an example of a distributed ledger. It enables the developers to create their own applications.
11. Ripple is another example of a distributed ledger that is an open-source ledger focusing on payments, especially cross-border transactions.

Que 1.14. Differentiate digital money and distributed ledger.

Answer

S. No.	Digital money	Distributed ledger
1.	Digital money refers to any means of payment that exists in a purely electronic form.	A distributed ledger is merely a type of database spread across multiple sites, regions, or participants.
2.	Digital money is susceptible to hacks.	Distributed ledgers are inherently harder to hacks because all of the distributed copies need to be attacked simultaneously for an attack to be successful.
3.	Bitcoin is a form of digital money.	Bitcoin uses blockchain which is a type of distributed ledger.

Que 1.15. What is a ledger ? Is blockchain an incorruptible ledger ? Explain common types of ledgers that can be considered by users in blockchain. **AKTU 2019-20, Marks 07**

Answer

Ledger : A ledger is the principal book or computer file for recording and adding economic transactions measured in terms of a monetary unit. A ledger is a file that is growing continuously. It stores the permanent record of all the transactions taking place between the two parties on the blockchain network.

Is blockchain an incorruptible ledger :

1. The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.
2. Blockchain is considered incorruptible. Any ill-intentioned individual acting alone is powerless.
3. To take over the network, an attacker would have to control more than 51 percent of its total computing power.
4. Also the attacker requires energy to power the computers needed for the blockchain system to work.

Ledgers used in blockchain :

A. Centralized ledgers :

1. A centralized ledger system is a compilation of all transactions which is controlled by a single entity.
2. A centralized ledger system has a single point of control.
3. In centralized ledger system internal and external reconciliation of data is required to ensure the integrity of transactions.
4. The centralized system provides no restrictions on the operations which can be performed in the ledger.
5. For example, any user can modify a transaction and back date them. This can lead to misstatement of financial transactions and fraudulent activities.
6. To avoid such transactional errors a decentralized system or a distributed ledger can be used.

B. Decentralized ledgers :

1. In decentralized ledger the control and decision-making is transferred from a centralized entity to a distributed network.
2. In a decentralized ledger no one has to know or trust anyone else.
3. Each member in the network has a copy of the exact same data in the form of a distributed ledger.
4. If a member's ledger is altered or corrupted in any way, it will be rejected by the majority of the members in the network.
5. In a decentralized ledger services are provided with better performance and consistency, as well as a reduced likelihood of catastrophic failure.

C. Distributed ledger :

1. A distributed ledger, also known as a shared ledger, is a list of shared and synchronized data which are geographically spread across multiple sites.
2. The data is exactly replicated and synchronized across all locations to maintain data integrity, availability and resiliency.
3. Unlike the centralized system, there is no central administrator or single point of control.
4. If one location abruptly fails then the remaining location has the capacity to maintain the ledger or all transaction details.
5. This way a distributed ledger provides real-time information and reduced error or fail rates of transactions.
6. This also reduces the costs of infrastructure as compared to the centralized ledger system.

7. A distributed ledger uses a peer-to-peer network to communicate with nodes which are spread around the globe.

Que 1.16. How is blockchain distributed ledger different from a traditional ledger ? **AKTU 2020-21, Marks 07**

OR

What are function modifiers in solidity ? How is blockchain distributed ledger different from a traditional ledger ? **AKTU 2021-22, Marks 07**

Answer

Function Modifiers in Solidity :

1. Function Modifiers are code that can be run before and/or after a function call.
2. Function Modifiers are used to modify the behaviour of a function.
3. Function Modifiers can be used to :
   i. Restrict access
   ii. Validate inputs
   iii. Guard against reentrancy hack

S. No.	Blockchain ledger	Traditional ledger
1.	Information registered on a blockchain distributed ledgers is irreversible.	Information registered on a traditional ledger is reversible.
2.	A blockchain distributed ledger is more secure.	A traditional ledger is less secure than blockchain distributed ledger.
3.	In a blockchain distributed ledger, there is no central authority.	Traditional ledgers are based on the concept of centralized control, which controls all transactions.
4.	In a blockchain distributed ledger, identities of all participants are unknown and hidden.	In traditional ledger identities of all participants have to be known before the transactions happen.
5.	In a blockchain distributed ledger, there is no single point of failure as the data is distributed and information is shared across multiple nodes.	Traditional ledgers have a single point of failure. If a single system crashes, the entire network comes to a standstill.

6.	In a blockchain distributed ledger, data modification or change cannot be done.	In a traditional ledger, data modification or change is possible.
7.	In a blockchain distributed ledger, validation is done by the participants in the network.	In a traditional ledger, validation is done by a centralized authority.
8.	The copy of the ledger is shared amongst participants in a blockchain distributed ledger.	In a traditional ledger, a single copy is maintained in a centralized location. It is not shared amongst the participants.

Que 1.17. Write a short note on : Bitcoin.

Answer

1. Bitcoin is a digital and global money system cryptocurrency.
2. It allows people to send or receive money across the internet.
3. It is the first of its kind technology that allows the transfer of digital currency across the internet without needing a third party.
4. Money can be exchanged without being linked to a real identity.
5. The mathematical field of cryptography is the basis for Bitcoin's security.
6. There are no physical Bitcoins, only balances kept on a public ledger that everyone has transparent access to.
7. All Bitcoin transactions are verified by a massive amount of computing power via a process known as "mining."
8. Bitcoin is built on a distributed digital record called a blockchain.
9. Blockchain is a record of all transactions that have taken place in the Bitcoin network.
10. It also keeps track of new Bitcoins as they are generated.

Que 1.18. How are transactions and blocks encrypted in the bitcoin implementation ? What are the benefits of blockchain technology ?

AKTU 2019-20, Marks 07

Answer

Encryption of transactions and blocks in the bitcoin :

1. Bitcoin blocks are public and they are not encrypted in any way.
2. The block content in Bitcoin is processed using a special hash function called "SHA256" and the resulting value is stored in blockchain.

3. Block hash not only prevents modifications, it also guarantees the data integrity in the block content.

Benefits of blockchain technology : Refer Q. 1.10., Page 1–11P, Unit-1.

Que 1.19. How will you handle the risk management when it comes to securing the transactions records ? **AKTU 2020-21, Marks 07**

Answer

1. Risk management is basically a process of finding the threats and all the vulnerabilities to the financial records of an organization.
2. The best thing that can be done with this approach is to take the right countermeasures against them immediately.
3. Another approach is to pay attention to a backup plan.
4. Based on the value of information, more approaches such as buying new risk management software can simply be considered.
5. The prime risk to information is from black-hat hackers.

Que 1.20. What is the difference between off-chain transactions and on-chain transactions ? **AKTU 2020-21, Marks 07**

Answer

S. No.	On-chain transactions	Off-chain transactions
1.	On-chain transactions are the transaction that occurs on the blockchain themselves.	Off-chain transactions are the transaction that does not occurs on the blockchain but outside of it.
2.	On-chain transactions take longer because of the different steps that have to happen before a transaction is deemed to be successful.	Off-chain transactions are done instantly, without having to wait for the network confirmations.
3.	On-chain transactions are visible to all the nodes on the blockchain network.	Off-chain transactions are more private. These transactions are not visible on the public blockchain.
4.	A high cost of transaction is associated with on-chain transactions.	Off-chain transactions are cheaper. In off-chain transactions made are usually free.
5.	On-chain transactions are best for cryptocurrency transfers.	Off-chain transactions are best for non-crypto related transfers.

Que 1.21. Write a short note on : Ethereum.

Answer

1. Ethereum is a decentralized, open-source blockchain with smart contract functionality.
2. Ethereum is a blockchain-based platform that is best known for its cryptocurrency, Ether, or ETH, or simply Ethereum.
3. The blockchain technology that powers Ethereum enables secure digital ledgers to be publicly created and maintained.
4. As a cryptocurrency, Ethereum is second in market value only to Bitcoin.
5. Bitcoin and Ethereum have many similarities but different long-term visions and limitations.
6. Ethereum is transitioning to an operational protocol that offers incentives to process transactions to those who own the largest amounts of ETH.
7. Open-source development is currently underway for a major upgrade to Ethereum known as Ethereum 2.0 or Eth2.
8. The main purpose of the upgrade is to increase transaction throughput for the network from the current of about 15 transactions per second to up to tens of thousands of transactions per second.

Que 1.22. List and explain the parts of EVM memory.

AKTU 2020-21, Marks 07

OR

Mention and list the parts of EVM memory in blockchaining.

AKTU 2021-22, Marks 07

Answer

Ethereum Virtual Machine (EVM) :

1. Ethereum Virtual Machine (EVM) is a computation engine which acts like a decentralized computer that has millions of executable projects.
2. It acts as the virtual machine which is the bedrock of Ethereum's entire operating structure.
3. It is considered to be the part of the Ethereum that runs execution and smart contract deployment.
4. The role of the EVM is to deploy a number of extra functionalities to the blockchain to ensure users face limited issues on the distributed ledger.
5. Every Ethereum node runs on the EVM to maintain consensus across the blockchain.

6. Ethereum facilitates smart contract, which is a piece of code that is running on Ethereum.
7. EVM is completely isolated meaning the code inside the EVM has no access to the network, file system or other processes.

Parts of EVM Memory :

The memory of an EVM is divided into three types :

Storage :

1. Storage values are stored permanently on the blockchain network.
2. It is extremely expensive.

Memory :

1. Memory is a temporary modifiable storage.
2. It can be accessed only during contract execution. Once the execution is finished, its data is lost.

Stack :

1. A stack is temporary and non-modifiable storage.
2. Here, when the execution completes, the content is lost.

Que 1.23. What is a dapp and how is it different from a normal application ? **AKTU 2020-21, Marks 07**

OR

What is the concept of double spending ? What is a dapps in blockchain ? **AKTU 2021-22, Marks 07**

Answer

Double Spending :

1. Double-spending is a potential flaw in a digital currency scheme in which the same single digital token can be spent more than once.
2. Unlike physical cash, a digital token consists of a digital file that can be duplicated or falsified.
3. The primary reason for double-spending is that digital currency can be very easily reproduced.
4. Double-spending leads to inflation by creating a new amount of copied currency that did not previously exist.
5. There are primarily two ways to combat double-spending - central clearing counterparty and blockchain.
6. Fundamental cryptographic techniques to prevent double-spending are blind signatures and secret splitting.

dapps in blockchain :

1. A decentralized application (dapp) is an application built on a decentralized network that combines a smart contract and a frontend user interface.
2. A dapp has its backend code running on a decentralized peer-to-peer network.
3. A dapp can have frontend code and user interfaces written in any language to make calls to its backend.
4. Its frontend can get hosted on decentralized storage such as InterPlanetary File System (IPFS).

Difference between dapp and a normal application :

S. No.	dapp	Normal app
1.	dapps run on a decentralized network or system.	Normal apps are not designed to work in a decentralized ecosystem.
2.	Most dapps charge users a fee to participate.	Many normal apps are free.
3.	dapps store user data on the application itself.	Normal apps store user data on a separate server.
4.	dapps tends to have a slower verification process.	Normal apps have faster verification process.
5.	dapps does not require any intermediary and it connects with users automatically.	An app requires an intermediary to connect the users with application.
6.	dapp changes codes and functions automatically and it resists the involvement of developers.	An app is always under the control of developers. They only can make changes in codes and functionalities.

Que 1.24. Mention the benefits and drawbacks of dapp development.

Answer

Benefits of dapp development : Following are the benefits of dapp development :

1. **Zero downtime :** Using smart contract, the network as a whole serve clients looking to interact with the contract. Malicious actors cannot launch denial-of-service attacks targeted towards individual dapps.
2. **Privacy :** Individuals real-world identity is not needed to interact with a dapp.

3. **Resistance to censorship :** No single entity on the network can block users from submitting transactions, deploying dapps, or reading data from the blockchain.
4. **Complete data integrity :** Data stored on the blockchain is immutable and indisputable. Malicious actors cannot forge data that has already been made public.
5. **Trustless computation :** Smart contracts can be analyzed and are guaranteed to execute in predictable ways, without the need to trust a central authority.

Drawbacks of dapp development : Following are the drawbacks of dapp development :

1. **Maintenance :** Dapps can be harder to maintain because the code and data published to the blockchain are harder to modify. It's hard for developers to make updates to their dapps once they are deployed.
2. **Performance overhead :** To achieve the level of security, integrity, transparency, and reliability every node runs and stores every transaction. Due to this there is a huge performance overhead.
3. **Network congestion :** When one dapp uses too many computational resources, the entire network gets backed up.
4. **User experience :** It is harder to engineer user-friendly experiences because the average end-user find it too difficult to interact with the blockchain in a truly secure fashion.
5. **Centralization :** User-friendly and developer-friendly solutions built on top of the base layer of Ethereum might end up looking like centralized services anyways. Centralization eliminates many of the advantages of blockchain over the traditional model.

Que 1.25. What do you know about blockchain ? What is the difference between Bitcoin blockchain and Ethereum blockchain ?

AKTU 2019-20, Marks 07

Answer

Blockchain : Refer Q. 1.1, Page 1–2P, Unit-1.

Difference between Bitcoin and Ethereum blockchain :

S. No.	Bitcoin blockchain	Ethereum blockchain
1.	Bitcoin was the first true cryptocurrency and has been in circulation since 2009.	Ethereum is a far more recent development, going live in 2015.
2.	Bitcoin blockchain is a database of accounts with an amount of currency stored in each.	The Ethereum blockchain is a more sophisticated construction, capable of storing computer code.

3.	Each block on the Bitcoin blockchain is verified and created at an interval of 10 minutes.	Each block on the Ethereum blockchain is verified and created every 10-20 seconds.
4.	Bitcoin uses SHA-256 algorithm.	Ethereum uses ethash algorithm.
5.	Bitcoin was created as an alternative to national currencies.	Ethereum was intended as a platform to facilitate contracts and applications via its own currency.
6.	There is a strict cap of 21 million Bitcoins that will ever be created.	Unlike Bitcoin, there is no limit on the supply of ETH in the market.

Que 1.26. What are tokens ? Give the types of token used in blockchain ?

Answer

1. A token is a unit of value that is issued and defined by a specific organization that is both accepted by a certain group of buyers and sellers.
2. Within the crypto framework, a token needs to be supported by an underlying blockchain network.
3. In this context, we can define a token as a cryptocurrency built onto an existing blockchain.
4. The token is supported and given value based on the support and market value of the specific blockchain frameworks capabilities.

Types of tokens : There are essentially two types of tokens :

A. Utility Tokens :

1. Utility tokens are essentially cryptocurrencies that are used for a specific purpose, like buying a particular good or service.
2. For example, if you have to store large amounts of data you would have to rely on companies like Google, Amazon, or Dropbox.
3. These large companies have a monopoly on data server storage so they are able to dictate the price.
4. This is where the decentralized blockchain comes in with its utility token.
5. Coins like Filecoin promise to store data in similar cloud storage without using massive servers.
6. Users will be able to simply store data on the hard drives of other people in the network.

7. Essentially, you would pay someone running a hosting node through the Filecoin utility token.
8. The more data you store the more Filecoin will deduct from your token balance.

B. Security Tokens :

1. A security token represents ownership in an underlying real-world asset.
2. It essentially represents proof of ownership.
3. This framework is very much like the buying and selling of traditional stocks and bonds.
4. Regular securities are tracked in a centralized database.
5. Security tokens use a blockchain system - a decentralized database- to do the tracking of who owns which assets.
6. Using blockchain-based security tokens expands trading beyond regular bankers' and stock-market hours.
7. Security tokens also make it easy for people and investors to access a wider portfolio revealing a number of transactions and investments.

Que 1.27. What are different types of blockchains ? Also explain why a blockchain needs a token to operate ?

AKTU 2020-21, Marks 07

OR

Explain why a blockchain needs token to operate ?

AKTU 2019-20, Marks 07

Answer

Different types of blockchains : Refer Q. 1.3, Page 1–3P , Unit-1.

Blockchain needs a token to operate : Following are the reasons why blockchains need tokens to operate :

i. Tokens are needed to power blockchain.
ii. Tokens are a currency.
iii. Tokens can represent asset ownership.
iv. Tokens can represent stake or equity ownership.
v. Tokens incentivize miners or nodes owners.
vi. Tokens can be tracking devices.
vii. Tokens allow for crowdfunding.
viii. Tokenization of non-physical assets and documents.

PART-3

Design Primitives : Protocols, Security, Consensus, Permissions, Privacy.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.28. What are blockchain protocols ? Give examples of blockchain protocols.

