PVP 20

Code: **20CS4601C**

III B.Tech - II Semester – Regular / Supplementary Examinations APRIL 2025

BLOCKCHAIN TECHNOLOGY

(COMPUTER SCIENCE & ENGINEERING)

Duration: 3 hours Max. Marks: 70

Scheme of Valuation

UNIT-I

1. a) What are the key features of blockchain technology? Explain how these features contribute to its security, transparency and immutability. 7 M

- Definition: 2.5 Marks,
- Explanation 4.5 Marks (each feature 1.5 Marks)

1. b) Analyze the benefits and limitations of blockchain technology. 7 M

- Any 2 benefits 3.5 Marks
- Any 2 Limitations – 3.5 Marks

OR

2. a) Define consensus protocols in blockchain. Explain the working principles of Proof of Work (PoW) and Proof of Stake (PoS). 7 M

- Explantion of consensus mechanism: 3 Marks
- Explantion of Proof of Work (PoW) and Proof of Stake (PoS). 4 Marks (2 Marks each)

2. b) Explain the concept of Merkle Trees in blockchain. How do Merkle Trees enhance security and efficiency in data verification? 7 M

- Explantion of Merkle trees with diagram – 7 Marks

UNIT-II

3. a) What is decentralization, and how does blockchain technology facilitate decentralized systems? 7 M

- Relevant Explanation – 7 Marks

3. b) Discuss the different methods of decentralization. How do consensus mechanisms contribute to decentralization in blockchain networks? 7 M

- Explantion of Two mechanisms - 7 Marks (3.5 Marks each)

OR

4. a) Build a block diagram to visualize the blockchain decentralized systems. 7 M

- Any Relevant explanation with diagram – 7 Marks

4. b) What does full ecosystem decentralization mean in the context of blockchain? 7 M

- Diagram - 3 Marks
- Explanation – 4 Marks

UNIT-III

5. a) What are cryptographic primitives, and why are they essential in designing secure cryptographic protocols? 7 M

- Explanation of Symmetric and Asymmetric mechanism – 7 Marks

5. b) Explain the role of cryptographic keys in Bitcoin. **7 M**

- Explanation on Public Keys – 3.5 Marks
- Explanation on Private Keys - 3.5 Marks

OR

6. a) Explain the differences between hash functions, symmetric key encryption and public key encryption as cryptographic primitives. **7 M**

- Explanation of three mechanisms – 7 Marks

6. b) Explain the need of Bitcoin Improvements proposals (BIP). **7 M**

- Explanation on BIP - 7 Marks

UNIT-IV

7. a) What is the Ethereum Virtual Machine (EVM) and why is it crucial for executing smart contracts? **7 M**

- EVM Explanation – 4 Marks
- Justification – 3 Marks

7. b) Explain the architecture of the Ethereum network and how it enables decentralized applications (DApps). **7 M**

- Architecture of Ethereum network- 4 Marks
- Explanation on how it enables decentralized applications (DApps)-3 Marks

OR

8. a) What is gas in Ethereum? Why is it important for executing transactions and smart contracts? **7 M**

- Valid Explanation on Gas– 7 Marks

8. b) What are the key challenges in DApp development and adoption? **7 M**

- Any two challenges – 7 marks

UNIT-V

9. a) What is Hyperledger and how does it differ from public blockchains like Ethereum? **7 M**

- Definition of Hyperledger- 3 Marks
- Differences – 4 Marks

9. b) How can blockchain be integrated with the Internet of Things (IoT)? Provide examples of real-world applications. **7 M**

- Explanation along with any one real world example – 7 Marks

OR

10. a) Describe the key features of Hyperledger Fabric. **7 M**

- Valid Explantion on key features of Hyperledger Fabric - 7 Marks

10. b) Discuss the role of blockchain in government services. **7 M**

- Any two Valid Services – 7 Marks

PVP 20

Code: **20CS4601C**

III B.Tech - II Semester – Regular / Supplementary Examinations APRIL 2025

BLOCKCHAIN TECHNOLOGY

(COMPUTER SCIENCE & ENGINEERING)

Duration: 3 hours Max. Marks: 70

Detailed Solution Set

1. a) What are the key features of blockchain technology? Explain how these features contribute to its security, transparency and immutability. 7 M

Ans:

Technical definition**:** Blockchain is a peer-to-peer, distributed ledger that is cryptographically-secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.

Dissecting the technical definition further reveals that blockchain is a distributed ledger, which simply means that a ledger is spread across the network among all peers in the network, and each peer holds a copy of the complete ledger.

Next, we see that this ledger is cryptographically-secure, which means that cryptography has been used to provide security services which make this ledger secure against tampering and misuse. These services include non-repudiation, data integrity, and data origin authentication.

Another property that we encounter is that blockchain is append-only, which means that data can only be added to the blockchain in time-ordered sequential order. This property implies that once data is added to the blockchain, it is almost impossible to change that data and can be considered practically immutable. Nonetheless, it can be changed in rare scenarios wherein collusion against the blockchain network succeeds in gaining more than 51 percent of the power.

Finally, the most critical attribute of a blockchain is that it is updateable only via consensus. This is what gives it the power of decentralization. In this scenario, no central authority is in control of updating the ledger. Instead, any update made to the blockchain is validated against strict criteria defined by the blockchain protocol and added to the blockchain only after a consensus has been reached among all participating peers/nodes on the network. To achieve consensus, there are various consensus facilitation algorithms which ensure that all parties are in agreement about the final state of the data on the blockchain network and resolutely agree upon it to be true.

