SOLUTIONS KEY

T1 Examination Questions (EVEN 2023)

21B12CS317: Introduction to Blockchain Technologies

---

1. **[CO1: 4 Marks] List and explain in detail the need of blockchain technology when there exists standard centralized applications in use. Also provide the role of trust in decentralization.**

Blockchain technology is a decentralized, distributed ledger system that has been designed to address some of the shortcomings of centralized applications. The key need for blockchain technology can be explained as follows: [2 Marks]

- **Decentralization: The main advantage of blockchain technology over centralized applications is that it is decentralized. This means that there is no central authority controlling the system, and instead, the system is run by a network of nodes that are spread across the globe. This eliminates the need for intermediaries, such as banks, which can reduce transaction costs and increase efficiency.**
- **Security: Blockchain technology provides a high level of security by using cryptographic techniques to ensure that transactions are verified and cannot be altered once they have been recorded. This ensures that the data stored in the blockchain is tamper-proof and provides an added layer of security for sensitive information.**
- **Transparency: Blockchain technology provides a high level of transparency by allowing anyone to view the transactions on the blockchain. This can increase accountability and trust, especially in industries where transparency is crucial, such as supply chain management.**
- **Immunity to fraud: Due to the distributed nature of the blockchain, it is much more difficult for hackers to gain control of the system. This makes blockchain technology much more resilient to fraud and other cyber threats.**

[2 Marks]

Trust plays a crucial role in the decentralization of blockchain technology. In traditional centralized systems, trust is placed in a central authority or intermediary. However, in a decentralized system, trust is placed in the network of nodes that make up the blockchain. This is achieved through a consensus mechanism, such as Proof of Work or Proof of Stake, which ensures that all nodes in the network agree on the state of the blockchain.

Trust and Privacy Issues in Banking Systems:

- **Trust and privacy issues can arise due to the centralized nature of traditional banking, where a single entity holds and controls all financial information.**
- **This can make personal and financial information vulnerable to hackers and other malicious actors.**
- **Additionally, traditional banking systems can be opaque, making it difficult for customers to understand how their data is being used and shared.**
- **These issues can lead to a lack of trust in the banking system and reluctance to use digital financial services.**

Decentralization allows for a greater level of trust as there is no single point of failure or authority. This can increase confidence in the system and reduce the risk of fraud and corruption. Additionally, the transparency of the blockchain allows users to verify the transactions and ensure that they are legitimate, further increasing trust in the system.

2. **[CO1: 4 Marks] Recall and present various design principles to be followed in developing blockchain projects along with focus on implementation challenges.**

Blockchain Design principles [2 Marks]

- **Network integrity: Blockchain systems rely on a network of nodes to validate and record transactions. Network integrity refers to the ability of the network to maintain the accuracy and consistency of the blockchain ledger. In order to maintain network integrity, consensus mechanisms**

and cryptographic algorithms are used to ensure that all nodes have a copy of the same data and that any new transactions are valid.

- **Distributed power: Blockchain technology is built on the principle of distributed power, meaning that no single entity has control over the network. Instead, power is spread out among all the nodes in the network. This decentralization of power ensures that the blockchain is resistant to censorship and tampering.**
- **Value as incentives: In order to ensure that nodes are motivated to participate in the network, blockchain systems often use value as incentives. For example, in public blockchains, nodes are incentivized to validate transactions and add new blocks to the blockchain through the use of cryptocurrency rewards.**
- **Security: Blockchain systems use advanced cryptographic algorithms to secure transactions and protect the integrity of the network. These security measures include hashing, digital signatures, and secure multiparty computation.**
- **Privacy: Blockchain technology can be used to provide privacy and anonymity for users. For example, the Enigma protocol uses homomorphic encryption to allow for computations to be performed on encrypted data without the need to decrypt it first.**

Implementation Challenges [2 Marks]