Answer

Blockchain protocols :

1. Protocols are crucial components of blockchain technologies that enable information to be shared automatically across cryptocurrency networks securely and reliably.
2. In the field of computing, protocols are rules that define data transfer between different computer systems.
3. Protocols define the way that data must be structured and they establish safeguards to prevent malicious users from causing damage.
4. A blockchain is a network of multiple devices (nodes) connected to each other through the internet.
5. Essentially, a blockchain is a ledger which stores the record of what has come in and gone out after the transaction has been verified by all participating nodes.
6. This distributed ledger works on pre-defined rules which are agreed upon by all the participating nodes in the network.
7. These rules include :
   i. A how-to for governing and validating transactions,
   ii. An algorithm that defines the mechanism for all participating nodes to interact with each other, and
   iii. Application programming interface.
8. These rules that govern a blockchain network are referred to as a protocol.
9. It is essentially the common communication rules that the network follows.

Examples of Blockchain Protocols : Following five major protocols are often used in blockchain development services :

1. **Hyperledger :**
   i. Hyperledger is an open-source project that helps to deploy blockchain technologies quickly and effectively.
   ii. The protocol is commonly used in blockchain software solutions because it comes with its libraries that help to speed up development.
   iii. The Linux Foundation is a strong supporter of Hyperledger.
2. **Multichain :**
   i. Multichain helps create private blockchains to facilitate more efficient transactions and to develop new applications for the proof-of-work systems.
   ii. Multichain offer an API that can be used by blockchain development services to streamline integration and accelerate deployment.
3. **Enterprise Ethereum :**
   i. The goal of Ethereum Enterprise is to increase the business use cases of blockchain software development.
   ii. The major advantage of Ethereum Enterprise is that it allows businesses to create proprietary variants of Ethereum while still taking full advantage of the latest Ethereum code.
4. **Corda :**
   i. Corda offers a protocol designed for enterprises in the finance and banking field.
   ii. Corda is accredited by the R3 banking consortium, so it is a good choice for blockchain development solutions in the finance industry.
5. **Quorum :**
   i. Quorum also offers a protocol designed for enterprises in the finance sector.
   ii. Quorum is significant because it has strong backing from the financial community.
   iii. Quorum is also strongly associated with Ethereum since the project started by modifying the Ethereum code.

Que 1.29. Why selection of a blockchain protocol matters ?

Answer

1. The selection of a blockchain protocol is one of the most important decisions to be made when launching a blockchain software development project.
2. Protocols matter because they determine the scope of functionality that software can provide.
3. To develop protocol on your own requires the collaboration of thousands of computer scientists.

4. Instead of reinventing the wheel, your project can be completed in less time and with fewer resources by taking advantage of an existing protocol.
5. Therefore the selection of a blockchain protocol matters.
6. Also protocols are highly complex, so it is advisable to work with customized blockchain developers.
7. Professionals can help you to seamlessly integrate existing software with blockchain technologies.
8. Also they can ensure that the software is deployed and maintained securely.

Que 1.30. Explain security in blockchain.

Answer

1. Security of blockchain involves the protection of information and data used in cryptocurrency transactions and in blocks against various attacks.
2. Blockchain technology uses several techniques to ensure the security required in transaction data or block data.
3. Several applications like Bitcoin use cryptographic techniques for data safety.
4. Protection of information and data involves implementation of following strategies :
   i. **Defense in penetration :** This method enforces various corrective measures to protect the data. It works on the principle of protecting data in multiple layers of security.
   ii. **Minimum privilege :** In this strategy, the accessibility of data is reduced to the lowest possible level to strengthen and enhance the security level.
   iii. **Manage vulnerabilities :** Vulnerabilities are checked and manage by modifying, identifying, authenticating the user, and patching the gap.
   iv. **Manage risks :** Risks of an environment are processed by identifying, assessing, and by controlling the possibility of risks.
   v. **Manage patches :** The administered part like code, application, operating system are patched by acquiring, testing, and installing patches.

Que 1.31. What are Consensus Protocols ? How do Consensus Protocols work ?

Answer

Consensus Protocols :

1. A blockchain is spread across nodes whose job is to verify transactions on the network.
2. Anyone can submit information to be stored onto a blockchain.
3. Therefore it is important that there are processes in place that can ensure everyone agrees on what information to add and what to discard.
4. These rules are essentially known as consensus protocols. They verify transactions and help keep the network safe.
5. Consensus protocols form the backbone of blockchain by helping all the nodes in the network verify the transactions.
6. A consensus protocol is traditionally set before the blockchain is first created.
7. Consensus protocols prevent a single entity taking control.
8. Consensus protocols allow users on a decentralized network to trust other users without a controlling third-party.

Working of Consensus Protocols :

1. The consensus protocol gives a specific method for verifying whether a transaction is true or not.
2. It provides a method of review and confirmation of what data should be added to a blockchain's record.
3. Blockchain networks don't have a centralized authority, so all nodes on a blockchain must agree on the state of the network, following the predefined protocol.
4. For Bitcoin, the consensus protocol is Proof-of-Work (PoW), the block mining process which confirms each transaction.

Que 1.32. Explain permissions in blockchain.

Answer

1. In certain blockchain the access to the network is permissioned. This means that permission and role for each node have to be granted.
2. These blockchains can be thought of as closed ecosystems that can only be accessed by those who are allowed access.
3. Each contributor in the network will have the whole record of the transactions and the associated blocks.
4. All blocks are encrypted by a private key and cannot be interpreted by anyone.
5. They are controlled only by authorized users of a specific organization.

6. This is useful for companies, banks, and institutions that are comfortable to comply with the regulations and are very concerned about having complete control of their data.
7. Examples of permissioned blockchain are Hyperledger Fabric, Corda, and Quorum.

Que 1.33. Explain privacy in blockchain.

Answer

1. In a blockchain all transactions are transparent.
2. As the information is available to the public, it could be used to reach the users involved in the transaction.
3. Each user can be identified through the nodes it connects to.
4. This information could be used to find the beginning of a transaction.
5. This violates the privacy of the user.
6. Methods to tackle this are as follows :
   i. **Mixing :** This refers to performing transactions through multiple input and output addresses. This would make it difficult to find a relationship between the two participants.
   ii. **Anonymous :** This refers to the idea of completely anonymous transactions where the miners do not have any information about the transaction and the user information is encrypted.
   iii. **Off chain :** Sensitive data are not stored on the blockchain and can only be accessed by authorized personnel. This also solves the problem of space as some of the information is stored in a different location.

PART-4

Blockchain Architecture and Design.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.34. Explain blockchain architecture in detail.

AKTU 2020-21, Marks 07

OR

Write and explain the blockchain architecture in depth. What are the primary benefits of immutability in blockchaining ?

AKTU 2021-22, Marks 07

Answer

The following diagram displays the layered architecture of blockchain :

Application and Presentation Layer Smart Contracts, dapps, User Interface
Consensus Layer PoW, PoS, DPoS, PoET, PBFT
Network Layer Peer-to-Peer (P2P)
Data Layer Digital Signature, Hash, Merkle Tree, Transaction
Hardware / Infrastructure Layer Virtual Machine, Containers, Services, Messaging

Fig. 1.34.1. Blockchain layered architecture.

A. Hardware / Infrastructure layer :

1. Blockchain is a P2P network of computers that computes transactions, validates them, and stores them in an ordered form in a shared ledger.
2. Each computer in a P2P network is called a node. These nodes are decentralized and distributed.
3. Nodes are responsible for validating transactions, organizing them into blocks, and broadcasting them to the blockchain network.
4. Upon reaching consensus, nodes commit the block to the blockchain network and update their local ledger copy.

B. Data layer :

1. Blockchain is a decentralized, massively replicated database (distributed ledger), where transactions are arranged in blocks, and placed in a P2P network.
2. The current state of all accounts is stored in such a database.
3. The data structure of a blockchain can be represented as a linked-list of blocks, where transactions are ordered.
4. The blockchain's data structure includes two primary components-pointers and a linked list.

5. The pointers are the variables, which refer to the location of another variable.
6. Linked list is a list of chained blocks, where each block has data and pointers to the previous block.

C. Network layer :

1. In a P2P network computers (nodes) are distributed and share the network's workload to reach the end goal.
2. Nodes perform transactions on the blockchain.
3. The network layer, also known as the P2P layer, is responsible for inter node communication.
4. It takes care of discovery, transactions, and block propagation. This layer can also be termed as propagation layer.
5. This P2P layer ensures that nodes can discover each other and can communicate, propagate and synchronize with each other to maintain valid current state of the blockchain network.
6. This layer also takes care of the world state propagation.

D. Consensus layer :

1. The consensus protocol is the core to the existence of blockchain platforms. Behind every blockchain there is a consensus algorithm.
2. The consensus layer is the most critical and crucial layer for any blockchain.
3. Consensus is responsible for validating the blocks, ordering the blocks, and ensuring everyone agrees on it.
4. Following are the key points regarding the consensus layer :
   i. Consensus protocols (algorithms) create an undeniable set of agreements between nodes across the distributed P2P network.
   ii. Consensus keeps all the nodes synchronized. Consensus ensures that all the nodes agree to the truth.
   iii. Consensus ensures that power remains distributed and decentralized. No single entity can control the entire blockchain network.
   iv. Reliability in a P2P network is achieved by a consensus protocol.

E. Application layer :

1. The application layer is comprised of smart contracts, chaincode, dapps and user interface.
2. Application layer can be further divided into two sub layers- application layer and execution layer.
3. Application layer has the applications that are used by end users to interact with the blockchain network.
4. It comprises of scripts, APIs, user interfaces, frameworks.

5. Execution layer is the sub layer which constitutes of smart contracts, underlying rules and chaincode.
6. This sub layer has the actual code that gets executed and rules that are executed.
7. A transaction propagates from application layer to execution layer; however the transaction is validated and executed at the semantic layer (smart contracts and rules).

Benefits of immutability in blockchain : Following are some benefits of immutability :

1. **Complete data integrity :**
   i. Using blockchain technology ledger, you can guarantee the data trail and full history of an application.
   ii. We can easily validate the chain's integrity by re-calculating the block hashes.
   iii. If discrepancy exists between the block data and its corresponding hash, it means the transactions are not valid.
   iv. This allows organizations and its industry regulators to quickly detect data tinkering.
2. **It simplifies auditing :**
   i. The ability of an organization to produce a complete and indisputable history of a transactional ledger makes the auditing process easy and efficient.
   ii. Furthermore, the ability to prove that data has not been tampered with is a great benefit for organizations that comply with the industry regulations.
3. **It increases efficiencies :**
   i. The immutability of blockchain not only benefit auditing, it also offers new opportunities in analytics, query, and overall business processes.
   ii. This ability helps an organization save time and cost when auditing specific application data, tracking major bugs, backing up and restoring a database to retrieve information, etc.
4. **It can be used as Proof of Fault :**
   i. It is common for organizations to have disputes over fault in business.
   ii. Although you cannot use blockchain to dissolve a massive category of legal proceedings, you can leverage it to prevent the majority of disputes related to data provenance and integrity.
   iii. Blockchain finality allows us essentially to prove who did what and at what time.

Que 1.35. Explain Blockchain architecture. Differentiate Digital money and Distributed ledger. **AKTU 2019-20, Marks 07**

Answer

i. **Blockchain architecture :** Refer Q. 1.34, Page 1–29P, Unit-1.

ii. **Differentiate Digital money and Distributed ledger :** Refer Q. 1.14, Page 1–14P, Unit-1.

PART-5

Basic Crypto Primitives : Hash, Signature.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.36. Discuss crypto primitives hash function and digital signature in detail.

OR

What are the basic crypto primitives that can be applied to a blockchain ?

Answer

1. Cryptographic primitives, or crypto primitives, are low-level cryptographic algorithms that form the basic building blocks of a protocol.
2. Common examples of crypto primitives in the blockchain include hash functions and digital signature.
3. Hash functions are mainly used in linking of blocks and in consensus algorithms.
4. Digital signature is used in blockchain network for authentication.

A. Hashing/Hash functions :

1. Hash value denotes a numeric value of a fixed length that will be generated using cryptographic hash algorithm.
2. It identifies the data uniquely and blockchain state is represented by hash function SHA256.
3. Hashing generates a fixed length hash value that uniquely represents the contents of an arbitrary length string.
4. Identical strings generate the same hash value.

5. Retrieving the original string from hashed values is not possible, since it is a one-way function.
6. Genesis block hash is calculated using initial transactions.
7. Index of the block, previous block hash, timestamp, block data, and nonce are used for calculating the hash value of the consecutive blocks.
8. Example of a hash function :

Data : Blockchain concepts Book chapter

Hash : 06ecd9a034556c403064a9114d26e2d227324520e4c2d5b330cf5f881564ac9b

Even a very small change in input string results a new hash value. In the above-mentioned string, only 'b' is changed in the book string. It creates a completely new hash value for the new string.

Data : Blockchain concepts book chapter

Hash : def6a36ca079b54d3004cadfe14068c54880b6a1873e6da467f20ac9f44ba5b5

B. Digital signature :

1. Digital signature implements an asymmetric cryptography.
2. It uses public and private key pairs for encryption and decryption of the data by the user, thus ensuring the privacy and security.
3. Both the keys are used in blockchain network for authentication.
4. A pair of private and public keys is possessed by every user.
5. The transactions are signed by private key and the transactions are broadcasted in the whole network.
6. The transactions are accessed using public key by the users of the network.
7. Signing and verification phases are two phases which are involved in blockchain.

PART-6

Hash Chain to Blockchain.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.37. Write a short note on : Hash chain.

Answer

1. A hash chain is commonly defined as the repeated application of a cryptographic hash function to a given data.
2. This type of hash cryptography can be extremely useful in security setups.
3. By providing a successive chain, hash chains make it harder for a hacker to hijack data by applying a single input.
4. In hash chain a user supplies an individual input on the first session, and then adds authenticating data on the next session.
5. Over a set of sessions, those individual hash inputs create a "hash chain" that authenticates a single user input in a more profound way.
6. Security properties of hash chain come from the fact that the hash function is a one-way function; therefore retrieving the original data is not possible.
7. A hash chain is similar to a blockchain, as they both utilize a cryptographic hash function for creating a link between two nodes.
8. However, a blockchain is generally intended to support distributed consensus around a public ledger (data), and incorporates a set of rules for encapsulation of data and associated data permissions.

PART-7

Basic Consensus Mechanisms.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.38. What are the various basic consensus mechanisms used in blockchain systems ?

OR

What is Consensus algorithm ? Explain the types of Consensus algorithm. **AKTU 2020-21, Marks 07**

Answer

A consensus mechanism/algorithm is a fault-tolerant mechanism that is used in blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes.

Following are the basic consensus mechanisms used in blockchain systems :

1. **Proof of Work (PoW) :**
   i. First algorithm PoW is developed and used in Bitcoin cryptocurrency.
   ii. This algorithm is widely used in mining process.
   iii. In this algorithm, the nodes/computers in the network agree on the hash of the miner and block will be added in the network.
   iv. First miner will get the reward for solving puzzle.
2. **Proof of Stake (PoS) :**
   i. This algorithm validates the block according to the stake of participants.
   ii. Validation is determined by the investment of the currency.
   iii. Miners are not rewarded with the money.
3. **Practical Byzantine Fault Tolerance :**
   i. This algorithm is based on reaching agreement even when the failure of the nodes happened in the network.
   ii. This algorithm is focused on the node failure by considering both faulty and working nodes.
   iii. Fault tolerance can be achieved by taking the correct values of working nodes and assigning the default vote value for the faulty nodes.
   iv. Thus network reaches an agreement on correct values.
4. **Proof of Activity (PoA) :**
   i. It is a combined approach of PoW and PoS.
   ii. It provides assurance that all transactions are genuine in nature and users reach at a consensus on the status of the ledger.
   iii. In first phase, miners are trying to find out the new block using PoW consensus.
   iv. When new block is identified, process changes into PoS.
5. **Proof of Burn Time :**
   i. The principle behind this consensus algorithm is burning or destroying coins detained by the miners.
   ii. It ensures the agreement of all participating nodes by valid state of network, thus avoiding cryptocoin double spending.
   iii. Miners are allowed to write block proportion for destroying or burning the number of tokens.
6. **Proof of Capacity :**
   i. This algorithm is based on hard disk space instead of computational power of the node.
   ii. Hard disk space of the nodes is utilized for mining the cryptocoins.

iii. Miners can store the possible solutions in the hard drive before mining, thus avoiding changes in the header value rapidly.

iv. Miners can match the required hash value from the list for winning the reward.