1. b) Analyze the benefits and limitations of blockchain technology. 7 M

Ans:

Numerous advantages of blockchain technology have been discussed in many industries and proposed by thought leaders around the world who are participating in the blockchain space. The notable benefits of blockchain technology are as follows:

- Decentralization: This is a core concept and benefit of the blockchain. There is no need for a trusted third party or intermediary to validate transactions; instead, a consensus mechanism is used to agree on the validity of transactions.
- Transparency and trust: Because blockchains are shared and everyone can see what is on the blockchain, this allows the system to be transparent. As a result, trust is established. This is more relevant in scenarios such as the disbursement of funds or benefits where personal discretion in relation to selecting beneficiaries needs to be restricted.
- Immutability: Once the data has been written to the blockchain, it is extremely difficult to change it back. It is not genuinely immutable, but because changing data is so

challenging and nearly impossible, this is seen as a benefit to maintaining an immutable ledger of transactions.

- High availability: As the system is based on thousands of nodes in a peer-to-peer network, and the data is replicated and updated on every node, the system becomes highly available. Even if some nodes leave the network or become inaccessible, the network as a whole continues to work, thus making it highly available. This redundancy results in high availability.
- Highly secure: All transactions on a blockchain are cryptographically secured and thus provide network integrity.
- Simplification of current paradigms: The current blockchain model in many industries, such as finance or health, is somewhat disorganized. In this model, multiple entities maintain their own databases and data sharing can become very difficult due to the disparate nature of the systems. However, as a blockchain can serve as a single shared ledger among many interested parties, this can result in simplifying the model by reducing the complexity of managing the separate systems maintained by each entity.
- Faster dealings: In the financial industry, especially in post-trade settlement functions, blockchain can play a vital role by enabling the quick settlement of trades. Blockchain does not require a lengthy process of verification, reconciliation, and clearance because a single version of agreed-upon data is already available on a shared ledger between financial organizations.
- Cost saving: As no trusted third party or clearing house is required in the blockchain model, this can massively eliminate overhead costs in the form of the fees which are paid to such parties.

As with any technology, some challenges need to be addressed in order to make a system more robust, useful, and accessible. Blockchain technology is no exception. In fact, much effort is being made in both academia and industry to overcome the challenges posed by blockchain technology. The most sensitive blockchain problems are as follows:

- Scalability: Significant computing power is expended by miners leading to substantial energy consumption and wastage. Hence, it is not suitable for organizations that require instant transaction results within milliseconds.
- Adaptability: If a time-tested and fully functional database and the operational network are already in place, the benefits of replacing or introducing blockchain may not produce the required return on investment.
- Not every node has the capacity to maintain and run a full copy of the blockchain. This can potentially affect consensus and immutability
- Privacy: Stronger players (nodes with higher computing power or with pooling) can take control of the network, impacting decentralization. In smaller blockchains, there is a risk of a 51% attack. If one or group of malicious nodes can get 51% of the mining hash rate, they can manipulate the transactions.
- Regulation: The regulatory standards from the Government and Technological point of view have to be designed.
- Relatively immature technology: Since the technology is new much research is being done to overcome the issues related to scalability and security are being improved.

2. a) Define consensus protocols in blockchain. Explain the working principles of Proof of Work (PoW) and Proof of Stake (PoS). 7 M

Ans:

Consensus is a distributed computing concept that has been used in blockchain in order to provide a means of agreeing to a single version of the truth by all peers on the blockchain network.

The two main categories of consensus mechanisms:

- Proof-based, leader-election lottery based, or the Nakamoto consensus whereby a leader is elected at random (using an algorithm) and proposes a final value. This category is also referred to as the fully decentralized or permissionless type of consensus mechanism. This type is well used in the Bitcoin and Ethereum blockchain in the form of a PoW mechanism.
- BFT-based is a more traditional approach based on rounds of votes. This class of consensus is also known as the consortium or permissioned type of consensus mechanism.

The consensus algorithms available today which are widely in use are:

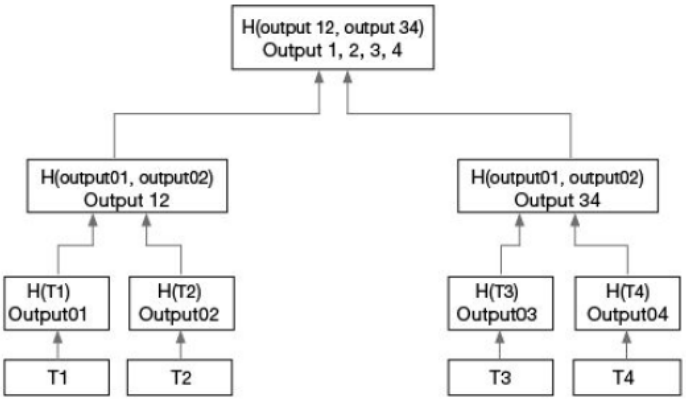
- Proof of Work (PoW): This type of consensus mechanism relies on proof that adequate computational resources have been spent before proposing a value for acceptance by the network. This scheme is used in Bitcoin, Litecoin, and other cryptocurrency blockchains. Currently, it is the only algorithm that has proven to be astonishingly successful against any collusion attacks on a blockchain network, such as the Sybil attack.
- Proof of Stake (PoS): This algorithm works on the idea that a node or user has an adequate stake in the system; that is, the user has invested enough in the system so that any malicious attempt by that user would outweigh the benefits of performing such an attack on the network. This idea was first introduced by Peercoin, and it is going to be used in the Ethereum blockchain version called Serenity. Another important concept in PoS is coin age, which is a criterion derived from the amount of time and number of coins that have not been spent. In this model, the chances of proposing and signing the next block increase with the coin age.

2. b) Explain the concept of Merkle Trees in blockchain. How do Merkle Trees enhance security and efficiency in data verification? 7 M

Ans:

A Merkle root is synonymous to a fingerprint of all the transactions in the block, which is created by hashing together pairs of Transaction IDs, to a short and unique fingerprint for all the transactions in a block. This is also a field in a block header. Sometimes, the Transaction ID (TXID) gets hashed twice using SHA256 protocol. This is done for enhanced security.