- **The Technology challenges: Implementing blockchain technology can be a complex and difficult task, requiring specialized knowledge and skills. The technology is still in its early stages of development, and there are many unknowns and uncertainties surrounding its use and implementation. This can make it difficult for organizations to develop and implement effective blockchain solutions.**
- **The Energy Consumption: The energy consumption associated with blockchain technology can be significant, as it requires a large number of computers to validate and process transactions. This can be a major challenge for organizations looking to implement blockchain solutions, as it can increase their energy costs and negatively impact their bottom line.**
- **Governments role: Governments have a significant role to play in the development and regulation of blockchain technology. They can shape its use and adoption through laws, regulations and policies. However, governments have been hesitant to fully embrace the technology due to concerns about its impact on financial systems and the potential for illegal activities.**
- **Impact of Old Paradigms: Blockchain technology represents a fundamental shift in the way organizations operate, and it can be challenging for them to adapt to this new paradigm. Many organizations are used to working with centralized systems, and they may be hesitant to adopt decentralized systems like blockchain.**
- **Challenges with the Incentives: Blockchain technology relies on incentives to encourage users to participate in the network, but it can be difficult to create incentives that are both effective and sustainable. This can be a major challenge for organizations looking to implement blockchain solutions, as it can impact the adoption and success of the technology.**
- **Blockchain as Job Killer: Blockchain technology has the potential to automate many processes, which can lead to job loss. This can be a major concern for governments and organizations, as it can have a negative impact on the economy.**
- **Governing the Protocols: Governing the protocols of blockchain networks is a difficult task, as it requires a large degree of coordination and cooperation among participants. This can be a major challenge.**

3. [CO2: 4 Marks] Explain various properties that make a hash function cryptographically secure along with the hash functions usage in maintaining data in Blockchain.

Hashing in cryptography is used to maintain integrity of data.
The output of a hash function is also called as digest/ hash value.
Hash functions takes any length string as input, and outputs a fixed length hash value or digest.

Hash functions do not require keys to generated hash value.
Blocks in a Blockchain consists of various hash digests.

- **Hash of current block, Hash of previous block, Hash of all transactions in the block, Merkle root hash etc, in the block header.**
- **Transactions do not convey the identity as they are represented using hashes. Complete anonymity is maintained. In block body.**
- **Blockchain uses hash algorithms that produce 256-bit length hash value.**

Hash value is used to compare the data.
Let x be the input of any size but the Hash function H(x) produces a fixed length digest.
Hashing should be deterministic and pseudo random

Hashing should be collision free

Let x1 and x2 are two messages and $x1 \neq x2$ then $H(x1) \neq H(x2)$
To find collisions, try 2(N/2) randomly chosen inputs (Where N is the length of hash value), then there will be > 98% chance that two inputs will collide.
Pigeon hole principle. (Birthday paradox)
This procedure will take too long time.
Is there any faster method to find collisions?
No Hash function has been proven collision free.
Hash function should process Hiding
Given a digest H(x), it is impossible to find x.
Is the above statement true always?
It may fail in case of very small set of values of x.