7. Proof of Importance :

i. This algorithm is based on PoS.

ii. It works on the concept of harvesting and vesting.

iii. Harvesting determines the node's eligibility for adding block into the network and node vests transaction fees in turn within that block.

Que 1.39. Mention the difference/state difference between proof-of-work and proof-of-stake in blockchaining.

AKTU 2021-22, Marks 07

Answer

		Proof-of-Work	Proof-of-Stake
1.	Mining/ validating a block	The amount of computing work determines the probability of mining a block.	The amount of stake or number of coins determines the likelihood of validating a new block.
2.	Distribution of reward	One who mines the block first, receives a reward.	The validator does not receive a block reward as they are paid a network fee.
3.	Competition	Miners must compete to solve complex puzzles using their computer processing power.	An algorithm determines a winner based on the size of their stake.
4.	Specialized equipment	Application-specific integrated circuits and Graphics Processing Unit are used to mine the coins.	A standard server-grade device is sufficient for PoS-based systems.

5.	Efficiency and reliability	PoW systems are less energy-efficient and less expensive, but they are more reliable.	PoS systems are far more cost and energy-efficient although they are less reliable.
6.	Security	The greater the hash, the more secure the network is.	Staking helps lock crypto assets to secure the network in exchange for a reward.
7.	Forking	Through an economic incentive, PoW systems naturally prevent constant forking.	Forking is not automatically discouraged by PoS systems.

Que 1.40. Explain the steps that are involved in the blockchain project implementation. **AKTU 2020-21, Marks 07**

OR

Explain the steps that are in the blockchain project implementation. Mention the significance of blind signature and how it is useful ? **AKTU 2021-22, Marks 07**

Answer

The blockchain development process consists of the following six stages :

1. **Identify the goal :**
   - i. First of all, it is essential to develop a problem statement and understand all of the issues you want to solve with a proposed solution.
   - ii. Ensure that the blockchain solution will benefit your business abilities.
   - iii. Analyze whether you need to migrate your current solution to the blockchain, or you require a new application to be developed from scratch.
   - iv. Once you decide that you need a blockchain solution for your business operations, the next step is to select the right blockchain platform and blockchain development tools for your project.
2. **Choose the right blockchain platform :**
   - i. Building a blockchain from scratch requires thorough research and takes months to years to develop it successfully.

ii. Therefore, you should build a blockchain app on top of a blockchain platform that meets your business requirements.

iii. You should identify the right blockchain platform for your application based on the factors like consensus mechanism and problems you want to solve.

iv. When the blockchain platform is identified, you must do brainstorming and understand the exact business needs.

3. Brainstorming and blockchain ideation :

i. Once you identify the blockchain platform, you should focus on drafting business requirements and brainstorming ideas.

ii. Find what technology components should be added as off-chain or on-chain entities on the blockchain ecosystem.

iii. Create a roadmap of the product that will help you to build an application within a decided deadline.

iv. You should come up with a blockchain model and conceptual workflow of the blockchain application.

v. Also, decide if the application needs to be developed on a permissioned or permissionless blockchain network.

4. Proof of Concept (PoC) :

i. A proof of concept is done to represent the practical applicability of a blockchain project.

ii. It can be either a design prototype or a theoretical build-up.

iii. In theoretical build-up, each project requires theoretical cases so that users could understand the applicability and viability of the product.

iv. After creating theoretical build-up and receiving feedback, a prototype is designed.

v. When the client approves the PoC, the next step is to prepare technical and visual designs for the application.

5. Visual and technical designs :

i. Visual designs are created to give a look and feel to the application, whereas technical designs represent the application's technology architecture.

ii. UIs are created for each software component.

iii. APIs are designed and integrated to run an application at the back-end.

iv. Once the admin consoles and user interfaces are designed, the application gets ready for development.

6. Development :

i. Development is the significant phase of the blockchain development process, where you should be ready to build the blockchain app.

ii. In this specific stage, you either have to develop or integrate APIs for particular use cases of the application.

iii. The application is built under multiple versions.

Significance of blind signature :

1. Blind signature is a kind of digital signature in which the message is blinded before it is signed. Therefore, the signer will not learn the message content.
2. After blinding the signed message can be unblinded. At this moment, it is similar to a normal digital signature, and it can be publicly checked against the original message.
3. Blind signature can be implemented using a number of public-key encryption schemes.
4. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties.

Use of blind signature :

1. The blind signature is widely used in cryptography applications.
2. The blind signature is used in election/voting systems.
3. The blind signature is used in digital cash schemes.

2 UNIT

Consensus

CONTENTS

PART-1

Consensus : Requirements for the Consensus Protocols.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.1. **What do you understand by consensus and consensus mechanisms ? Explain requirements for the consensus protocols.**

OR

Discuss consensus. Explain requirements for the consensus protocols. **AKTU 2019-20, Marks 07**

Answer

Consensus :

1. Consensus is a process of agreement between distrusting nodes on a final state of data.
2. In order to achieve consensus different algorithms can be used.
3. When multiple nodes are participating in a distributed system and they need to agree on a single value it becomes very difficult to achieve consensus.
4. This concept of achieving consensus between multiple nodes is known as distributed consensus.

Consensus mechanisms :

1. Consensus mechanism is a set of steps that are taken by all the nodes in order to agree on a proposed state or value.
2. The consensus mechanism consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node, and mandatory participation of each node in the consensus process.
3. For decades, these mechanisms have been used to establish consensus among database nodes, application servers, and other enterprise infrastructure.
4. Consensus mechanisms have recently come into the limelight and gained much popularity with the advent of bitcoin and blockchain.

Requirements for the consensus protocols : Following are the various requirements which must be met in order to provide the desired results in a consensus mechanism :

1. **Agreement :** All honest nodes decide on the same value.
2. **Termination :** All honest nodes terminate execution of the consensus process and eventually reach a decision.
3. **Validity :** The value agreed upon by all honest nodes must be the same as the initial value proposed by at least one honest node.
4. **Fault tolerant :** The consensus algorithm should be able to run in the presence of faulty or malicious nodes (Byzantine nodes).
5. **Integrity :** This is a requirement whereby no node makes the decision more than once. The nodes make decisions only once in a single consensus cycle.

PART-2

Proof of Work (PoW).

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.2. Explain Proof of Work (PoW). Also mention its advantages and disadvantages.

Answer

1. The first consensus protocol used in the blockchain network was Proof of Work (PoW).
2. PoW selects one node to create a new block in each round of consensus by computational power competition.
3. In the competition, the participating nodes need to solve a cryptographic puzzle.
4. The node who first addresses the puzzle can have a right to create a new block.
5. The flow of the block creation in PoW is presented in Fig. 2.2.1.

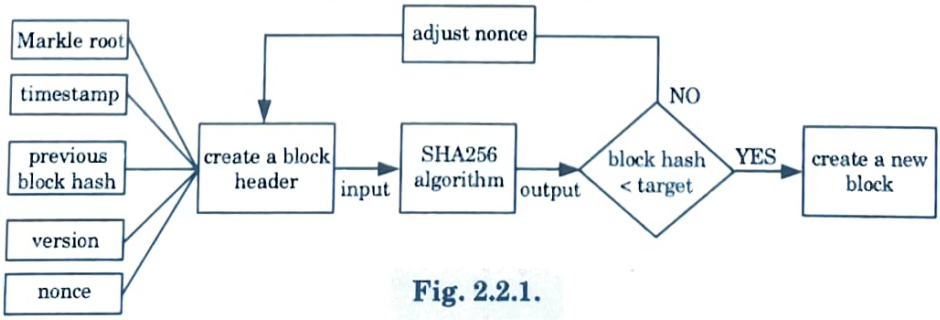

Fig. 2.2.1.

6. It is very difficult to solve a PoW puzzle.
7. Nodes need to keep adjusting the value of nonce (number used once) to get the correct answer, which requires much computational power.
8. It is feasible for a malicious attacker to overthrow one block in a chain.
9. But as the valid blocks in the chain increase, overthrowing a long chain requires a huge amount of computational power.
10. PoW belongs to the probabilistic-finality consensus protocols since it guarantees eventual consistency.

Advantages of PoW :

1. It is highly scalable.
2. High level of security.
3. Provides a decentralized method of verifying transactions.
4. Allows miners to earn crypto rewards.

Disadvantages of PoW :

1. Probability of a "51% attack".
2. Inefficient with slow transaction speeds and expensive fees.
3. High energy usage.
4. Mining often requires expensive equipment.

Que 2.3. Why is Proof of Work (PoW) in Bitcoin necessary ?

Answer

1. A proof of work verification is difficult, costly, and time-consuming to create, but easy to verify.
2. Bitcoin is secure because it is computationally infeasible to attack the network.
3. Requiring Proof of Work for participation is central to this property.
4. Hence Bitcoin relies on computational work on cryptographic challenges as the basis for trust.
5. Proof of Work (PoW) is necessary for security, which prevents fraud, which enables trust.
6. This security ensures that independent data processors (miners) can't lie about a transaction.
7. Proof of Work is used to securely sequence Bitcoin's transaction history while increasing the difficulty of altering data over time.
8. It is used to choose the most valid copy of the blockchain in the network if there are multiple copies.
9. Finally, proof of work is the key to creating a distributed clock, which allows miners to freely enter and leave the network while maintaining a constant rate of operation.

Que 2.4. Explain the working of Proof of Work (PoW) algorithm.

Answer

1. The Proof of Work (PoW) algorithm used by Bitcoin is a variant of Hashcash algorithm.
2. Hashcash was originally proposed as a way to slow malicious actors by making them play an expensive game of chance.
3. In the Bitcoin implementation, blocks are added to each miner's blockchain when one miner solves the game of chance.
4. In order for miners on a network to add blocks to the blockchain, they are required to guess a number which is less than or equal to a Difficulty Target.
5. This value is anywhere between 1 and 2^{256}, which is increased or decreased to change the difficulty required to guess the number.
6. To generate this number, the mining software takes the header of the block they are trying to add and uses SHA-256 encryption to hash it.
7. The header contains key data required by the block to make it secure, including a nonce (number used once) value in the header.
8. This number is altered by miners each time they try to guess the number.
9. If the number generated by the hash exceeds the Difficulty Target, the process is retried until a number less than the value is found.
10. The higher the target value is, the higher the probability of guessing the number and vice-versa.
11. The miners are rewarded in bitcoins and transaction fees if they are the first to find a number less than or equal to the Difficulty Target.
12. Every 4 years the block reward halves, slowing inflation and making each coin more scarce, which should increase the value of a Bitcoin.
13. This is designed to keep miners invested even while as they earn less Bitcoin units.
14. Another key aspect of the design is that the Difficulty Target aims to ensure blocks are added to the blockchain every 10 minutes or so-regardless of the computing power on the network.

PART-3

Scalability Aspects of Blockchain Consensus Protocols.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.5. Explain scalability aspects of blockchain consensus protocols. **AKTU 2019-20, Marks 07**

Answer

1. Scalability is a key barrier when applying blockchain to real business environments.
2. The primary focus is to improve the scalability of blockchain systems, which is due to the inefficiencies of the consensus mechanism- Proof of Work (PoW).
3. The scalability issue is analysed from the perspectives of throughput, storage and networking.
4. Currently, the throughput of the Bitcoin blockchain is restricted to approximately 7 transactions per second (TPS).
5. It is not possible to directly apply blockchain to real business environments where nodes have limited storage and computing resources.
6. The traditional blockchain network is a broadcast medium, in which each node relays all transactions. This data transmission mode cannot be scaled up to handle a large number of transactions due to the requirement for network bandwidth resources.

Approaches for improving the scalability of blockchain consensus protocols : Following approaches exist for improving the scalability of blockchain consensus protocols :

1. **Increasing the Block Size :**
   i. Increasing the block size is an obvious solution to increase throughput by including more transactions in each block.
   ii. However, this solution increases the block propagation delay and spends more nodes efforts to process and confirm transactions.
2. **Reducing the Transaction Size :**
   i. By increasing the number of transactions in each block we can reduce the transaction size.
   ii. In blockchain systems digital signatures account for 60-70 percent of the transaction size.
   iii. Segregated Witness (SegWit), separates digital signatures from the rest of the transaction data and moves the digital signatures to the end of blocks.
   iv. In this way, the transaction size is reduced, and one block can contain more transactions.
3. **Reducing the Number of Transactions Processed by Nodes :**
   i. An alternative to improving the throughput is to reduce the number of transactions processed by nodes.

ii. Off-chain transactions, sharding, and decoupling management/control from execution are three solutions.

A. **Off-chain transactions :** Off-chain transactions make use of the fact that if nodes make frequent transactions, then it is not necessary to store every transaction on the blockchain, only the net settlement is needed.

B. **Sharding :** Sharding is an effective technique to improve the horizontal scalability of blockchain systems. With blockchain sharding, nodes are separated into different shards. Each shard only processes a small portion of all transactions. In this way, transactions are processed in parallel. In sharding blockchain systems, the throughput increases linearly as more nodes join the systems.

C. **Decoupling Management/Control from Execution :** The decoupling of management/control from execution can be done via virtualization, with which multiple virtual DLT systems with varying characteristics can be dynamically created on the same substrate DLT system to accommodate different QoS requirements.

PART-4

Permissioned Blockchains.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.6. What are the permissioned blockchains ? What are its key characteristics ?

Answer

1. Permissioned blockchains are blockchain networks that require access to be part of.
2. These blockchains can be thought of as closed ecosystems that can only be accessed by those who are allowed access.
3. Permissioned blockchains use an access control layer to govern who has access to the network.
4. A permissioned blockchain provides a way to secure the interactions among a group of entities that have a common goal but which may not fully trust each other.
5. Each contributor in the network will have the whole record of the transactions and the associated blocks.

6. All blocks are encrypted by a private key and cannot be interpreted by anyone.
7. They are controlled only by authorized users of a specific organization.
8. A permissioned system also have a restriction on the consensus participants.
9. This makes permissioned blockchains highly configured and controlled by the owners.
10. Permissioned blockchains are crafted to take advantage of blockchains without sacrificing the authority aspect of a centralized system.
11. Examples of permissioned blockchain are Hyperledger Fabric, Corda, and Quorum.

Key characteristics of permissioned blockchains :

1. Controlled transparency based on the goals of participating organizations.
2. Development by private entities.
3. Lack of anonymity.
4. Lack of a central authority, but a private group authorizes decisions.

Que 2.7. Give the benefits and drawbacks of permissioned blockchains.

Answer

A. **Benefits of Permissioned Blockchains :** Following are the benefits of permissioned blockchains :

1. **Efficient performance :** The limited number of nodes on the platform removes the unnecessary computations required to reach consensus on the network, improving the overall performance.
2. **Proper governance structure :** Permissioned networks comes with an appropriate structure of governance. This means that they are organized. Administrators also require less time to update the rules over the network.
3. **Decentralized storage :** Permissioned networks utilizes blockchain decentralized nature for data storage.
4. **Cost-Effective :** Permissioned blockchains are more cost-effective when compared with the permissionless blockchains.

B. **Drawbacks of Permissioned Blockchains :** Following are the drawbacks of permissioned blockchains :

1. **Compromised security :** The security of a permissioned network is as good as the member's integrity. This means that a small section of a permissioned system can work together to modify the data stored within the network. In this way, the integrity of the network can be compromised.

2. **Control, Censorship, and Regulation :** Permissioned blockchains work like a public blockchains, but with regulations. However, the regulations bring censorship to the network, where the authority can restrict a transaction. These are a threat to any business that is using the permissioned network.

Que 2.8. **Differentiate between permissioned and permissionless blockchain.**

Answer

S. No.	Category	Permissioned	Permissionless
1.	Speed	Faster	Slower
2.	Privacy	Private membership	Transparent and open - anyone can become a member
3.	Development	via private entities	via open source
4.	Ownership	Managed by a group of nodes pre-defined	Public ownership - no one owns the network
5.	Decentralization	Partially decentralized	Truly decentralized
6.	Cost	Cost-effective	Not so cost-effective
7.	Security	Less secure	More secure

PART-5

Design Goals.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.9. **Explain design goals for permissioned blockchains.**

Answer

1. If you are trying to decide on the design goals for permissioned blockchains following are some things that you should take into account :
   i. The speed in which your blocks will need to be written into the blockchain.

ii. Type of network you will be using.

iii. How many miners, writers, or validators will be needed ?

iv. How "final" does a block need to be ?

v. To what degree do you put your trust in the nodes/operators ?