A Merkle tree (binary hash tree) involves taking large amounts of transaction data and constructing it in a way that is more convenient to process. Merkle trees have nodes and leaves. Original transactions present in the block acts as the leaves of the Merkle tree (refer Fig), and nodes in the tree act as a hash of leaves. Further, moving up the tree, new nodes are hashes of the lower nodes, and this process is repeated until the top of the tree is reached. The hash value at the top (peak) of the tree acts as a hash of the overall block (It is also called as Merkle Root).



In the above figure, “T1”, “T2”, “T3” and “T4” represent a typical transaction. These transactions are hashed (using SHA-256 in bitcoin) separately to get their corresponding hash value (which are at the next higher-level node). For example, “T1” is hashed to get its corresponding hash value of “H (T1) “. After each transaction (T1, T2, T3, and T4) has been separately hashed to generate its corresponding hash value, the new resultant hash values are further combined with an adjacent partner to be hashed once more. This process is repeated until the top of the tree is reached. For example, the hash values “H (T1)” and “H (T2)” are further combined (hashed) to get the hash “Output 12 (which is the H (H (T1), H (T2))”. In the above example (refer Fig. 4.11), there are four transactions with their corresponding hash value pairs. However, assume if there are an odd number of hash values, such as five, then the fifth hash is paired with itself (same hash) and hashed to produce a new hash value. That is, “H5” and “H5” would be combined to give “H55“. This process is repeated until the final hash value is obtained (called as Merkle root). The size of the Merkle root is 32 bytes and is part of the block header, which represents a summary of all transaction data. By comparing, the top-level hash ensures that the integrity of the data has not been compromised. To validate a transaction in a tree, we can selectively compare the hash with the selected nodes rather than finding a hash of the whole tree.

3. a) What is decentralization, and how does blockchain technology facilitate decentralized systems? 7 M

Ans:

Decentralization is a core benefit and service provided by blockchain technology. By design, blockchain is a perfect vehicle for providing a platform that does not need any intermediaries and that can function with many different leaders chosen via consensus mechanisms. This model allows anyone to compete to become the decision-making authority. This competition is governed by a consensus mechanism, and the most commonly used method is known as Proof of Work (PoW). Decentralization is applied in varying degrees from a semi-decentralized model to a fully decentralized one depending on the requirements and circumstances. Decentralization can be viewed from a blockchain perspective as a mechanism that provides a way to remodel existing applications and paradigms, or to build new applications, in order to give full control to users. A decentralized system is a type of network where nodes are not dependent on a single master node; instead, control is distributed among many nodes. This is analogous to a model where each department in an organization is in charge of its own database server, thus taking away the power from the central server and distributing it to the subdepartments who manage their own databases. A significant innovation in the decentralized paradigm that has given rise to this new era of decentralization of applications is decentralized consensus. This mechanism came into play with Bitcoin, and it enables a user to agree on something via a consensus algorithm without the need for a central, trusted third party, intermediary, or service provider. In the decentralized environment, anyone can access or write into the ledger. This inclusivity ensures that

- no single entity has sole control of the network
- there is no single infrastructural point of failure,
- there is a collective agreement on the state of the system via consensus

The decentralization that is inherent in Distributed Ledger Technology is the core of Blockchain Technology.

3. b) Discuss the different methods of decentralization. How do consensus mechanisms contribute to decentralization in blockchain networks? 7 M

Ans:

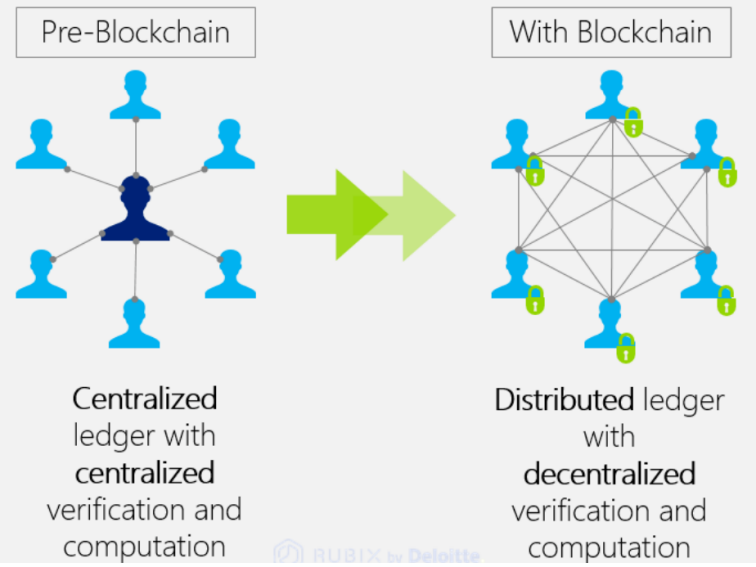
Two methods can be used to achieve decentralization: disintermediation and competition (Contest-driven decentralization).

- Disintermediation: The concept of disintermediation can be explained with the aid of an example. Imagine that you want to send money to a friend in another country. You go to a bank who, for a fee, will transfer your money to the bank in that country. In this case, the bank maintains a central database that is updated, confirming that you have sent the money. With blockchain technology, it is possible to send this money directly to your friend without the need for a bank. All you need is the address of your friend on the blockchain. This way, the intermediary; that is, the bank, is no longer required, and decentralization is achieved by disintermediation. It is debatable, however, how practical decentralization through disintermediation is in the financial sector due to massive regulatory and compliance requirements. Nevertheless, this model can be used not only in finance but in many different industries as well.
- Contest-driven decentralization: In the method involving competition, different service providers compete with each other in order to be selected for the provision of services by the system. This paradigm does not achieve complete decentralization. However, to a certain degree, it ensures that an intermediary or service provider is not monopolizing the service. In the context of blockchain technology, a system can be envisioned in which smart contracts can choose an external data provider from a large number of providers based on their reputation, previous score, reviews, and quality of service. This method will not result in full decentralization, but it allows smart contracts to make a free choice based on the criteria just mentioned. This way, an environment of competition is cultivated among service providers where they compete with each other to become the data provider of choice.

4. a) Build a block diagram to visualize the blockchain decentralized systems. 7 M

Ans:

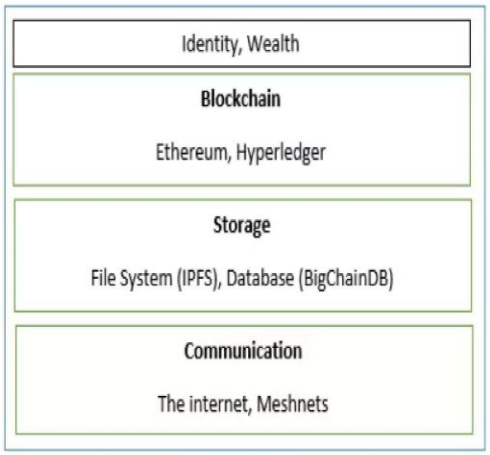
Blockchain decentralization refers to the distribution of authority and control across a network of participants, rather than relying on a single central entity. This means no one organization or individual has sole control over the network or the data it stores. Instead, independent participants, known as nodes, collectively verify and approve transactions, ensuring the blockchain's integrity and security. The key aspects of blockchain decentralization is Distributed Ledger. Blockchain data is not stored in one central location but is replicated across a network of computers, making it more difficult to tamper with.



4. b) What does full ecosystem decentralization mean in the context of blockchain? 7 M

Ans:

To achieve complete decentralization, it is necessary that the environment around the blockchain also be decentralized. The blockchain is a distributed ledger that runs on top of conventional systems. These elements include: storage, communication, and computation.



Decentralized ecosystem

Storage: Data can be stored directly in a blockchain, and with this fact it achieves decentralization. However, a significant disadvantage of this approach is that a blockchain is not suitable for storing large amounts of data by design. A better alternative for storing data is to use Distributed Hash Tables (DHTs). DHTs were used initially in peer-to-peer file sharing software, such as BitTorrent, Napster, Kazaa, and Gnutella. There are other alternatives for data storage, such as Ethereum, Swarm, Storj, and MaidSafe. Ethereum has its own decentralized and distributed ecosystem that uses Swarm for storage and the Whisper protocol for communication. MaidSafe aims to provide a decentralized World Wide Web. BigchainDB is another storage layer decentralization project aimed at providing a scalable, fast, and linearly scalable decentralized database as opposed to a traditional file system. BigchainDB complements decentralized processing platforms and file systems such as Ethereum and IPFS.

Communication: The internet (the communication layer in blockchain) is considered to to be decentralized . This model is based on unconditional trust of a central authority (the service provider) where users are not in control of their data. Even user passwords are stored on trusted third-party systems. Thus, there is a need to provide control to individual users in such a way that access to their data is guaranteed and is not dependent on a single third party. Access to the internet (the communication layer) is based on Internet Service Providers (ISPs) who act as a central hub for internet users. If the ISP is shut down for any reason, then no communication is possible with this model. An alternative is to use mesh networks. Even though they are limited in functionality when compared to the internet, they still provide a decentralized alternative where nodes can talk directly to each other without a central hub such as an ISP. Example: Firechat – iphone Now imagine a network that allows users to be in control of their communication; no one can shut it down for any reason. This could be the next step toward decentralizing communication networks in the blockchain ecosystem.

Computing power and decentralization: Decentralization of computing or processing power is achieved by a blockchain technology such as Ethereum, where smart contracts with embedded business logic can run on the blockchain network.

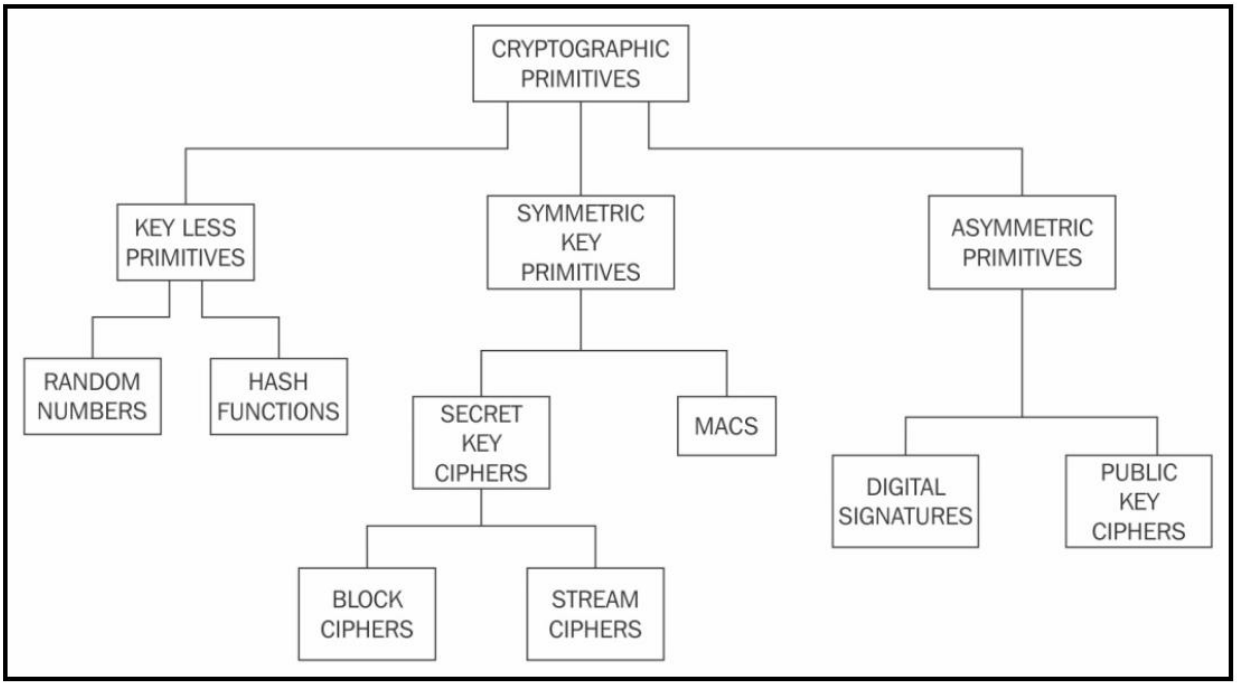
Other blockchain technologies also provide similar processing-layer platforms, where business logic can run over the network in a decentralized manner. At the bottom layer, the internet or Meshnets provide a decentralized communication layer. On the next layer up, a storage layer uses technologies such as IPFS and BigchainDB to enable decentralization. Finally, at the next level up, you can see that blockchain serves as a decentralized processing (computation) layer.