2. In a permissioned blockchain, choosing the right consensus protocol for permissioned blockchain depends on factors like the extent of decentralization required.

3. For example, how much the participants in a network trust each other, the number of permissions that must be granted to all the participants, etc.

4. Permissioned blockchains usually use Practical Byzantine Fault Tolerance (PBFT) algorithms and its variants like voting and lottery-based consensus.

5. Permissioned blockchains are crafted to take advantage of blockchains without sacrificing the authority aspect of a centralized system.

PART-6

Consensus Protocols for Permissioned Blockchains.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.10. What are various types of consensus protocol used in permissioned blockchain networks ?

Answer

Following are various types of consensus protocol used in permissioned blockchains :

A. Practical Byzantine Fault Tolerance (PBFT) Consensus :

1. One of the models that is used to facilitate consensus in permissioned blockchain is the Practical Byzantine Fault Tolerance (PBFT) algorithm.

2. In this model, each node exists in an internal state.

3. Each time a node receives a message, they use the message with respect to their internal state to perform a computation.

4. Consequently, this computation will send messages to other nodes to ask if the transaction is valid.

5. After receiving verification, the first node will broadcast that decision with all the other participants in the network.
6. A consensus decision is achieved based on the total confirmations submitted by all the nodes.
7. PBFT can be very beneficial for low latency storage systems.
8. This type of model is often used in digital assets backed platforms that don't need big amount of capacity, but carry out a large number of transactions.
9. PBFT makes sure that the transaction records within the network are accurate.
10. Hyperledger, a permissioned blockchain, use this model.

B. Federated Consensus :

1. In federated consensus, a set of signers help each node in the blockchain network to reach the consensus stage.
2. To carry out the process in an efficient manner the block signers use a single block generator.
3. This block generator receives, holds and filters all the transactions.
4. The generator's signature is used to coordinate with the signers for the block validation process.
5. Each block signer will verify the block which is signed by the block generator and which fulfills the certain conditions set by the network.
6. Once the block generator receives enough signatures from the network, the block will get published to the network.
7. This model guarantees security and transparency.
8. It is ideal for use cases such as cross border remittance, real time KYC, etc.
9. Common examples of blockchains that use this model are Stellar and Ripple.

C. Round Robin Consensus :

1. In Round Robin Consensus, validators take part in the consensus process by signing votes for blocks.
2. There are three main types of votes : a prevote, a precommit and a commit.
3. A block is considered to be committed by the network when a two third majority of validators have signed and broadcasted commits for that block.
4. At each height of the blockchain a round-based protocol is run to determine the next block.
5. Each round consists of three steps: propose, prevote, and precommit.

6. The propose, prevote, and precommit steps each take one third of the total time allocated for that round.
7. Each round is longer than the previous round followed by a small fixed increase of time.
8. This allows the network to eventually achieve consensus in a limited concurrent network.
9. In this model, several nodes play a major role in validating and signing transactions, which makes this process more secure.
10. There are also lower chances of double spend attacks due to the voting power distribution among trusted nodes.
11. Round robin consensus mechanism is ideal for the trade, finance and supply chain industries.
12. Common examples of blockchains that use this model are Multichain and Tendermint.

Que 2.11. What is a permissioned blockchain ? Explain design goals, consensus protocols for permissioned blockchains.

AKTU 2019-20, Marks 07

Answer

Permissioned blockchain : Refer Q. 2.6, Page 2–6P, Unit-2.

Design goals : Refer Q. 2.9, Page 2–9P, Unit-2.

Consensus protocols for permissioned blockchains : Refer Q. 2.10, Page 2–10P, Unit-2.

3 UNIT

Hyperledger Fabric

CONTENTS

PART-1

Hyperledger Fabric

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.1. What is Hyperledger Fabric ?

OR

Discuss Hyperledger Fabric.

Answer

1. The Linux Foundation founded the Hyperledger project in 2015 to advance cross-industry blockchain technologies.
2. Hyperledger Fabric is designed as modular, scalable and secure foundation for offering industrial blockchain solutions.
3. It encourages a collaborative approach to develop blockchain technologies via a community process that encourage open development and the adoption of key standards.
4. Hyperledger Fabric is one of the blockchain projects within Hyperledger.
5. It consists of a ledger, uses smart contracts, and is a system by which participants manage their transactions.
6. Hyperledger Fabric is private and permissioned.
7. The members of a Hyperledger Fabric network are enrolled through a trusted Membership Service Provider (MSP).
8. Hyperledger Fabric also offers several pluggable options.
9. Ledger data can be stored in multiple formats, consensus mechanisms can be swapped in and out, and different MSPs are supported.
10. Hyperledger Fabric also offers the ability to create channels, allowing a group of participants to create a separate ledger of transactions.

Que 3.2. Mention the key design features of Hyperledger Fabric model.

Answer

Following are the key design features of Hyperledger Fabric model :

1. **Assets :** Asset definitions enable the exchange of almost anything with monetary value over the network, from whole foods to antique cars to currency futures.

2. **Chaincode :** Chaincode execution is partitioned from transaction ordering, limiting the required levels of trust and verification across node types, and optimizing network scalability and performance.
3. **Ledger Features :** The immutable, shared ledger encodes the entire transaction history for each channel, and includes SQL-like query capability for efficient auditing and dispute resolution.
4. **Privacy :** Channels and private data collections enable private and confidential multi-lateral transactions that are usually required by competing businesses and regulated industries that exchange assets on a common network.
5. **Security and Membership Services :** Permissioned membership provides a trusted blockchain network, where participants know that all transactions can be detected and traced by authorized regulators and auditors.
6. **Consensus :** A unique approach to consensus enables the flexibility and scalability needed for the enterprise.

Que 3.3. What are the advantages of Hyperledger Fabric ?

Answer

Following are the advantages of Hyperledger Fabric :

1. **Rich queries :** One can run these queries to find the transactions that have been executed on the blockchain platform.
2. **Modular architecture :** Modular means that various modules can be used either together or on-need basis. Thus, it is different from Ethereum where you have to utilize the entire blockchain. In Hyperledger, you can use a module that you require.
3. **Protection of digital keys and sensitive data :** Hyperledger works on the same distributed ledger concept and keeps your digital keys and data secure from tampering.
4. **Permissioned data :** A party can view/use the data only if it is permissioned to do so. Unlike Ethereum and Bitcoin blockchain, everyone cannot see all the data. This is essential for enterprise applications.
5. **Performance and scalability :** Hyperledger is better than many other public blockchain networks when it comes to performance and scalability, as its target audience is enterprises who have stringent performance requirements. Moreover, it is undergoing further improvements in order to make it more efficient and scalable.

Que 3.4. Briefly discuss the Hyperledger Fabric architecture.

Answer

1. Hyperledger Fabric is a distributed operating system for permissioned blockchains that executes distributed applications written in general purpose programming languages.
2. Hyperledger Fabric introduces the execute-order-validate blockchain architecture and does not follow the standard order execute design.

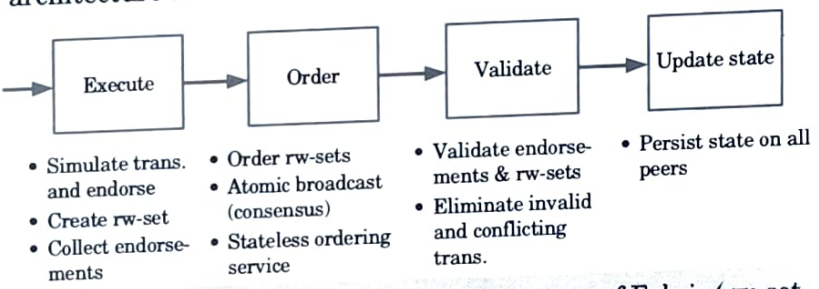

Fig. 3.4.1. Execute-order-validate architecture of Fabric (rw-set means a readset and writeset).

3. A distributed application for Fabric consists of two parts :
   i. A smart contract, called chaincode, which is program code that implements the application logic and runs during the execution phase.
   ii. An endorsement policy that is evaluated in the validation phase.
4. A Hyperledger Fabric blockchain consists of a set of nodes that form a network.
5. As Hyperledger Fabric is permissioned, all nodes that participate in the network have an identity, as provided by a modular membership service provider (MSP).
6. Nodes in a Fabric network take up one of three roles :
   i. Clients submit transaction proposals for execution, help orchestrate the execution phase, and, finally, broadcast transactions for ordering.
   ii. Peers execute transaction proposals and validate transactions.
   iii. Ordering Service Nodes (OSN) are the nodes that collectively form the ordering service. In short, the ordering service establishes the total order of all transactions in Hyperledger Fabric.
7. A Fabric network actually supports multiple blockchains connected to the same ordering service.
8. Each such blockchain is called a channel and may have different peers as its members.
9. Channels can be used to partition the state of the blockchain network, but consensus across channels is not coordinated and the total order of transactions in each channel is separate from the others.

Que 3.5. Explain the transaction flow diagram of consensus with example.

Answer

Following example explains the transactional mechanics that take place during a standard asset exchange :

Example :

1. The scenario includes two clients, A and B, who are buying and selling "Quantum Series".
2. They each have a peer on the network through which they send their transactions and interact with the ledger.

Process :

1. **Client A initiates a transaction :**
   - i. Client A sends a request to purchase "Quantum Series".
   - ii. This request targets peerA and peerB, since all peers must endorse any transaction.
   - iii. Next, the transaction proposal is constructed.
   - iv. The proposal is a request to invoke a chaincode function.
   - v. With the help of chaincode function the ledger is read and/or updated.
   - vi. The transaction proposal is submitted to a target peer, which will manage the transaction submission on behalf of the client.
2. **Endorsing peers verify signature and execute the transaction :**
   - i. The endorsing peers verify :
     - a. that the transaction proposal is well formed,
     - b. it has not been submitted already in the past,
     - c. the signature is valid, and
     - d. that the submitter is properly authorized to perform the proposed operation on that channel.
   - ii. The endorsing peers take the transaction proposal inputs as arguments to the invoked chaincode's function.
   - iii. The chaincode is then executed against the current state database to produce transaction results.
3. **Proposal responses are inspected :**
   - i. The target peer verifies that the proposal responses are the same prior to proceeding with the transaction submission.
4. **Target peer assembles endorsements into a transaction :**
   - i. The target peer "broadcasts" the transaction proposal and response within a "transaction message" to the ordering service.

ii. The ordering service receives transactions, orders them, and creates blocks of transactions per channel.

5. **Transaction is validated and committed :**
   i. The blocks of transactions are "delivered" to all peers on the channel.
   ii. The transactions within the block are validated to ensure endorsement policy is fulfilled and there is no changes in ledger state.
   iii. Transactions in the block are tagged as being valid or invalid.

6. **Ledger updated :**
   i. Each peer appends the block to the channel's chain.
   ii. An event is emitted by each peer to notify that the transaction has been immutably appended to the chain and whether the transaction was validated or invalidated.

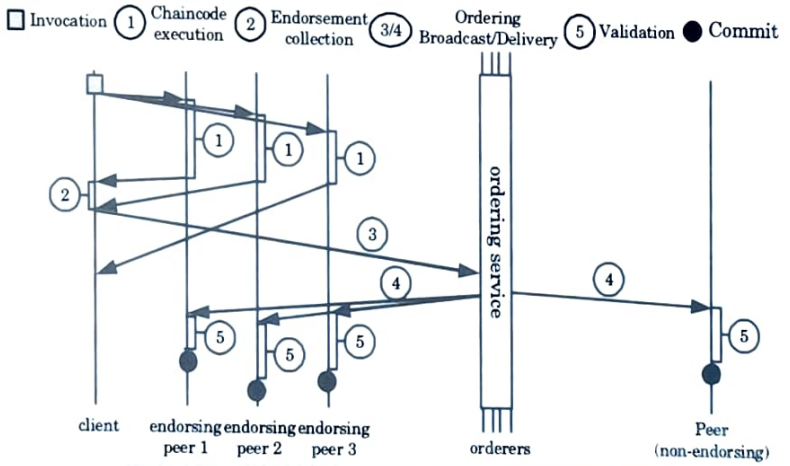

Fig. 3.5.1. Fabric high level transaction flow.

Que 3.6. **What do you mean by Identity in a blockchain network ?**

Answer

1. A blockchain network includes different actors like peers, orderers, client applications, administrators and more.
2. Each of these actors has a digital identity encapsulated in an X.509 digital certificate.
3. These identities determine the exact permissions over resources and access to information that actors have in a blockchain network.
4. A digital identity has some additional attributes that Hyperledger Fabric uses to determine permissions.
5. For an identity to be verifiable, it must come from a trusted authority.

6. A membership service provider (MSP) is that trusted authority in Hyperledger Fabric.
7. An MSP is a component that defines the rules that govern the valid identities for particular organization.
8. The default MSP implementation in Hyperledger Fabric uses X.509 certificates as identities, adopting a traditional Public Key Infrastructure (PKI) hierarchical model.

Que 3.7. What do you mean by Membership Service Provider (MSP) ?

Answer

1. Since Hyperledger Fabric is a permissioned network, blockchain participants need a way to prove their identity to the rest of the network in order to transact on the network.
2. Public Key Infrastructure (PKI) can provide verifiable identities through a chain of trust.
3. However, a private key can never be shared publicly.
4. To overcome this, a mechanism is required to enable that proof which is where the MSP comes in.
5. MSPs are used to define the organizations that are trusted by the network members.
6. MSPs are also the mechanism that provides members with a set of roles and permissions within the network.
7. The MSP is the mechanism that enables you to participate on a permissioned blockchain network.
8. The MSP identifies which Root CAs and Intermediate CAs are accepted to define the members of a trust domain.
9. MSP turns an identity into a role by identifying specific privileges an actor has on a node or channel.
10. A Hyperledger Fabric blockchain network can be governed by one or more MSPs.

Que 3.8. What is a policy ? Why are policies needed in Hyperledger Fabric ?

Answer

Policy : A policy is a set of rules that define the structure for how decisions are made and specific outcomes are reached.

Need of policies in Hyperledger Fabric :

1. Policies are one of the things that make Hyperledger Fabric different from other blockchains like Ethereum or Bitcoin.

2. The policies that govern the network are fixed at any point in time and can only be changed using the same process that governs the code.
3. Policies allow members to decide which organizations can access or update a Hyperledger Fabric network.
4. Policies contain the lists of organizations that have access to a given resource.
5. They also specify how many organizations need to agree on a proposal to update a resource.
6. Policies also evaluate the collection of signatures attached to transactions and validate if the signatures fulfill the governance agreed to by the network.

PART-2

Decomposing the Consensus Process.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.9. How do we decompose the consensus process ?

Answer

1. In distributed ledger technology, consensus has become synonymous with a specific algorithm, within a single function.
2. However, consensus encompasses more than simply agreeing upon the order of transactions.
3. This differentiation is highlighted in Hyperledger Fabric.
4. In Hyperledger Fabric consensus is defined as the full-circle verification of the correctness of a set of transactions comprising a block.
5. In Hyperledger Fabric consensus is achieved when the order and results of a block's transactions have met the explicit policy criteria checks.
6. These checks take place during the lifecycle of a transaction.
7. These checks include the usage of endorsement policies and system chaincodes to ensure that these policies are enforced.
8. These system chaincodes also helps to make sure that enough endorsements are present and they are derived from appropriate entities.
9. Also a versioning check takes place during which the current state of the ledger is agreed upon.

10. This versioning check takes place before any blocks containing transactions are appended to the ledger.
11. This final check provides protection against double spend operations and other threats.
12. In addition to these, there are ongoing identity verifications happening in all directions of the transaction flow.
13. Access control lists are implemented on hierarchical layers of the network.
14. Payloads are repeatedly signed, verified and authenticated as a transaction proposal passes through the different architectural components.
15. Consensus in Hyperledger Fabric is a byproduct of the ongoing verifications that take place during a transaction's journey from proposal to commitment.

Que 3.10. Discuss Hyperledger Fabric. How do we decompose the consensus process ? **AKTU 2019-20, Marks 07**

Answer

Hyperledger Fabric : Refer Q. 3.1, Page 3–2P, Unit-3.

Decomposing the consensus process : Refer Q. 3.9, Page 3–8P, Unit-3.

PART-3

Hyperledger Fabric Components.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.11. Mention the components of Hyperledger Fabric.

Answer

A Hyperledger Fabric network has following components :

1. **Assets :** An asset is anything that has value. An asset has state and ownership. Assets are represented in Hyperledger Fabric as a collection of key-value pairs.
2. **Shared ledger :** The ledger records the state and ownership of an asset. The ledger consists of two components :

i. **World state (State database) :** The world state describes the state of the ledger at a given point in time. It's the database of the ledger.

ii. **Blockchain :** The blockchain is a transaction log history that records all transactions.

3. **Smart Contract :**
   i. A smart contract is code that manages access and modifications to a set of key-value pairs in the world state.
   ii. Hyperledger Fabric smart contracts are called chaincode.
   iii. Chaincode is software that defines assets and related transactions.
   iv. Chaincode is invoked when an application needs to interact with the ledger.
   v. Chaincode is installed onto peer nodes and instantiated to one or more channels.

4. **Peer nodes :**
   i. Peers are a fundamental element of the network because they host ledgers and smart contracts.
   ii. A peer executes chaincode, accesses ledger data, endorses transactions, and interfaces with applications.
   iii. Peers are owned and maintained by members.

5. **Ordering service :**
   i. The ordering service packages transactions into blocks to be delivered to peers on a channel.
   ii. It guarantees the transaction delivery in the network.
   iii. It communicates with peers and endorsing peers.
   iv. The ordering service is a common binding for the overall network.
   v. It contains the cryptographic identity material tied to each member.
   vi. The supported configuration mechanisms for the ordering service are Solo and Kafka.

6. **Channels :**
   i. A channel is a private blockchain overlay which allows for data isolation and confidentiality.
   ii. A channel-specific ledger is shared across the peers in the channel.
   iii. Transacting parties must be properly authenticated to a channel in order to interact with it.
   iv. Channels are defined by a Configuration-Block.

7. **Hyperledger Fabric CA :**
   i. Hyperledger Fabric CA is the default Certificate Authority component, which issues PKI-based certificates to network member organizations and their users.

ii. The CA issues one root certificate to each member and one enrollment certificate to each authorized user.

PART-4

Chaincode Design and Implementation.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.12. What is Chaincode ?

Answer

1. Chaincode is the term for programs that run on top of the blockchain to implement the business logic of how applications interact with the ledger.
2. Chaincode is a program, written in Go, node.js, or Java.
3. The execution of chaincode is isolated from the endorsing peer process.
4. Chaincode initializes and manages ledger state through transactions submitted by applications.
5. A chaincode typically handles business logic agreed to by members of the network, so it may be considered as a "smart contract".
6. Each chaincode is implemented as an isolated program that maintains its own private state on the ledger.
7. State created by a chaincode can't be accessed directly by another chaincode.

Que 3.13. Mention the parameters required in chaincode design.

Answer

Following are the parameters required in chaincode design :

1. **Composite keys :**
   i. We often need to store multiple instances of one type on the ledger, for example, multiple trade agreements.
   ii. The keys of those instances are constructed from a combination of attributes.
   iii. API functions can be provided in SHIM library to construct a composite key of an instance based on a combination of several attributes.

iv. These functions simplify composite key construction.

v. Composite keys can then be used to record and retrieve values.

vi. Composite keys allow you to search for assets based on components of the key in range queries.

2. Range queries :

i. SHIM allows API functions to retrieve sets of assets based on a range criteria.

ii. The composite keys can be modeled to enable queries against multiple components of the key.

iii. The range functions return an iterator over a set of keys matching the query criteria.

iv. The returned keys are in lexical order.

v. Also, when a composite key has multiple attributes, the range query function can be used to search for keys matching a subset of the attributes.

3. State queries and CouchDB :

i. By default, Fabric uses LevelDB to store the world state.

ii. Fabric can configure peers to store world state in CouchDB.

iii. When assets are stored in the form of JSON documents, CouchDB allows you to perform complex queries for assets based on the asset state.

iv. Fabric forwards queries to CouchDB and returns an iterator which can be used to iterate over the result set.

4. Indexes :

i. Performing queries on large datasets is a computationally complex task.

ii. Fabric provides a mechanism for defining indexes on the CouchDB hosted world state to increase efficiency.

iii. Indexes are also required for sorting operations in queries.

iv. An index is defined in JSON in a separate file.

v. During compilation, the indexes are packaged along with the chaincode.

vi. Upon installation and instantiation of the chaincode on the peer, the indexes are automatically deployed onto the world state and used by queries.

5. ReadSet and WriteSet :

i. On receipt of a transaction invocation message, the endorsing peer executes a transaction.

ii. The execution invokes the chaincode in the context of the peer's world state.

iii. It records all reads and writes of data on the ledger into a WriteSet and ReadSet :

a. WriteSet :

i. The transaction's WriteSet contains a list of key and value pairs that were modified during the execution by the chaincode.

ii. When the value of a key is modified the WriteSet will contain the updated key and value pair.

iii. When a key is deleted, the WriteSet will contain the key with an attribute marking the key as deleted.

b. ReadSet :

i. The transaction's ReadSet contains a list of keys and their versions that were accessed during execution by the chaincode.

ii. The version number of a key is derived from a combination of the block number and the transaction number within the block.

iii. This design enables the efficient searching and processing of data.

iv. Whenever a chaincode reads the value of a key, the latest committed value in the ledger is returned.

6. Multiversion concurrency control :

i. Fabric uses a multiversion concurrency control (MVCC) mechanism to ensure consistency in the ledger and to prevent double spending.

ii. To ensure consistency, Fabric uses a versioning system of keys stored on the ledger.

iii. The aim of the versioning system is to ensure that transactions are ordered and committed into the ledger in a sequence that does not introduce inconsistencies.

Que 3.14. Explain the implementation of chaincode functions.

Answer

1. After establishing the basic building blocks of chaincode and the methods which initiates the chaincode, we need to implement the functions of the chaincode.
2. These functions help in recording and retrieving data to and from the ledger to provide the business logic of the smart contract.
3. Following steps are involved in the implementation of chaincode functions :

A. Defining chaincode assets :

1. We first define the structure of assets, which will be recorded onto the ledger.
2. The assets are defined as struct types with a list of attribute names and types.
3. The attribute names are used to serialize the assets into the JSON objects.

B. Coding chaincode functions :

1. In this section we will implement the chaincode functions.
2. To implement the chaincode functions, we will use three SHIM API functions that will read assets from the world state and record changes.
3. Reads and writes of these functions are recorded into ReadSet and WriteSet respectively.

C. Creating an asset :

1. After implementing the chaincode function, we will create a new asset.
2. Using a requestTrade function, we will create a new trade agreement and then record that agreement on the ledger.
3. The implementation of the function is as follows :
   i. The invoker invokes the function.
   ii. Then we validate and extract the arguments.
   iii. We serialize trade agreement with JSON into an array of bytes.
   iv. We create a unique key, under which we will store trade agreement.
   v. Finally, we use the key and serialized trade agreement to store the value into the WriteSet.

D. Reading and modifying an asset :

1. After implementing the function to create a trade agreement, we need to implement a function to accept the trade agreement.
2. This function will retrieve the agreement, modify its status to ACCEPTED, and put it back on the ledger.
3. The implementation of the function is as follows :
   i. First we construct the unique composite key of the trade agreement we want to retrieve.
   ii. Then we retrieve the value using function GetState.
   iii. Now, we deserialize the array of bytes into the instance of the trade agreement struct.
   iv. Then we modify the status so it reads ACCEPTED.

v. Finally, we store the updated value on the ledger.

E. Main function :

1. The main function is added at the initial point of a program.
2. When an instance of the chaincode is deployed on a peer, the main function is executed to start the chaincode.

Que 3.15. Write a short note on : Chaincode design and implementation.

Answer

1. Designing and implementing a well-functioning chaincode is a complex software engineering task.
2. It requires both the knowledge of the Fabric architecture as well as the correct implementation of the business requirements.
3. Following steps are involved in chaincode design and implementation :

Step 1 : Setting up the development environment :

1. Before we can start coding our chaincode, we need to first set up development environment.
2. This allows us to control how we built and run the chaincode.

Step 2 : Creating a chaincode : It consists of the following steps :

1. **The chaincode interface :** Every chaincode must implement the Chaincode interface, whose methods are called in response to the received transaction proposals.
2. **Setting up the chaincode file.**
3. **The Invoke method :** The Invoke method is invoked whenever the state of the blockchain is queried or modified.

Step 3 : Access control : A key feature of a secure and permissioned blockchain is access control mechanism. It consists of the following steps :

1. Registering a user.
2. Enrolling a user.
3. Retrieving user identities and attributes in chaincode.

Step 4 : Implementing chaincode functions : These functions help in recording and retrieving data to and from the ledger to provide the business logic of the smart contract.

Step 5 : Testing chaincode :

1. The test suite file provides functions for managing test states and supporting formatted test logs.
2. The output of the test is written into the standard output.
3. It can be inspected in the terminal.

PART-5

Beyond Chaincode : Fabric SDK and Front End.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.16. What are Hyperledger Fabric SDKs ?

Answer

1. The Hyperledger Fabric SDK allows applications to interact with a Fabric blockchain network.
2. It provides a simple API to submit transactions to a ledger or query the contents of a ledger with minimal code.
3. The Hyperledger Fabric SDK provides a structured environment of libraries for developers to write and test chaincode applications.
4. The SDK is fully configurable and extensible through a standard interface.
5. Components, including cryptographic algorithms for signatures, logging frameworks and state stores, are easily swapped in and out of the SDK.
6. The SDK provides APIs for transaction processing, membership services, node traversal and event handling.
7. Currently, there are three officially supported SDKs - for Node.js, Java, and Go.

Que 3.17. Write a short note on : Hyperledger Fabric SDK for Node.js.

Answer

1. The Hyperledger Fabric SDK for Node.js is designed in an Object-Oriented programming style.
2. Its modular construction enables application developers to plug in alternative implementations for handling transaction commit events, transaction evaluation (query), and other behaviors.
3. The SDK is composed of following modules :
   i. **fabric-network :** Provides high level APIs for client applications to interact with smart contracts (chaincode), and is the recommended API for building client applications.

ii. **fabric-ca-client :** Provides APIs to interact with the optional Certificate Authority component, fabric-ca, that contains services for membership management.

iii. **fabric-common :** A low-level API, used to implement fabric-network capability, that provides APIs to interact with the core components of a Hyperledger Fabric network, namely the peers, orderers and event streams.

Que 3.18. Write a short note on : Hyperledger Fabric SDK for Java.

Answer

1. The SDK provides a layer of abstraction to interact with a Hyperledger Fabric blockchain network.
2. It allows Java applications to manage the lifecycle of Hyperledger channels and user chaincode.
3. The SDK also provides a means to execute user chaincode, query blocks and transactions on the channel, and monitor events on the channel.
4. The SDK acts on behalf of a particular User which is defined by the embedding application through the implementation of the SDK's User interface.
5. Channels may be serialized via Java serialization in the context of a client.
6. Applications need to handle migration of serialized files between versions.
7. The SDK also provides a client for Hyperledger's certificate authority.
8. The SDK is however not dependent on this particular implementation of a certificate authority.
9. Other Certificate authority's maybe used by implementing the SDK's Enrollment interface.

Que 3.19. Write a short note on : Hyperledger Fabric SDK for Go.

Answer

1. This SDK enables Go developers to build solutions that interact with Hyperledger Fabric.
2. Package client enables Go developers to build client applications using the Hyperledger Fabric programming model.
3. Client applications interact with the blockchain network using a Fabric Gateway.
4. A client connection to a Fabric Gateway is established by calling client.Connect() with a client identity, client signing implementation, and client connection details.

5. The returned Gateway can be used to transact with smart contracts deployed to networks accessible through the Fabric Gateway.

Que 3.20. Write a short note on : Fabric front-end.

Answer

1. Front-end is typically written in HTML and makes up the user interface of the application.
2. The front-end of a blockchain application is really no different from that of a traditional web application.
3. Front-end devices can use the same CDNs and other libraries that they use for conventional web applications.
4. A node back-end server creates the blockchain interface for the front-end application.
5. This back-end interacts with the Fabric-SDK provided through the official Hyperledger Fabric repository.
6. The Hyperledger Fabric network acts as the back-end layer for client applications.
7. A client application can be anything such as a dapp, portal, business activity, or web site; these types of applications are the front-end layer.
8. They can access chaincodes, transactions, and events through coding the Hyperledger Fabric SDK.

PART-6

Hypeledger Composer Tool.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.21. Discuss Hyperledger Composer tool. What are its components ? **AKTU 2019-20, Marks 07**

Answer

1. Hyperledger Composer is a set of collaboration tools for building blockchain business networks.
2. It accelerate the development of smart contracts and blockchain applications, as well as their deployment across a distributed ledger.

3. Hyperledger Composer is used to model the participants, assets, transactions, and events in a particular business network.
4. This model is then used to generate blockchain smart contracts and ledgers that implement these elements to the blockchain network.
5. We also use the Hyperledger Composer model to generate a set of domain-specific APIs to access the transactions that manipulate them in the Hyperledger Fabric blockchain.
6. These APIs will be used by applications on behalf of individuals, organizations, systems, and devices.

Components of Hyperledger Composer : Hyperledger Composer includes the following main components :

1. **Business network archive :** The business network archive captures the core data of a business network like business model, transaction logic and access controls. It then package these elements and deploys them to runtime.
2. **Composer playground :** This web-based tool allows developers to learn Hyperledger Composer, model out their business network, test that network, and deploy that network to a live instance of a blockchain network. The Composer playground offers a repository of sample business networks that can provide a base for building your own business network.
3. **REST API support and integration capabilities :** A LoopBack connector for business networks has been developed that exposes a running network as a REST API which can easily be consumed by client applications and an integrate non-blockchain applications.

Que 3.22. What is the use of Hyperledger Composer tool for developers ?

Answer

Developers use Hyperledger Composer tool to :

1. Model reusable, core components in a business network-assets, participants, transaction logic, and access controls for the business network. These can then be shared across multiple organizations.
2. Generate JavaScript and REST APIs based on the business network definition that can be used to interact with applications.
3. Integrate legacy systems, create skeleton applications, and run analytics on the blockchain network.
4. Begin to develop and test on a web-based Composer playground without installing anything.
5. Deploy the business network to a live blockchain instance of Hyperledger Fabric or other blockchain network.

Que 3.23. What are the benefits of adopting Hyperledger Composer tool ?

Answer

Blockchain clients who adopt Hyperledger Composer experience the following benefits :

1. Faster creation of blockchain applications.
2. Eliminating the massive effort required to build blockchain applications from scratch.
3. Reduced risk with well-tested and efficient design.
4. Creates reusable assets based on best practices.
5. Greater flexibility as the higher-level abstractions make it far simpler to iterate.

4 UNIT

Use Case 1 & 2

CONTENTS

PART-1

Blockchain in Financial Software and Systems (FSS).

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.1. Discuss blockchain in financial software and systems.

Answer

Blockchain in financial software and systems :

1. Blockchain has been applied to banking and financial services in various ways and getting numerous benefits.
2. Smart contract service helps in conducting financial transactions without an intermediary.
3. It has the potential to manage securities, deeds, settlements, and claims in an automated manner.
4. Most people know the term "blockchain" in relation to the cryptocurrency Bitcoin.
5. However, mainstream financial institutions have started to use blockchain technology without Bitcoin to make their own transactions more efficient and secure.
6. Blockchain is essentially a ledger of recorded financial transactions.
7. This ledger is distributed, published, and stored in multiple locations. When a transaction occurs, it is added to each copy of the ledger.
8. This helps ensure an accurate record of transactions.
9. Because there are many copies of the ledger, blockchain is practically immutable and highly secure.
10. To alter any part of the record, a hacker would have to change every copy of the ledger simultaneously, which would be extremely difficult.

Que 4.2. What is the feature of blockchain that make its application useful in financial services ?

Answer

1. Blockchain is one of the most exalted technology today which has a pervading impact on financial services.

2. Blockchain uses digital signature to guarantee the provenance of the transaction.
3. The key advantage of blockchains resilient architecture is the protection of distributed ledger.
4. Blockchain has the promising feature to make financial services efficient and improve regulatory control.
5. Decentralized consensus mechanism makes transactions immutable and updatable only through consensus among peers over the network.
6. This design protect displace traditional third-party functions in a transaction.
7. Blockchain distributed ledger offers consensus and immutability about the transfer of assets within a business networks.

Que 4.3. What are the benefits of blockchain technology in financial sector ?