Blockchain in a limited way, provide a storage layer too, but that severely hampers the speed and capacity of the system. Therefore, other solutions such as IPFS and BigchainDB are more suitable to store large amounts of data in a decentralized way. The Identity, Wealth layers are shown at the top level. Identity on the internet is a vast topic, and systems such as BitAuth and OpenlD provide authentication and identification services with varying degrees of decentralization and security assumptions. The blockchain is capable of providing solutions to various issues relating to decentralization. A concept relevant to identity known as Zooko's Triangle requires that the naming system in a network protocol be secure, decentralized, and is able to provide human-meaningful and memorable names to the users.

5. a) What are cryptographic primitives, and why are they essential in designing secure cryptographic protocols? 7 M

Ans:

Cryptographic primitives are the basic building blocks of a security protocol or system. In the following section, you are introduced to cryptographic algorithms that are essential for building secure protocols and systems. A security protocol is a set of steps taken to achieve the required security goals by utilizing appropriate security mechanisms. Various types of security protocols are in use, such as authentication protocols, non-repudiation protocols, and key management protocols. The taxonomy of cryptographic primitives can be visualized as shown here:



As shown in the cryptographic primitives taxonomy diagram, cryptography is mainly divided into two categories: symmetric cryptography and asymmetric cryptography.

- Symmetric cryptography refers to a type of cryptography where the key that is used to encrypt the data is the same one that is used for decrypting the data. Thus, it is also known as shared key cryptography. The key must be established or agreed upon before the data exchange occurs between the communicating parties. This is the reason it is also called secret key cryptography.
- Asymmetric cryptography refers to a type of cryptography where the key that is used to encrypt the data is different from the key that is used to decrypt the data. This is also known as public key cryptography. It uses both public and private keys to encrypt and decrypt data, respectively.

5. b) Explain the role of cryptographic keys in Bitcoin. 7 M

Ans:

On the Bitcoin network, possession of bitcoins and transfer of value via transactions is reliant upon private keys, public keys, and addresses. Elliptic Curve Cryptography (ECC) is used to generate public and private key pairs in the Bitcoin network.

- Private keys in Bitcoin: Private keys are required to be kept safe and normally resides only on the owner's side. Private keys are used to digitally sign the transactions proving the ownership of the bitcoins. Private keys are fundamentally 256-bit numbers randomly chosen in the range specified by the secp256k1 ECDSA curve recommendation. Any randomly chosen 256-bit number from 0x1 to 0xFFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFE BAAE DCE6 AF48 A03B BFD2 5E8C D036 4140 is a valid private key. Private keys are usually encoded using Wallet Import Format (WIF) in order to make them easier to copy and use. It is a way to represent the full size private key in a different format. WIF can be converted into a private key and vice versa. Also, mini private key format is sometimes used to create the private key with a maximum of up to 30 characters in order to allow storage where physical space is limited, for example, etching on physical coins or encoding in damage-resistant QR codes. The QR code becomes more damage resistant because more dots can be used for error correction and less for encoding the private key. The private key encoded using mini private key format is also sometimes called minikey.
- Public keys in Bitcoin: Public keys exist on the blockchain and all network participants can see it. Public keys are derived from private keys due to their special mathematical relationship with the private keys. Once a transaction signed with the private key is broadcasted on the Bitcoin network, public keys are used by the nodes to verify that the transaction has indeed been signed with the corresponding private key. This process of verification proves the ownership of the bitcoin. Bitcoin uses ECC based on the secp256k1 standard. More specifically it makes use of ECDSA to ensure that funds remain secure and can only be spent by the legitimate owner.

6. a) Explain the differences between hash functions, symmetric key encryption and public key encryption as cryptographic primitives. 7 M

Ans:

- Cryptographic hash mode: Hash functions are primarily used to compress a message to a fixed-length digest. In cryptographic hash mode, block ciphers are used as a compression function to produce a hash of plaintext.
- Symmetric cryptography refers to a type of cryptography where the key that is used to encrypt the data is the same one that is used for decrypting the data. Thus, it is also known as shared key cryptography. The key must be established or agreed upon before the data exchange occurs between the communicating parties. This is the reason it is also called secret key cryptography.
- Asymmetric cryptography refers to a type of cryptography where the key that is used to encrypt the data is different from the key that is used to decrypt the data. This is also known as public key cryptography. It uses both public and private keys to encrypt and decrypt data, respectively.

6. b) Explain the need of Bitcoin Improvements proposals (BIP). 7 M

Ans:

These documents are used to propose or inform the Bitcoin community about the improvements suggested, the design issues, or information about some aspects of the bitcoin ecosystem. There are three types of Bitcoin improvement proposals, abbreviated as BIPs:

- Standard BIP: Used to describe the major changes that have a major impact on the Bitcoin system, for example, block size changes, network protocol changes, or transaction verification changes.
- Process BIP: A major difference between standard and process BIPs is that standard BIPs cover protocol changes, whereas process BIPs usually deal with proposing a change in a process that is outside the core Bitcoin protocol. These are implemented only after a consensus among bitcoin users.
- Informational BIP: These are usually used to just advise or record some information about the Bitcoin ecosystem, such as design issues.