Answer

Financial sector is using blockchain because of the following benefits :

1. **Transparency :**
   i. The distributed ledger is shared among all the participants over the network.
   ii. All can keep an eye on every ongoing transaction leaving behind any chance of discrepancy.
2. **Security :**
   i. Hackers are trying all their tactics to hack the device.
   ii. It is very pricey to hack the blockchain network in terms of time.
   iii. Blockchain technology is developed such that even if one block is altered, all information of the block gets spoiled, making it worthless to hack.
3. **Secure platform :**
   i. Blockchain provides a digital platform which ensures security to all the intellectual property.
   ii. The digital certification and certification of ownership is some of the reason to trust this technology.
4. **Prevents payment scams :**
   i. Basic reason of why Blockchain provides powerful security is because if a coin is spent, it cannot be used for next payment.
   ii. This is the way it stops corruption.
   iii. Another reason of popularity of the technology is that if a transaction occurs between two parties, it has digital signature from both parties which prevents any fraud.

5. Transactions in minutes :

i. One can send or receive money or financial documents in minutes, thus it saves time.

ii. Traditional payment system directs every document to the clearing house for approval using third party, which causes down time in the transaction.

PART-2

Settlements.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.4. Discuss application of blockchain in financial software and systems with respect to settlements.

OR

Discuss application of blockchain with respect to settlements.

Answer

1. Settlement can be defined as the process of transferring of funds through a central agency, from payer to payee, through participation of their respective banks.
2. In the current financial system, some payments can take up to a week to finally settle.
3. The reason behind it is mainly the presence of multiple intermediaries in the system.
4. Present financial system is multi-layered, which means that every transaction has to go through at least a couple of intermediaries in order to settle.
5. These intermediaries can be front and back offices of a bank, third parties like currency exchangers in case of cross-border payments.
6. The presence of these intermediaries is a way to ensure security and authenticity in a centralized system, but it leads to long settlement time.
7. Using blockchain peer-to-peer (P2P) transactions are possible.
8. It eliminates the need of intermediaries as smart contracts will be able to manage transactions successfully.
9. As the "layers" of the system will be reduced, instant settlements of payments will be facilitated.

10. Blockchain payment systems can also be implemented to facilitate cross-border payments instantaneously.
11. In this way, blockchain facilitate instant settlements in financial services.

PART-3

KYC (Know Your Customer).

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.5. Discuss application of blockchain in financial software and systems with respect to KYC (Know Your Customer).

OR

Discuss application of blockchain with respect to KYC (Know Your Customer).

Answer

1. KYC (Know Your Customer) processes are the backbones of a financial institution's anti-money laundering efforts.
2. Regulatory compliance committee in India has enforced KYC for every bank.
3. However, KYC process takes long time for collecting and uploading the data individually in the system.
4. It is estimated that 80% of KYC efforts go on gathering information and processing.
5. Also, there is high possibility of false entry and duplication of the data.
6. Blockchain carries the key to eliminating inefficiencies and duplication in KYC processes.
7. Blockchain stores this data in a central repository and generates a reference number.
8. This reference number is shared among all banks and financial institutions in near real time.
9. Banks can access the same data for due diligence related to any customer's request for any other service in the same bank or with other banks.
10. This helps in removing the efforts of collecting and checking KYC information again and again.
11. Since the data are stored in encrypted form, security is maintained.

Que 4.6. Mention the benefits of blockchain in KYC process.

Answer

The benefit of a blockchain solution for KYC are :

1. **Data quality :** All data alterations are tracked and monitored in real-time.
2. **Lowered turnaround time :** Through KYC blockchain software solutions, financial institutions get direct access to the data which saves data gathering and processing time.
3. **Reduced manual labor :** KYC on blockchain eliminates paperwork from the process.
4. **Validation of information accuracy :** KYC blockchain systems enable transparency and immutability that, in turn, allows financial institutions to validate the trustworthiness of data present in the DLT platform.
5. **Real-time updated user data :** Every time a KYC transaction is performed, the information is shared within a distributed ledger. This blockchain technology KYC system enables other participating institutions to access real-time updated information.
6. **Distributed data collection :** The introduction of blockchain in KYC brings data on a decentralized network which can be accessed by parties after permission has been given to them.

Que 4.7. Is blockchain solutions the answer to KYC issues ?

Answer

1. Gathering information and processing it takes up a great amount of cost, time, and effort in the KYC process leaving very few resources available for monitoring and assessing user behavior.
2. By offering speedy access to up-to-date data, blockchain KYC solutions can lower the time needed for the laborious tasks.
3. This saved time can then be employed to find solutions to more complex KYC challenges.
4. However, blockchain cannot solve all the issues faced by KYC.
5. After the data is acquired, financial institutions still have to validate the information.
6. For this, Artificial Intelligence and cognitive processing-like technologies have to be employed for greater efficiencies.
7. In its present state, blockchain when used in combination with other technologies can showcase high potential to help institutions lower the cost and time linked with the KYC process.

PART-4

Capital Markets.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.8. Discuss application of blockchain in financial software and systems with respect to Capital Markets.

OR

Discuss application of blockchain with respect to Capital Markets.

Answer

1. In capital market trading, different parties like exchanges, central counter parties, Central Securities Depositories (CSDs), and brokers are involved.
2. They have to maintain their ledgers based on the exchanged messages between them.
3. For completing a transaction, the ledgers must be up-to-date and need intermediate beneficiaries for cash management.
4. This leads to delay for the final settlement and involves additional costs.
5. Blockchain plays a vital role in each and every stage of the trade.
6. Blockchain system facilitates for Know Your Customer (KYC) check and avoids multiple numbers of same checks again and again.
7. It provides transparency and verification of holdings and reduced credit exposure.
8. In the trade stage, it ensures the real-time transaction in more transparent and secure way and provides the automatic reporting.
9. In post-trade, blockchain removes the concept of central clearing needed for real-time cash transactions.
10. Blockchain also helps in the areas of Custody and Securities Servicing, Pre-Initial Public Offer (IPO) shares allotment, Loan Syndication, Bond Trading, Supply Chain Financing, etc.

Que 4.9. How investors in capital markets are benefitted from blockchain ?

Answer

1. Blockchain technology significantly reduces the barrier to issue new assets or financial products.

2. Due to blockchain the cost of issuance of new securities drops and the speed of issuance increases.
3. Using blockchain issuers will be able to tailor new instruments to the needs of each investor.
4. The enhanced ability to more exactly match investor desire for return will create a direct bond between capital seekers and investors.
5. Investors aim to mitigate risk while increasing their potential returns. One of the key drivers of risk is a lack of liquidity.
6. This is addressed by the programmable nature of digital assets and financial instruments which allows for lower transaction costs, increasing the potential liquidity of an asset.
7. Combined with the increased connectivity and efficiencies across capital markets, investors will see greater liquidity and a decreased cost of capital.
8. The transparent and distributed blockchain ledger will enable more robust insights into asset quality.

Que 4.10. Discuss blockchain in financial software and systems with respect to KYC and capital markets.

AKTU 2019-20, Marks 07

Answer

KYC : Refer Q. 4.5, Page 4–5P, Unit-4.

Capital Markets : Refer Q. 4.8, Page 4–7P, Unit-4.

PART-5

Insurance.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.11. Discuss application of blockchain in financial software and systems with respect to insurance sector.

OR

Discuss application of blockchain with respect to insurance sector.

Answer

1. Blockchain is transforming the insurance sector by bringing optimization in the business processes and sharing the information with better efficiency, security, and transparency.
2. Using the smart contracts it is shifting insurance system from manual to automated, thereby eliminating the traditional processing system.
3. Due to decentralization of blockchain, insurance sector will get streamlined in underwriting, payments, claims, and reinsurance processes.
4. In blockchain as the data is not stored at any centralized place it provides higher level of protection and cost saving.
5. Blockchain technology provides benefits to following insurance verticals :

A. Health insurance :

1. Health insurance is in direct connection with the medical institutions and patients using advanced data analytics.
2. All such processes and operations can be done through blockchain in an efficient, secure, immutable, and transparent manner.

B. Life insurance :

1. Blockchain can be used to connect various segments in life insurance, namely, insurance companies, insuree, beneficiaries, government, etc.
2. With the help of smart contract technology, insurance companies can automate the whole processing.
3. They can operate smoothly with better efficiency, reduced time and money on operations.

C. Auto insurance :

1. Auto insurance industry can be benefitted in terms of reducing the level of paperwork and making underwriting easier.
2. Blockchain can help in faster resolution of accident claims.

D. Travel insurance :

1. Travel insurance could also be a vertical which use blockchain to protect the traveler in case of flight delay.
2. Operational efficiency in this vertical of insurance would increase international coverage.

Que 4.12. How blockchain technology can be used for claim settlement in insurance sector ?

Answer

1. Settlement of claims is the biggest challenge in insurance sector.
2. These claims settlement can become simpler with the help of custom smart contract.
3. This smart contract takes various parameters of insurance policy and processes the operation automatically through trustless identity verification mode.
4. In distributed ledger system, smart contract processes the funds for claims settlement.
5. Also, controlling is not done exclusively by either policy holder or insurance company.
6. Funds can be directed to the genuine party automatically after the verification using the digital contract.
7. Smart contracts can settle the insurance claims in a faster and speedy manner without the requirement of any paper documents, photocopies, and complicated web portals.

Que 4.13. How blockchain technology can be used for underwriting in insurance sector ?

Answer

1. The process of underwriting involves calculation of the coverage amount on the policy for policy holder and the annual premium charge.
2. It is very time-consuming process and need high level of data analysis.
3. With the help of blockchain, data analysis can be done automatically using its tools for analysis.
4. It can help the underwriters to reduce the risk liability and automate insurance policy price determination process.
5. This results in cost-efficient model of insurance and better experience for the customer.
6. Transparency in the underwriting process helps in building trust between customers and insurance companies.

Que 4.14. How blockchain technology can be used for reinsurance in insurance sector ?

Answer

1. Reinsurance occurs when multiple insurance companies share risk by purchasing insurance policies from other insurers to limit their own total loss in case of disaster.
2. It is described as "insurance of insurance companies."

3. Premiums paid by the insured are typically shared by all of the insurance companies involved.
4. Blockchain can be used for reinsurance purpose, as it helps in automating all calculations, balances, and reconciliation.
5. This technology can track the funds available for settlement of claims.
6. It can help the insurance companies in assessing financial risks and improving upon the reinsurance strategy in totality.
7. Also, it can simultaneously benefit the insurance companies in terms of minimizing cost and time.

PART-6

Blockchain in Trade / Supply Chain.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.15. Discuss application of blockchain technology in trade/ supply chain.

Answer

1. With manufacturing process taking place across the globe and the need of transparency between suppliers and supply chains are must.
2. Supply chain is integrated with logistics industry, freight, trucking, shipping, and other modes of transportation.
3. There is a strong need to streamline and make its system transparent.
4. Blockchain is perfectly suitable for supply chain management, with real-time tracking of goods.
5. It is especially appealing to companies having multiple supply chains.
6. With the help of BCT, all inefficient and incompetent supply chain will be eliminated.
7. Businesses are getting transformed with the help of blockchain-based supply chain solutions which offer end-to-end decentralized processes through DLT and digital public ledger.

Que 4.16. What are the problems associated with traditional supply chain management ? How these problems are overcome by decentralization of supply chain management ?

Answer

A. Problems associated with traditional supply chain management :

1. The existing supply chain management system is outdated.
2. It is unable to match the pace of changes happening across the globe.
3. The speed of existing supply chain is extremely slow.
4. Following are the major problems which have been face by the industry in supply chain management :
   i. Problem of transparency related to supply of goods from one place to other.
   ii. No surety of goods genuineness as "real" and "certified".
   iii. Identifying the true value of transaction.
   iv. Expensive and inefficient systems.
5. Risk of counterfeiting and fraud, lack of trust, unreliability, and insecurity in data are also problems which have been observed.

B. Decentralization of supply chain management :

1. There are numerous benefits of decentralization of supply chain management.
2. Major benefits are bringing traceability and transparency into the system.
3. Real-time tracking of data is possible which helps to locate the items and their conditions, resulting in reduction of human error.
4. There would be a change in the speed of transactions and efficiency level will also be enhanced.
5. Since blockchain is trustless chain therefore it provides more security and eliminates the chances of fraud and errors.
6. Other benefits of decentralized supply chain are improved inventory management, lower courier costs, less paperwork, and faster issue identification.

PART-7

Provenance of Goods.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.17. **Discuss blockchain in trade/supply chain with respect to provenance of goods.**

OR

Discuss application of blockchain technology in provenance of goods.

Answer

1. In the supply chain industry, "provenance of goods" refers to the ability to identify the origin location of a product.
2. Tracking provenance throughout supply chain journey is crucial to ensuring product authenticity.
3. The complexity of supply chain has grown significantly due to the expansion of globalization in the 21st century.
4. Due to the rise of globalization, it is now extremely challenging to ensure the provenance (origin) of goods.
5. For big multinational companies, it is difficult to keep track of all transactions and records.
6. This creates questions of company's reputation and reliability.
7. Blockchain-based supply chain solutions provide answers to such issues.
8. It makes provenance tracking possible with easy access to product information using embedded sensors and RFID tags.
9. Blockchain can document provenance of goods to a single shared ledger, which provides complete data visibility and a single source of truth.
10. Because transactions are always time-stamped and up to date, companies can query a product's status and origin at any point in time.
11. This helps to combat issues like counterfeit goods.

PART-8

Visibility.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.18. **What does visibility in supply chain mean ? Explain how blockchain helps in supply chain visibility (SCV) ?**

Answer

1. Supply Chain Visibility (SCV) is the ability to track individual components, sub-assemblies and final products as they travel from supplier to manufacturer to consumer.
2. This data helps companies maneuver around inventory shortages, avoid bottlenecks, meet compliance directives and track products through to delivery.

Blockchain and supply chain visibility (SCV) :

1. A significant motivation for companies investing in blockchain for SCV is increasing consumer demand for information about product origins.
2. The internet has enabled information sharing among customers, and blockchain offers the potential for the kind of visibility that can be corroborated by the system.
3. The level and quality of visible data that blockchain might offer could increase service quality to consumers, creating greater value.
4. Blockchain is demonstrated as an enabler of visibility in supply chains.
5. Blockchain potentially offers the upstream visibility in supply chains.
6. This is largely a result of the decentralised, consensus-based trust mechanism underpinning the technology.
7. The visibility provided by blockchain solutions aids decision-making by enabling stakeholders to see timely, accurate, and reliable information.
8. Blockchain integrated with product labelling solutions offers a level of visibility that was previously not possible.

PART-9

Trade / Supply Chain Finance.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.19. What do you understand by supply chain finance ? Explain the role of blockchain in supply chain finance.

Answer

1. Supply Chain Financing (SCF) is a financial management solution that benefits both suppliers and buyers to increase working capital.

2. Buyers use trade credit as cash flow management to maintain business financial liquidity.
3. From the supplier's point of view, trade credit allows suppliers to set favorable payment dates without disrupting their cash flow.
4. SCF main goals is to optimize financial flows between various levels of business processes through solutions offered by financial institutions, technology providers and other related parties.

Role of blockchain in supply chain finance :

1. Blockchain promises a supply chain data storage method with secure, irreversible and transparent access.
2. Blockchain allows decentralization of data so that no party can claim ownership of the supply chain data as their own.
3. Blockchain creates an immutable audit trail for all transactions. This has the potential to increase trust between the relevant parties.
4. Blockchain can be used to achieve a single source of truth for activities such as invoice receipt and approval.
5. Smart contracts can be used to automate transactions.
6. Blockchain provides the ability to access a wider range of funding providers than a traditional supply chain finance solution.
7. In supply chain finance blockchain could be a useful tool to streamline today's often manual and costly processes by catalyzing digitization.
8. In supply chain finance blockchain could increase the speed of transactions as well as their security, facilitating financial flows between counterparties.
9. Blockchain provides solutions to SCF automation problems such as Know Your Customer (KYC), accounting, and transaction settlement.

Que 4.20. What are the advantages and limitations of blockchain in supply chain finance ?

Answer

Advantages of blockchain in supply chain finance include :

1. Decentralized and secure databases.
2. Anonymous and inexpensive transactions.
3. Smart contracts and product traceability.

Limitations of blockchain in supply chain finance :

1. Validation of successful adoption of blockchain technology.
2. Integration with existing IT systems.
3. Scalability.
4. Lack of computing power.
5. Regulatory and legal governance.

PART-10

Invoice Management.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.21. What is invoice management/processing ? Explain problems associated with manual invoice processing. Describe the role of blockchain in invoice management.

Answer

1. Invoice management (invoice processing) is the method by which companies track and pay supplier invoices.
2. The process involves receiving an invoice from a third party, validating it as legitimate, paying the supplier, and noting the payment in company records.

Problems associated with manual invoice processing :

1. **Lack of Process Transparency :** The status of manual invoice processing is opaque. The status of the entire process and the duration it will take to mature often lacks transparency.
2. **Hidden Costs :** Hidden costs often linger in manual invoice processing, where one invoice is handled several times, even before an approval decision is made.
3. **High Error Rates :** Manual invoicing is vulnerable to numerous errors with accuracy plainly in the hands of the invoice processing handlers. This can give rise to costly problems.
4. **Unnecessarily Complex Processing :** During the early stages, a business might handle invoices as they arrive. However, as a company grows, its processes become unnecessarily complex.

Role of blockchain in invoice processing :

1. Blockchain technology can streamline invoice processing, save costs, minimize settlement times, and improve the business agility.
2. In an environment where businesses experience errors and fraud attempts concerning invoice processing, guaranteeing trust becomes obligatory.
3. For this purpose, blockchain offers an invoicing solution that brings trust to every step of the invoicing process.
4. The solution leverages blockchain technology to gather and process data in a faster and effective manner.

5. The invoice solution ensures that invoices are from legitimate suppliers and for expected and genuine orders.
6. It also inhibits fake and erroneous typing and double spending of invoices.
7. With this invoice solution, businesses can confirm and authorize every step of the invoicing process, match invoice data with purchase order data, from the reception of an invoice to the authorization of payment.

Que 4.22. Discuss blockchain in trade/supply chain with respect to trade/supply chain finance, and invoice management.

AKTU 2019-20, Marks 07

Answer

Trade/Supply Chain Finance : Refer Q. 4.19, Page 4–14P, Unit-4.

Invoice Management : Refer Q. 4.21, Page 4–16P, Unit-4.

PART-11

Invoice Discounting.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.23. What is invoice discounting ? Describe the role of blockchain in invoice discounting.

Answer

1. Invoice discounting is a funding option provided to businesses that are issued by finance companies.
2. Under the invoice discounting process, the business uses the unpaid invoices of its customers as collateral to access advances on cash funds that improve the working capital and cash flow position of their business.
3. Invoice discounting significantly improves the cash flow and growth of a business.
4. This is because the business obtains fast funding as immediate cash rather than having to wait the usual 30-60 days.
5. This improved cash flow is critical for businesses as businesses can then invest in growth.
6. The two major downsides of invoice discounting are the cost and the reduced funding capacity.

Role of blockchain in invoice discounting :

1. Blockchain adoption enhances the overall invoice discounting process.
2. The trust and security mechanisms of the blockchain allow for the elimination of on-site audits of receivables and debtors.
3. Adoption of blockchain will also allow for a fast and cheaper value transfer, in particular for cross-border payments.
4. Using blockchain, debtor's verification of the invoice validity, reduces significantly the risk of dispute and non-payment of that invoice.
5. Using blockchain the record of debtor invoices would be visible to his suppliers and thus it could be used to influence the payment terms and the offered contract prices.
6. This immutable debtor's verification could also potentially eliminate the risk of invoice fraud.
7. The blockchain provides a complete and transparent record of a supplier's completed transactions and their success rate on which to ground funding and recourse decisions.
8. The blockchain provides a complete and transparent record of debtor's payment history that can be used to evaluate decisions about credit limits and debtor limits.

Que 4.24. What is the concept of executive accounting ? Does blockchain support the same ? **AKTU 2021-22, Marks 07**

Answer

1. Executive accounting is designed for service type businesses that require a sophisticated yet simple to use accounting system.
2. Executive accounting contains many advanced features such as three styles of invoicing, multi-currency capabilities, multiple bank account capabilities and other powerful features.
3. Executive accounting is a single-user system that can be upgraded to an unlimited number of users.
4. Executive accounting is designed exclusively for a business that offers services to the people.
5. There is no strict upper limit on services and a business can manage any service through the executive accounting.
6. Yes, blockchain support executive accounting.
7. Blockchain has algorithms that are specially meant to handle executive accounting.
8. In fact, it cut down many problems that are associated with executive accounting.

5 UNIT

Use Case 3

CONTENTS

PART-1

Blockchain for Government.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.1. How governments can harness the potential of blockchain ?

OR

What are the benefits of blockchain in government sector ?

Answer

1. Government adoption of blockchain can be viewed from regulatory, consumer, and developer perspectives.
2. As a governing body, a state may wish to monitor how blockchains are used.
3. As a user of applications, governments may use blockchains to improve processes.
4. A blockchain-based government can protect data, streamline processes, and reduce fraud, waste, and abuse while simultaneously increasing trust and accountability.
5. On a blockchain-based government model, individuals, businesses, and governments share resources over a secured distributed ledger.
6. This structure eliminates a single point of failure and inherently protects sensitive data.
7. A blockchain-based government enables the following advantages :
   i. Secure storage of government, citizen, and business data.
   ii. Reduction of labour-intensive processes.
   iii. Reduction of excessive costs associated with managing accountability.
   iv. Reduced potential for corruption and abuse.
   v. Increased trust in government and online civil systems.
8. The distributed ledger format can be leveraged to support an array of government applications, including digital identity, land records, public distribution system, social welfare systems, etc.

PART-2

Digital Identity.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.2. What are the problems associated with existing digital identity management system ? How blockchain helps in overcoming those problems ?

OR

Discuss blockchain for government with respect to digital identity.

Answer

A. Problems in the existing identity management system :

1. Due to the lack of common platform of digital identity management, individuals every time need to verify and authenticate their identities at all places.
2. Existing digital identity management system are based on biometric identification, which is password-based and stored in an unsecured system.
3. These unsecured systems are highly prone to data theft and hacking.
4. The centralized systems are identity centric and people get one social security number containing all details.
5. Misuse of this information may result in disastrous acts such as frauds in banking, purchasing, fake identity creation, etc.
6. Moreover, companies also sell the personal information for commercial purposes and generate revenues.

B. Role of blockchain in overcoming existing identity management problems :

1. Blockchains decentralized mechanism of identity management helps resolves all existing issues by providing a new model of identity management using BCT.
2. Cryptography is used to separate data from the identity of individuals for better security.

3. With the help of separate data management companies can possess and obtain data which is of their use while preserving the individuals' privacy.
4. This creates a win-win situation for government, individuals', and companies.

Que 5.3. Give some use cases for blockchain application in identity management.

Answer

Following are some use cases for blockchain application in identity management :

1. **Data collection and its analysis :**
   i. Accuracy of data is of utmost importance for any country, state, or company.
   ii. The real-time data storage using blockchain can be analyzed and improved in numerous industry practices.
   iii. This will also bring faith in terms of security of data.
   iv. Analysis and analytics can be applied in a better manner for the research and development, decision-making, and further betterment of the society.
2. **E-Residency :**
   i. The identity management done using BCT can help individuals to vote, file their income tax returns, perform various other processes in a more efficient and secure manner.
   ii. It can also help virtual residency authentication due to government verified ID's maintained using DLT.
   iii. All the government transactions can be moved to blockchain using e-residency identity management in order to streamline all interactions among individuals and government.
3. **Immigration and identity :**
   i. Digital identity card can be linked to the details on the blockchain, and this will act as a temporary ID card when entering in new country.
   ii. This will help immigration services to get smoother.
   iii. Travelers can also link their debit/credit cards and can monitor their account activity.
4. **Self-sovereign identities :**
   i. The individuals can have a better life with the secure, transparent, reliable, and accurate identity management system provided by BCT.

ii. This will eliminate the involvement of third parties for digital/manual identity management; eliminate identity sprawl and identity theft.

PART-3

Land Records.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.4. Discuss blockchain for government with respect to land records.

Answer

1. A number of governments around the world suffer from bad land registry records.
2. There are hundreds of years of land records, which make keeping track of land ownership difficult.
3. Factors contributing to the growing problems faced by land registry officials are :
   i. Discrepancies with the paperwork.
   ii. Forged documents and counterfeit titles.
   iii. Occasional loss of all documents.
4. For developing countries bad land registry records, government corruption, the use of paper-only systems, and natural disasters all contribute to the growing problems faced by land registry officials.
5. Blockchain-based technology is a cost-effective solution to these problems.
6. The transparent nature of blockchain makes it an effective technology for use in public records systems, title registry, and land right management.
7. Blockchain is more efficient, reliable and cost-effective than current models in use.
8. It provides immutable records, secure access and storage, user friendliness, and operational simplicity.
9. Blockchain technology allows users to easily secure the deeds of transactions by entering the details and uploading them on distributed document storage with immutable logs.

PART-4

Other Kinds of Record Keeping between Government Entities.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.5. What type of records can be kept in a blockchain ? Is there any restriction on same ? **AKTU 2021-22, Marks 07**

Answer

1. Following are two types of records that can be kept in the blockchain :
   i. Transactional Records
   ii. Block Records
2. Both these records can be easily accessed.
3. It is also possible to integrate them without following the complex algorithms.

Restriction for keeping records :

1. No, it is not possible to give restriction for keeping records in the blockchain approach.
2. We can put any type of data on a blockchain such as bank records, medical records, images, documents, Instagram messages, etc.
3. However, blockchains are not designed to store large data.
4. It is recommended to not keep large dataset in blockchain.

Que 5.6. Explain government adoption of blockchain in health sector/healthcare.

Answer

1. Digitization of health records is a significant task in the public health sector, which is huge, complex and associated with ethical issues.
2. Medical records are scattered and erroneous, with inconsistent data handling processes.
3. Sometimes, hospitals and clinics are forced to work with incorrect or incomplete patient records.
4. Blockchain technology can help public health by creating a secure and flexible ecosystem for exchanging patient's electronic health records.

5. Blockchains in healthcare can be envisaged in five primary areas :
   i. Managing electronic medical record (EMR) data.
   ii. Protection of healthcare data.
   iii. Personal health record data management.
   iv. Point-of-care genomics management.
   v. Electronics health records data management.
6. This technology could also make the space more transparent by creating a basis for critical drugs, blood, organs, etc.
7. In addition, by putting all medical licenses on a blockchain, fraudulent medical practitioners, druggists, chemists be prevented from practicing and selling drugs.

Que 5.7. Explain government adoption of blockchain in energy resources management in smart city.

Answer

1. By 2030, 60% of mankind will be city-inhabitants.
2. Populace thick urban communities are enormous and generate a comparable extent of worldwide carbon discharges.
3. Due to this urban communities are major contributor of environmental pollution.
4. To balance this there is a need to develop distributed energy resources to supports urban communities and incorporate more sustainable power sources.
5. The distributed energy resources reduce variable costs of retail payment processing and accounting.
6. They improve greater transparency into billing and greater customer choice of energy supply.

Role of blockchain in energy resources management in smart city :

1. Blockchain could improve retail power by utilizing digital currencies for bill repayment.
2. Blockchain could lessen the variable expenses of installment handling and bookkeeping.
3. Blockchain could improve client's relationship by empowering more prominent straightforwardness into vitality charges and bill segments.
4. Blockchain could impart clients with the capacity to enter and leave vitality contracts any time.
5. Blockchain could help utility make more prominent decision and build straightforwardness into vitality supply.

Que 5.8. **Give the application of blockchain in voting.**

Answer

1. A democratic country depends on voter consensus to elect officials.
2. Unfortunately, the voting systems at present are inefficient and manipulation prone.
3. Blockchain can improve the system to identify the rationality of the individual citizens.
4. BCT uses decentralized ledger to store voting data. The result is not managed by a centralized authority.
5. This eliminates the menace of voting result manipulations.
6. Voters can cast votes the same way they initiate other secure transactions.
7. They can also validate that their votes were cast or not.
8. Potential solutions are currently working to blend secure digital identity management, anonymous vote-casting, individualized ballot processes, and ballot casting confirmation verifiable by the voter.

Que 5.9. **Give the application of blockchain in notary services.**

Answer

1. Notary services may be transformed using blockchain.
2. These administrative time stamps actually validate an action that happens in a person's life including :
   i. birth and death details,
   ii. documentation for new identity,
   iii. receiving educational certificate,
   iv. transfer of ownership titles.
3. As of now, many of these practices are done on secluded databases or through brick-and-mortar offices, which are generally prone to errors.
4. Due to the encryption of the data and information stored in a blockchain, all these recorded data will be stored safely.
5. These recorded data will be only observable to the owner or the permitted parties.

Que 5.10. **Give the application of blockchain in energy sector.**

Answer

1. Blockchain in the energy sector can involve multiple aspects, ranging from energy trading to management of IoT devices and energy resources management.

2. Energy trading, especially renewable energy trading and management, is one of the main areas found in current blockchain projects.
3. The projects utilize the cryptocurrency side of the blockchain technology to build the trading system.
4. The energy is first converted into tradable values and sent to the blockchain network.
5. The real-time trading prices are then calculated according to the exchange cost and demand.
6. When the transactions are finalized, energy can be exchanged locally without having to be transmitted to a central location.
7. These methods have been shown to greatly reduce the management and trading cost.
8. The adoption of blockchain could potentially reduce the cost for any financial transaction in the energy sector and remove the need for a trusted single party.

Que 5.11. Discuss blockchain for government with respect to digital identity, land records and other kinds of record keeping between government entities. Is it safe ? Justify your answer.

AKTU 2019-20, Marks 07

Answer

Refer Q. 5.2, Page 5–3P, Q. 5.4, Page 5–5P, Q.5.5 to Q. 5.9; Unit-5.

PART-5

Public Distribution System.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.12. What do you understand by Public Distribution System (PDS) ? Give the process flow for PDS.

Answer

Public Distribution System (PDS) :

1. Public distribution system is a government-sponsored chain of shops entrusted with the work of distributing basic food and non-food commodities to the needy sections of the society at very cheap prices.

2. Subsidised ration distribution takes place each month to the ration card holders under public distribution system (PDS).
3. PDS involves procurement from the farmers till distribution to ration card beneficiaries.
4. PDS comprises different entities such as central and state agencies, millers, transporters, shop owners and the beneficiaries.
5. A major feature of the PDS is the general lack of accountability down the entire supply chain.
6. Blockchain technology can be useful in managing supply chain effectively using distributed ledger technology.
7. Entire supply chain starting from procurement till disbursement can be part of blockchain.
8. Blockchain provides an effective way to combat corruption, exclusion errors of targeted beneficiaries, leakage of PDS food grains and is cost-effective.

Process flow for PDS :

1. Farmer cultivates the food grains which are then procured by the government under minimum support price (MSP).
2. Millers identified by the government collect food grains initially and then hull it to be returned to government.
3. It is then moved to state godowns to be distributed to various block godowns.
4. From the block godowns these commodities gets distributed to various fair price shops (FPS) for beneficiary distribution.

Que 5.13. Explain the role of blockchain in PDS.

Answer

1. The blockchain technology implemented in Public Distribution System advances the management structure of the process by using standard procedures and entry systems.
2. It keeps track and create secured and reliable architecture with permissions to all nodes to transact and review the updates.
3. Use of blockchain can remove delay in payment to the farmers based on procurement done by the miller. However, unless the transaction is approved by the farmer, miller cannot register the quantity collected.
4. This makes each transaction Non-repudiation.
5. Since calculation and payment must happen based on this initial data, data provenance (recording history of data) can be sealed using blockchain technology.

6. The decentralized distributed ledger makes all the stake holders refer to their local copy of the ledger to make decisions and act accordingly.
7. Certain activities such as payment to farmers can be done without waiting for the miller to hull them.
8. Since the procurement season is defined for each commodity, payment can start immediately without waiting for the other actors to complete their process.
9. This makes each transaction as non-time critical and thus eligible to be part of blockchain technology.

PART-6

Social Welfare Systems.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.14. Explain the role of blockchain in social welfare systems. Give an example of blockchain based social welfare system.

Answer

1. Government in its several welfare schemes get benefited by adopting blockchain technology.
2. It can improve its delivery services, eliminate the middleman, and prevent tax fraud cases.
3. Most of the government functions and blockchain technology are essentially the same.
4. Government launches welfare schemes that can be considered as a network involving several stakeholders.
5. Similarly blockchain maintains a distributed ledger.

Example : GovCoin blockchain-based system :

1. The UK government has teamed up with the company GovCoin in order to develop a blockchain for welfare payments.
2. GovCoin has developed specialized blockchain systems for seamless welfare transactions.
3. The welfare distribution mechanism with the assistance of blockchain systems is fairly straightforward.