These improvement proposals are usually made in the form of BIPs or fundamentally new versions of Bitcoin protocols resulting in a new network altogether. Some of the changes proposed are implementable via a soft fork but few need a hard fork and as a result, give birth to a new currency.

Various Bitcoin Improvement Proposals (BIPs) have been proposed and finalized in order to introduce and standardize bitcoin payments. Most notably, BIP 70 (Payment Protocol) describes the protocol for secure communication between a merchant and customers. Several other BIPs, such as BIP 71 (Payment Protocol MIME types) and BIP 72 (URI extensions for Payment Protocol), have also been implemented to standardize payment scheme to support BIP 70 (Payment Protocol).

7. a) What is the Ethereum Virtual Machine (EVM) and why is it crucial for executing smart contracts? 7 M

Ans:

The Ethereum Virtual Machine (EVM) is a simple stack-based execution machine that runs bytecode instructions to transform the system state from one state to another. The word size of the virtual machine is set to 256-bit. The stack size is limited to 1024 elements and is based on the Last In, First Out (LIFO) queue. EVM is a Turing-complete machine but is limited by the amount of gas that is required to run any instruction. This means that infinite loops that can result in denial of service attacks are not possible due to gas requirements. EVM also supports exception handling, in case exceptions occur, such as not having enough gas or invalid instructions, in which case the machine would immediately halt and return the error to the executing agent.

EVM is an entirely isolated and sandboxed runtime environment. The code that runs on the EVM does not have access to any external resources, such as a network or filesystem. This results in increased security, deterministic execution and allows untrusted code (anyone can run code) to be run on Ethereum blockchain. EVM is big-endian by design, and it uses 256-bit wide words. This word size allows for Keccak 256-bit hash and ECC computations. It is sufficient to say here that Ethereum supports the development of smart contracts that run on the EVM. There are also various contracts that are available in the precompiled format in Ethereum blockchain to support different functions. These contracts, known as precompiled contracts or native contracts. These are not strictly smart contracts in the sense of user programmed solidity smart contracts, but in fact are functions that are available natively on the blockchain to support various computationally intensive tasks. They run on the local node and are coded within the Ethereum client, for example, parity or geth.

In summary, a smart contract has the following four properties: Automatically executable, Enforceable, Semantically sound, Secure and unstoppable The first two properties are required as a minimum, whereas the latter two may not be required or implementable in some scenarios and can be relaxed. For example, a financial derivatives contract does not perhaps need to be semantically sound and unstoppable but should at least be automatically executable and enforceable at a fundamental level. On the other hand, a title deed needs to be

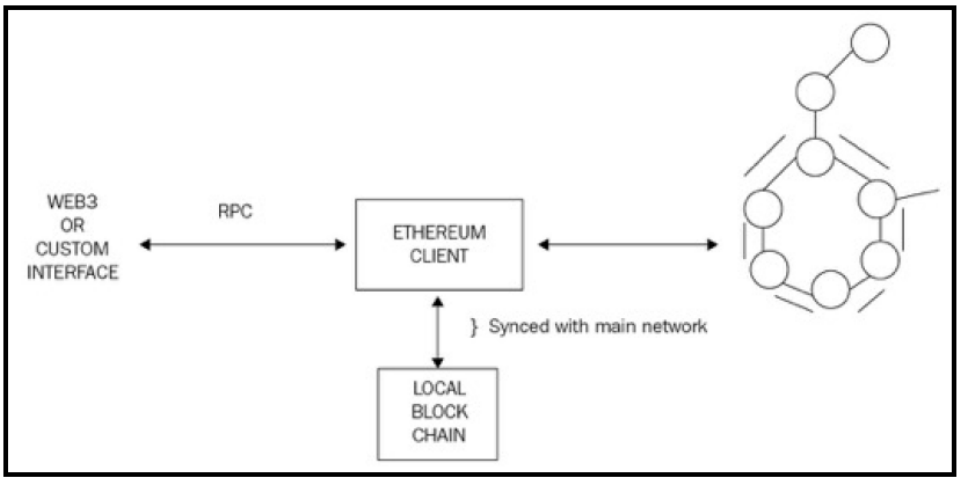
semantically sound and complete, therefore, for it to be implemented as a smart contract, the language must be understood by both computers and people.

7. b) Explain the architecture of the Ethereum network and how it enables decentralized applications (DApps). 7 M

Ans:

The Ethereum blockchain stack consists of various components. At the core, there is the Ethereum blockchain running on the peer-to-peer Ethereum network. Secondly, there's an Ethereum client (usually Geth) that runs on the nodes and connects to the peer-to-peer Ethereum network from where blockchain is downloaded and stored locally. It provides various functions, such as mining and account management. The local copy of the blockchain is synchronized regularly with the network. Another component is the web3.js library that allows interaction with the geth client via the Remote Procedure Call (RPC) interface. A formal list of all high-level elements present in the Ethereum blockchain are:

- Keys and addresses
- Accounts
- Transactions and messages
- Ether cryptocurrency/tokens
- The EVM
- Smart contracts



The Ethereum stack showing various components

The Ethereum network enables decentralized applications (DApps) by providing a platform for building and deploying smart contracts and applications that operate on a decentralized, peer-to-peer network, rather than relying on centralized servers. This decentralization offers enhanced security, resilience, and user control. Smart contracts may or may not be deployed on a blockchain, but it makes sense to deploy them on a blockchain due to the distributed and decentralized consensus mechanism provided by blockchain. Ethereum is an example of a blockchain platform that natively supports the development and deployment of smart contracts. Smart contracts on Ethereum blockchain are usually part of a broader application such as Decentralized Autonomous organization (DAOs).