4. The GovCoin-powered mobile application allows individuals on welfare support to use transferred monetary amounts to cover grocery, rent, maintenance and other daily expenses.
5. Additionally, the distributed ledger can also monitor where exactly the money handed out is being spent.

PART-7

Blockchain Cryptography.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.15. Explain how blockchain uses cryptography ?

Answer

1. Blockchain uses cryptography to derive most of its properties.
2. Each participant on the network is categorized as a node and has a pair of public and private keys.
3. The public key acts as a public address of the node, and private key is used for authentication.
4. When a transaction is created, it will have the public key of the sender, public key of the receiver, and the transaction message.
5. Then the transaction is cryptographically signed using the private key and transmitted over the blockchain network.
6. This completes one transaction.
7. A block is a collection of many such valid transactions which are sent over the network within a specified time limit.
8. Validation of transaction ensures that the transaction is legitimate and generated from a valid and connected node.

Que 5.16. How cryptography provides trustless environment in blockchain network ?

Answer

1. Cryptography is method for protecting information through the use of encrypting and decrypting the data.
2. Blockchains mainly make use of two types of cryptographic algorithms :
   i. Hash functions

ii. Asymmetric-key algorithms

3. Hashing is mainly used in linking of blocks and in consensus algorithms.
4. Asymmetric key cryptography is driving the blockchain applications for identifying the contributors of the network and proof of their ownership.
5. So cryptography is an excellent way for replacing the third parties and provides trustless environment in blockchain network.

PART-8

Privacy on Blockchain.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.17. Discuss privacy issues of blockchain technology.

Answer

1. Different blockchain applications present different and unique privacy challenges.
2. Following three general categories currently concern legal privacy experts :
   i. The first involves the necessary bridge between the physical and cyberspace limits.
   ii. The second involves sensitive information that is actually stored on the blockchain.
   iii. The third involves the very existence of blockchains.
3. Each of these options offers tradeoffs between security, privacy, speed, and functionality.
4. Different applications require different blockchain networks to work according to each application's specific requirements.

A. Physical-cyberspace boundary :

1. The "physical cyberspace boundary" refers to the concept that when a person interacts in cyberspace, he do so through an "online identifier."
2. A connection between person and his online identifier needs to be established to participate in a transaction.
3. At present, this is achieved through username and passwords, sometimes with the expansion of multifaceted verification techniques.

4. In the near future, biometric identifiers will be used as the methods for intersecting the physical-cyberspace boundary.
5. For a person to log into a network, the network must have a copy of the login credentials coupled with the online identifier of that person.
6. These credentials would be stored in a blockchain network on all the nodes with which you want to interact, some of which can be more easily compromised.
7. This is particularly important when it comes to biometric identifiers, which are not easily changed once they are compromised by identity thieves.

B. Information storage and inference :

1. Some of the data which will be stored on blockchains will be particularly sensitive.
2. While any sensitive information stored on the blockchain will be encrypted, hackers may target those specific nodes that can be more easily compromised to access the encrypted information.
3. Privacy risks can be mitigated by operating in closed networks.
4. However, there are benefits to open networks that require at least some blockchains containing sensitive information to operate in networks that are less than completely closed.
5. Another concern about open networks is that, although the information itself is encrypted, sensitive information can be gathered from the fact that transactions took place.
6. Also it is unclear who might be legally liable in the event, the information is accessed and harm results to the owner of the information.

C. Nature of the blockchain (Eternal Records) :

1. As we create more data and as these data are cataloged and easily searched, the data becomes eternal and visible to the general public.
2. The technology of blockchain is likely to accelerate this trend.
3. As the types of transactions stored in blockchains increase, eternal records of each transaction will increase.
4. You will have no control over where this information is stored or how it is used and no way to delete it.
5. There are numerous concerns about privacy involved in these eternal records.
6. For example, the simple fact that these records exist could pose problems for anyone who does not want to have a complete record of all their transactions for all time.
7. In addition, there is currently no clear agreement on who "owns" the information in these records as a legal matter.

8. In the absence of clear ownership rules, public bodies and private citizens may also have access to these data.

PART-9

Security on Blockchain.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.18. What are the key principles in blockchain that are helpful in eliminating the security threats that needs to be followed ?

AKTU 2020-21, 2021-22; Marks 07

Answer

The fundamental principles in blockchain that must be followed to eliminate security threats are :

1. **Auditing :**
   - i. An audit involves an assessment that recorded transactions are supported by evidence that is relevant, reliable, objective, accurate, and verifiable.
   - ii. The acceptance of a transaction into a reliable blockchain may constitute sufficient appropriate audit evidence for certain financial statement assertions such as the occurrence of the transaction.
   - iii. For example, in a Bitcoin transaction for a product, the transfer of Bitcoin is recorded on the blockchain.
   - iv. However, the auditor may or may not be able to determine the product that was delivered by solely evaluating information on the Bitcoin blockchain.
2. **Securing applications :**
   - i. Blockchain technology produces a structure of data with inherent security qualities.
   - ii. It's based on principles of cryptography, decentralization and consensus, which ensure trust in transactions.
3. **Securing testing and similar approaches :**
   - i. To guarantee trust, testers must ensure that all the components of a blockchain are working perfectly and that all applications are interacting with it in a trusted manner.

ii. Some of the core tests that should be run include functional, performance, API, node testing, and other specialized tests.

4. **Database security :**
   i. The records on a blockchain are secured through cryptography.
   ii. Network participants have their own private keys that are assigned to the transactions they make and act as a personal digital signature.
5. **Continuity planning :**
   i. Business Continuity Planning (BCP) is the process involved in creating a system of prevention and recovery from potential threats to a company.
   ii. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster.
6. **Digital workforce training :**
   i. The digital workforce is use to describe a variety of robotic and automated solutions for driving productivity efficiencies in the workplace.
   ii. Digital workforce training helps in making blockchain security more efficient.

Que 5.19. Explain the use of cryptography Hash function/Hashing in blockchain network.

Answer

1. Data in blockchain are cryptographically hashed.
2. Hash function is a one-way function which means that hash can be generated from the plain text, but deriving the plain text from the hash is extremely difficult.
3. Thus, tracking of information and unauthorized tampering of data cannot be done.
4. Hash value denotes a numeric value of a fixed length that will be generated using cryptographic hash algorithm.
5. It identifies the data uniquely and blockchain state is represented by hash function SHA256.
6. Hashing generates a fixed length hash value that uniquely represents the contents of an arbitrary length string.
7. Identical strings are generating the same hash value.
8. Retrieving the original string from hashed values is not possible, since it is a one-way function.
9. Genesis block hash is calculated using initial transactions.
10. Index of the block, previous block hash, timestamp, block data, and nonce are used for calculating the hash value of the consecutive blocks.

Que 5.20. Explain the use of cryptographic digital signature in blockchain network.

Answer

1. Asymmetric cryptographic mechanism is used to verify the credibility of the transaction in a deceitful environment.
2. Digital signature works on the principle of asymmetric cryptography.
3. Each transaction member is provided with a private and public key.
4. A private key is stored confidentially because it is used for signing negotiations.
5. The transactions that are signed are transmitted across the distributed network and the public keys are used for their accessibility.
6. In digital signature there are two levels involved: verification phase and signing.
7. During the phase of signing, the encryption of the data is carried out using the private key by the sender.
8. Encrypted result and native data are delivered, which are sent to the receiver of the transaction.
9. For the validation of the received value by the receiver, the public key is used and the data are checked if it has been meddled.
10. Elliptic Curve Digital Signature Algorithm (ECDSA) is used to implement digital signature mechanism in blockchains.
11. Fig. 5.20.1 shows the process of assignment of the digital signature.

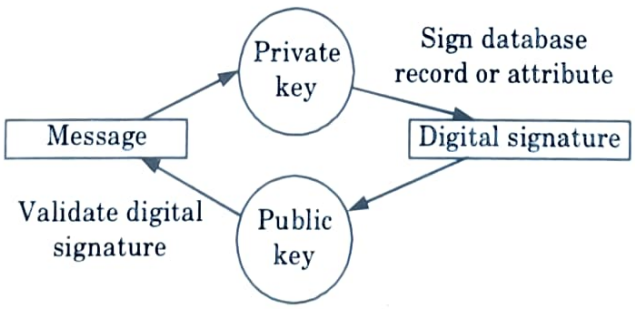

Fig. 5.20.1. Digital signature assignment process.

12. The private key is used to sign and record various messages, while the digital signature is validated using the public key.

Que 5.21. What is Elliptic Curve Cryptography (ECC) ?

Answer

1. Elliptic Curve Cryptography (ECC) is a key-based technique for encrypting data.

2. ECC focuses on pairs of public and private keys for decryption and encryption in blockchain network.
3. ECC is a powerful cryptography approach.
4. It generates security between key pairs for public key encryption by using the mathematics of elliptic curves.
5. ECC has gradually been growing in popularity due to its smaller key size and ability to maintain security.
6. ECC bases its approach to public key cryptographic systems on how elliptic curves are structured algebraically over finite fields.
7. ECC creates keys that are more difficult, mathematically, to crack.
8. For this reason, ECC is considered to be the next generation implementation of public key cryptography in blockchain network.

Que 5.22. What is SHA-256 hashing algorithm ?

Answer

1. Secure Hashing Algorithm (SHA)-256 is the hash function and mining algorithm of the Bitcoin protocol.
2. It refers to the cryptographic hash function that outputs a 256 bits long value.
3. It moderates the creation and management of addresses, and is also used for transaction verification.
4. It is a Secure Hashing Algorithm, commonly used for digital signatures and authentication.
5. SHA-256 is the most famous of all cryptographic hash functions because it's used extensively in blockchain technology.
6. SHA-256 Hashing algorithm was developed by the National Security Agency (NSA) in 2001.
7. The algorithm is a variant of the SHA-2 (Secure Hash Algorithm 2).
8. SHA-256 is also used in popular encryption protocols such as SSL, TLS, SSH and open source operating systems such as Unix/Linux.
9. The hash algorithm is extremely secure and its workings aren't known in the public domain.
10. It is use to protect sensitive information, due to its ability to verify a content of data without revealing it.
11. It is also utilized for password verification, since it does not require the storage of exact passwords.
12. Due to the astronomical number of potential combinations a brute force attack is extremely unlikely to succeed.

Que 5.23. What is Merkle Tree and Merkle Root ?

Answer

Merkle Tree :

1. A Merkle tree is a data structure that is used in computer science applications.
2. In bitcoin and other cryptocurrencies, they're used to encrypt blockchain data more efficiently and securely.
3. It's a mathematical data structure made up of hashes of various data blocks that summarize all the transactions in a block.
4. It also enables quick and secure content verification across big datasets and verifies the consistency and content of the data.

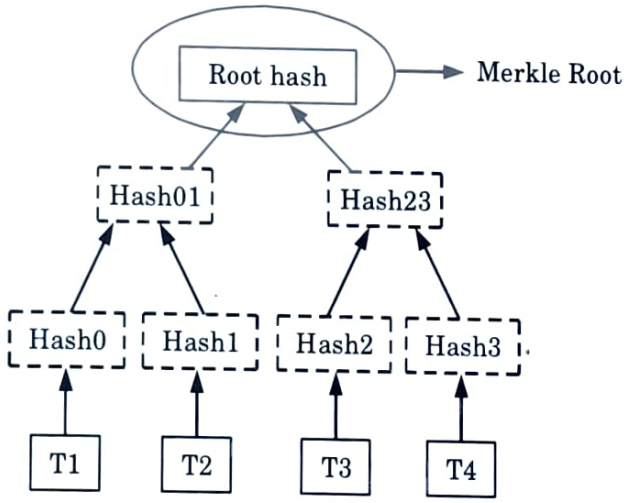

Fig. 5.23.1. Merkle tree.

Merkle Root :

1. Merkle root is the name of the root node in the tree.
2. A Merkle root is a simple mathematical method for confirming the facts on a Merkle tree.
3. They're used in cryptocurrency to ensure that data blocks sent through a peer-to-peer network are whole, undamaged, and unaltered.
4. They play a very crucial role in the computation required to keep cryptocurrencies like Bitcoin and Ether running.

Que 5.24. Explain the working of Merkle Trees.

Answer

1. A Merkle tree totals all transactions in a block and generates a digital fingerprint of the entire set of operations, allowing the user to verify whether it includes a transaction in the block.

2. Merkle trees are made by hashing pairs of nodes repeatedly until only one hash remains.
3. This hash is known as the Merkle Root or the Root Hash.
4. They're built from the bottom, using Transaction IDs, which are hashes of individual transactions.
5. Each non-leaf node is a hash of its previous hash, and every leaf node is a hash of transactional data.

Example : Consider the following scenario :

1. A, B, C, and D are four transactions, all executed on the same block.
2. Each transaction is then hashed. After hashing we get the following :

   Hash A Hash B Hash C Hash D
3. The hashes are paired together, resulting in Hash AB and Hash CD.
4. The Merkle Root is formed by combining these two hashes i.e., Hash ABCD.

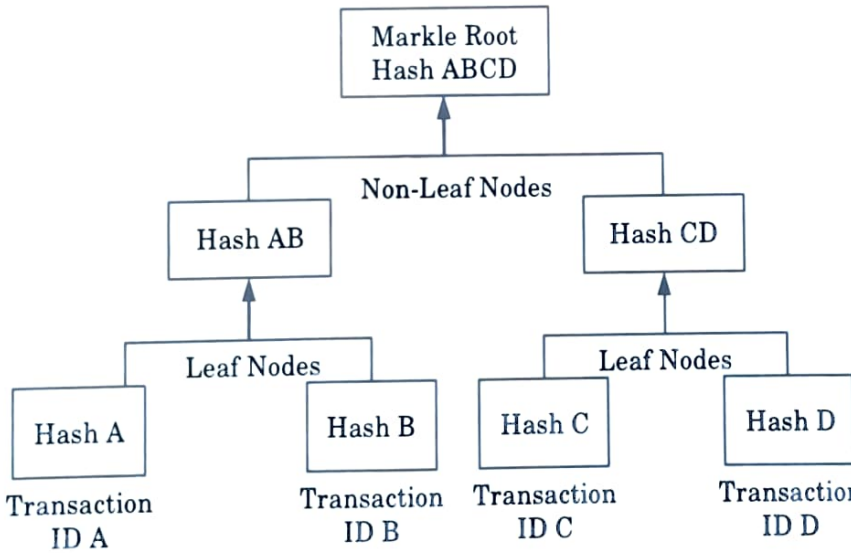

Fig. 5.24.1. Working of merkle tree.

Que 5.25. **What is the application of merkle trees ? Write use of merkle trees in blockchains ?** **AKTU 2021-22, Marks 07**

Answer

Application of Merkle trees :

1. Merkle trees are used in distributed systems for efficient data verification.
2. Merkle trees can be used to verify any kind of data stored, handled and transferred in and between computers.

3. Merkle trees help ensure that data blocks received from other peers in a peer-to-peer network are received undamaged and unaltered.
4. Merkle trees can be used to check that other peers in a peer-to-peer network do not lie and send fake blocks.
5. Merkle trees can be used to check inconsistencies.

Use of Merkle trees in blockchains : Following are various Merkle tree implementations in blockchains :

1. Git, a distributed version control system, is one of the most widely used. Git uses Merkle tree to store its data (source).
2. Interplanetary File System, a peer-to-peer distributed protocol, uses Merkle tree to provide a solution for private file storage in the blockchain.
3. Apache Cassandra uses Merkle Trees to detect inconsistencies in replicas.
4. Amazon DynamoDB, a No-SQL distributed databases, use Merkle trees to control discrepancies.
5. Ethereum also uses a Merkle Tree, but a different type than Bitcoin. Ethereum uses a Merkle Patricia Trie.

Que 5.26. Mention security components used in blockchain.

Answer

Following security components are used in blockchain :

1. **Hash Function :** Refer Q. 5.19, Page 5–16P, Unit-5.
2. **Digital Signature :** Refer Q. 5.20, Page 5–17P, Unit-5.
3. **Elliptic Curve Cryptography :** Refer Q. 5.21, Page 5–17P, Unit-5.
4. **Merkle Tree :** Refer Q. 5.23, Page 5–18P, Unit-5.

Que 5.27. Which cryptographic algorithm is used in blockchain ? Explain in detail. **AKTU 2020-21, 2021-22; Marks 07**

Answer

Following cryptographic algorithms are used in blockchain :

1. **Elliptic Curve Cryptography (ECC) :** Refer Q. 5.21, Page 5–17P, Unit-5.
2. **SHA-256 Hashing Algorithm :** Refer Q. 5.22, Page 5–18P, Unit-5.