8. a) What is gas in Ethereum? Why is it important for executing transactions and smart contracts? 7 M

Ans:

Ether is paid as commission for any execution that affects the state in Ethereum. Ether (ETH) is traded on people exchanges and its particular selling price value changes each day. Its value

could be high on certain days, when it is used for payment and lower on other days. Individuals may wait for the price of Ether to fall to perform their transactions. This condition is not ideal for the Ethereum platform. The gas helps in alleviating this problem. Gas is the internal currency of Ethereum. The execution and resource utilization costs are predetermined in Ethereum in terms of Gas units. This is also known as Gas Cost.
Additionally, a gas price may be corrected to lower the costs whenever the amount tag on Ether increases and increase the price as soon as the amount tag on Ether decreases. For instance, to set up a function at a transaction that simplifies a series will probably cost predetermined gas, and consumers need to pay in the denomination of gas to guarantee implementation of the transaction.

8. b) What are the key challenges in DApp development and adoption? 7 M

Ans:

Key challenges in DApp development and adoption include scalability issues, security vulnerabilities, the need for specialized knowledge, and building user trust in a decentralized environment. Additionally, ensuring a good user experience, managing complex smart contracts, and navigating regulatory landscapes are also significant hurdles.

- Scalability: DApps, particularly those built on blockchains like Ethereum, often struggle with handling large numbers of transactions, leading to slower speeds and higher transaction costs.
- Security: Smart contracts, which are the core of DApps, can be vulnerable to exploits and hacks, potentially leading to significant financial losses.
- User Trust: Building trust in a decentralized system can be challenging, as users need to understand and trust the technology, as well as the other participants in the network.
- User Experience (UX): Many early DApps have struggled to provide a user-friendly experience compared to traditional web applications, hindering adoption.
- Specialized Knowledge: DApp development requires specialized knowledge of blockchain technology, smart contracts, and decentralized systems, which can be a barrier for many developers.
- Smart Contract Complexity: Managing complex smart contracts, which are essentially code that automatically executes when certain conditions are met, can be challenging.
- Regulatory Compliance: The regulatory landscape for DApps is still evolving, and developers need to navigate complex regulations across different jurisdictions.
- Interoperability: The ability for DApps to interact with each other and other systems is crucial for widespread adoption, but current interoperability limitations can hinder this.
- Adoption and Network Effects: Building a strong user base and achieving network effects, where the value of a DApp increases as more users join, is a significant challenge.

9. a) What is Hyperledger and how does it differ from public blockchains like Ethereum? 7 M

Ans:

Hyperledger is not a blockchain, but it is a project that was initiated by the Linux Foundation in December 2015 to advance blockchain technology. This project is a collaborative effort by its members to build an open source distributed ledger framework that can be used to develop and implement cross-industry blockchain applications and systems. The principal focus is to develop and run platforms that support global business transactions. The project also focuses on improving the reliability and performance of blockchain systems. Projects under Hyperledger undergo various stages of development, starting from proposal to incubation and graduating to

an active state. Projects can also be deprecated or in end-of life state where they are no longer actively developed. For a project to be able to move into the incubation stage, it must have a fully working code base along with an active community of developers. Hyperledger is aiming to build new blockchain platforms that are driven by industry use cases. As there have been many contributions made to the Hyperledger project by the community, Hyperledger blockchain platform is evolving into a protocol for business transactions. Hyperledger is also evolving into a specification that can be used as a reference to build blockchain platforms as compared to earlier blockchain solutions that address only a specific type of industry or requirement.

Feature	**Ethereum**	**Hyperledger**
Architecture	Public, open-source, permissionless	Private or permissioned, modular, extensible
Purpose	General-purpose platform for dApps and smart contracts	Framework for building private blockchain networks for enterprise use
Smart Contracts	Uses Solidity language for smart contracts	Uses Chaincode (e.g., Go, Javascript, Java) for smart contracts
Token Economy	Has a native cryptocurrency, Ether (ETH)	Does not have a native cryptocurrency; can implement custom tokens if needed
Consensus	Uses Proof of Stake (PoS)	Offers various consensus mechanisms, including Kafka, Raft, and Solo
Community	Community-driven	Managed by the Linux Foundation
Use Cases	Decentralized finance (DeFi), NFTs, dApps, and general blockchain applications	Enterprise applications, supply chain management, financial services, etc.

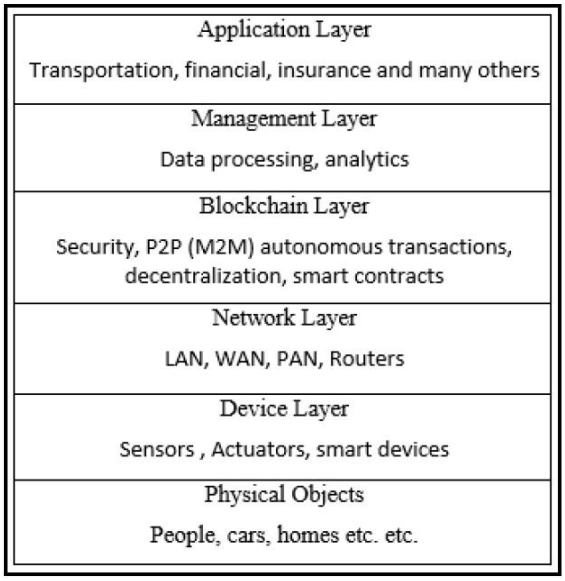
9. b) How can blockchain be integrated with the Internet of Things (IoT)? Provide examples of real-world applications. 7 M

Ans:

According to IBM, blockchain for IoT can help to build trust, reduce costs, and accelerate transactions. Additionally, decentralization, which is at the very core of blockchain technology, can eliminate single points of failure in an IoT network. For example, a central server perhaps is not able to cope with the amount of data that billions of IoT devices (things) are producing at high frequency. Also, the peer-to-peer communication model provided by blockchain can help to reduce costs because there is no need to build high-cost centralized data centers or implementation of complex public key infrastructure for security. Devices can communicate with each other directly or via routers. As an estimate of various researchers and companies, by 2020 there will be roughly 22 billion devices connected to the internet. With this explosion of billions of devices connecting to the internet, it is hard to imagine that centralized infrastructures will be able to cope with the high demands of bandwidth, services, and availability without incurring excessive expenditure. Blockchain-based IoT will be able to solve scalability, privacy, and reliability issues in the current IoT model.

Blockchain enables things to communicate and transact with each other directly and with the availability of smart contracts, negotiation, and financial transactions can also occur directly between the devices instead of requiring an intermediary, authority, or human intervention. For example, if a room in a hotel is vacant, it can rent itself out, negotiate the rent, and can open the door lock for a human who has paid the right amount of funds. Another example could be that if a washing machine runs out of detergent, it could order it online after finding the best price and value based on the logic programmed in its smart contract.

The aforementioned five-layer IoT model can be adapted to a blockchain-based model by adding a blockchain layer on top of the network layer. This layer will run smart contracts, and provide security, privacy, integrity, autonomy, scalability, and decentralization services to the IoT ecosystem. The management layer, in this case, can consist of only software related to analytics and processing, and security and control can be moved to the blockchain layer. This model can be visualized in the following diagram:



Blockchain-based IoT model

In this model, other layers would perhaps remain the same, but an additional blockchain layer will be introduced as a middleware between all participants of the IoT network. It can also be visualized as a peer-to-peer IoT network after abstracting away all the layers mentioned earlier. This model is shown in the following diagram where all devices are communicating and negotiating with each other without a central command and control entity:

Blockchain-based direct communication model, source: IBM

It can also result in cost saving which is due to easier device management by using a blockchain based decentralized approach. The IoT network can be optimized for performance by using blockchain. In this case, there will be no need to store IoT data centrally for millions of devices because storage and processing requirements can be distributed to all IoT devices on the blockchain. This can result in completely removing the need for large data centers for processing and storing the IoT data.

10. a) Describe the key features of Hyperledger Fabric. 7 M

Ans:

Fabric can be defined as a collection of components providing a foundation layer that can be used to deliver a blockchain network. There are various types and capabilities of a fabric network, but all fabrics share common attributes such as immutability and are consensus-driven. Some fabrics can provide a modular approach towards building blockchain networks. In this case, the blockchain network can have multiple pluggable modules to perform a various function on the network. Fabric is also the name given to the code contribution made by IBM to the Hyperledger foundation and is formally called Hyperledger Fabric. This contribution aims to enable a modular, open, and flexible approach towards building blockchain networks. Various functions in the fabric are pluggable, and it also allows the use of any language to develop smart contracts. This functionality is possible because it is based on container technology (Docker), which can host any language.

Chaincode is sandboxed in a secure container, which includes a secure operating system, chaincode language, runtime environment, and SDKs for Go, Java, and Node.js. Other languages can be supported too in future, if required, but needs some development work. Smart contracts are called chaincode in the fabric. This ability is a compelling feature compared to domain-specific languages in Ethereum, or the limited scripted language in Bitcoin. It is a permissioned network that aims to address issues such as scalability, privacy, and confidentiality. The fundamental idea behind this is modularization, which would allow for flexibility in design and implementation of the business blockchain. This can then result in achieving scalability, privacy, and other desired attributes and fine tune them according to the requirements.

Transactions in the fabric are private, confidential, and anonymous for general users, but they can still be traced and linked to the users by authorized auditors. As a permissioned network, all participants are required to be registered with the membership services to access the blockchain network. This ledger also provided auditability functionality to meet the regulatory and compliance needs required by the user.

10. b) Discuss the role of blockchain in government services. 7 M

Ans:

There are various applications of blockchain being researched currently that can support government functions and take the current model of e-government to the next level. Few use cases such as:

- **e-voting**: Voting in any government is a key function and allows citizens to participate in the democratic election process. While voting has evolved into a much more mature and secure process, it still has limitations that need to be addressed to achieve a desired level of maturity. Usually, the limitations in current voting systems revolve around fraud, weaknesses in operational processes, and especially transparency. Over the years, secure voting mechanisms (machines) have been built which make use of specialized voting machines that promised security and privacy, but they still had vulnerabilities that could be exploited to subvert the security mechanisms of those machines. These vulnerabilities can lead to serious implications for the whole voting process and can result in mistrust in the government by the public. Blockchain-based voting systems can resolve these issues

by introducing end-to-end security and transparency in the process. Security is provided in the form of integrity and authenticity of votes by using public key cryptography which comes as standard in a blockchain. Moreover, immutability guaranteed by blockchain ensures that votes cast once cannot be cast again. This can be achieved through a combination of biometric features and a smart contract maintaining a list of votes already cast.

- **Homeland security (border control):** Blockchain can provide a solution to this problem by maintaining a blacklist in a smart contract which can be updated as required and any changes will be immediately visible to all agencies and border control points thus enabling immediate control over the movement of a suspected travel document. It could be argued that traditional mechanisms like PKIs and peer-to-peer networks can also be used for this purpose, but they do not provide the benefits that a blockchain can provide. With blockchain, the whole system can be simplified without the requirement of complex networks and PKI setups which will also result in cost reduction. Moreover, blockchain based systems will provide cryptographically guaranteed immutability which helps with auditing and discourages any fraudulent activity.
- **Electronic IDs (citizen ID cards):** Digital identity is not only limited to just government-issued ID cards; it is a concept that applies to online social networks and forums too. There can be multiple identities used for different purposes. A blockchain-based online digital identity allows control over personal information sharing. Users can see who used their data and for what purpose and can control access to it. This is not possible with the current infrastructures which are centrally controlled. The key benefit is that a single identity issued by the government can be used easily and in a transparent manner for multiple services via a single government blockchain. In this case, the blockchain serves as a platform where a government is providing various services such as pensions, taxation, or benefits and a single ID is being used for accessing all these services. Blockchain, in this case, provides a permanent record of every change and transaction made by a digital ID, thus ensuring integrity and transparency of the system. Also, citizens can notarize birth certificates, marriages, deeds, and many other documents on the blockchain tied with their digital ID as a proof of existence.