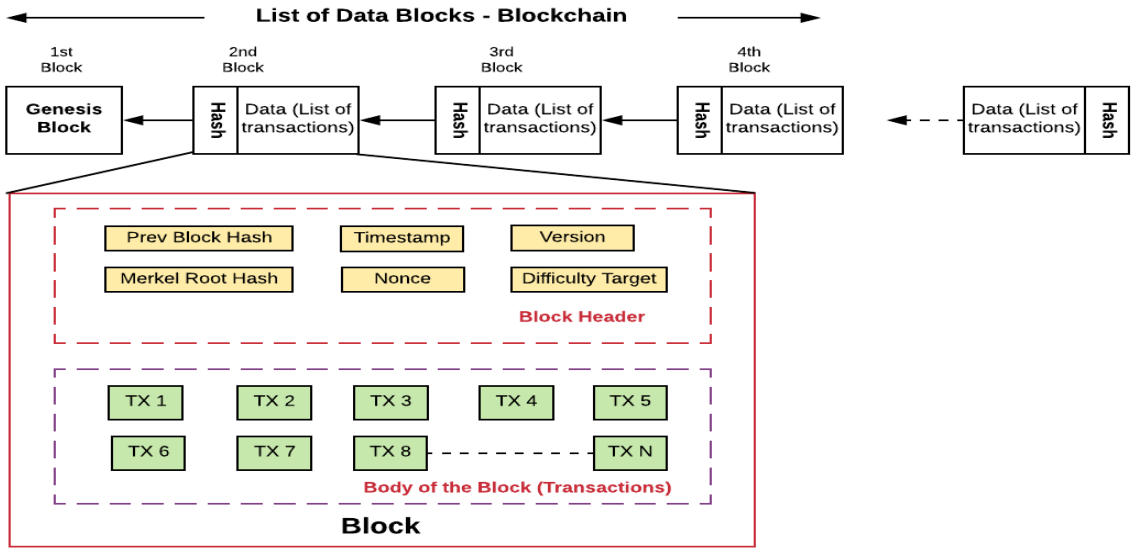
- **Hiding property states that, if k is chosen from a very spread out probability distribution (no particular value is chosen with more than negligible probability / having high min-entropy) then, given H(k | x) it is infeasible to find x.**
- **Hashing should be puzzle friendly**
- **For every possible digest value dv, if k is chosen from a distribution with high min-entropy, then it is infeasible to find x given that H(k | x) = dv.**
- **Given a "puzzle ID" id (from a high min-entropy distribution) and a target set Y , then try to find a solution x such that H(id | x) belongs to Y.**
- **Puzzle friendly property implies that no solving strategy is better than trying random value of x.**

4. <u>Write short note on the following</u>

a. <u>[CO1: 2 Marks] Structure of Block and main components of blockcian.</u>

The main components of a blockchain system include:

- **Nodes: the computers or devices that participate in the network and maintain a copy of the blockchain**
- **Transactions: the digital records of an exchange of value or information**
- **Blocks: the grouping of transactions into a secure and verifiable unit of data**
- **Mining: the process of adding new blocks to the blockchain through complex mathematical computations**
- **Cryptography: the use of mathematical algorithms to secure and validate transactions and blocks**



b. [CO2: 2 Marks] Advantages of Elliptic Curve Cryptography over other Public key cryptography algorithms.

Elliptic Curve Cryptography (ECC) is a type of public key cryptography that uses the mathematics of elliptic curves to generate secure key pairs. ECC offers several advantages over other types of public key cryptography, such as RSA. Some of these advantages include:

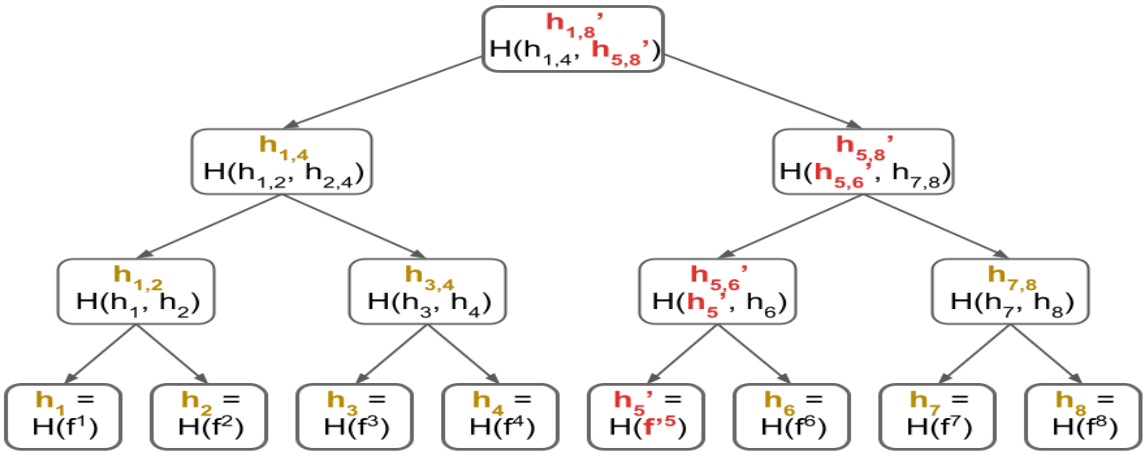
- **Smaller key size: ECC requires smaller key sizes to achieve the same level of security as RSA. This means that ECC can offer the same level of security with a fraction of the key size of RSA, making it more efficient and less resource-intensive. For example, security strength of 256-bit ECC key is equivalent to a 3072-bit RSA key, and 384-bit ECC key is equivalent to a 7680-bit RSA key.**
- **Faster encryption and decryption: ECC algorithms are faster than RSA algorithms for encryption and decryption, making it more suitable for low-power devices and embedded systems.**
- **Increased security: ECC is considered to be more secure than RSA due to the fact that it is based on the discrete logarithm problem, which is considered to be harder to solve than the factoring problem that RSA is based on.**
- **Increased scalability: ECC is more scalable than RSA, and it can be used in a wide range of cryptographic applications, including digital signature, key exchange, and encryption.**
- **Improved resistance to quantum computing: As RSA is based on the factoring problem, which is more vulnerable to quantum computing attacks, ECC is considered to be more resistant to quantum computing attacks as it is based on the discrete logarithm problem.**
- **Better performance in small devices and embedded systems: ECC requires smaller key sizes and less computational power than RSA, making it more suitable for use in small devices and embedded systems.**

5. [CO2: 4 Marks] Consider the following scenario in blockchain: A, B, C, and D are four transactions, all executed on the same block. Discuss the suitable data structure with diagram that ensures that the data blocks sent through a peer-to-peer network are whole, undamaged, and unaltered.

In order to ensure that data blocks sent through a peer-to-peer network are whole, undamaged, and unaltered, a suitable data structure is the Merkle tree. The Merkle tree is a hash tree that uses a cryptographic hash function to ensure data integrity and authenticity. In a Merkle tree, data blocks (in this case, transactions A, B, C, and D) are organized into pairs and hashed together, forming a new hash. These hashes are then paired and hashed together, forming a new hash, and so on, until a single root hash is produced. This root hash is used to represent the entire data set and can be used to verify the integrity of the data.

1. A Merkle tree is[1] a **collision-resistant hash function**, denoted by MHT, that takes n inputs $(x_1, ..., x_n)$ and outputs a *Merkle root hash* $h = \mathsf{MHT}(x_1, ..., x_n)$,
2. A verifier who only has the root hash h can be given an x_i and an associated **Merkle proof** which convinces them that x_i was the ith input used to compute h.
   - In other words, convinces them that there exist other x_j's such that $h = \mathsf{MHT}(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n)$.
   - This ability to verify that an x_i is the element at the ith position against the root hash h (i.e., without having to store all n inputs) is the fundamental power of Merkle trees which we explore in this post.
3. If a Merkle proof says that x_i was the ith input used to computed h, no attacker can come up with another Merkle proof that says a different $x_i' \neq x_i$ was the ith input.
   - More formally, an attacker cannot come up with a Merkle root h and two values $x_i \neq x_i'$ with proofs π_i and π_i' that both verify for position i w.r.t. h.

Example Merkle tree



In the above diagram, each leaf node represents a transaction, and each intermediate node represents the hash of its children. The root node represents the final hash of the entire set of transactions. This Merkle tree can be used to ensure the integrity of the data by comparing the root hash received from a peer with the root hash generated locally. If they match, the data is considered valid and unaltered. If they don't match, the data may have been tampered with during transmission.

Data structures used other than linear chaining and Merkle tree is DAG

The Directed Acyclic Graph (DAG) is a data structure that uses topological ordering and is an implementation of a directed graphical structure. DAGs are mostly used for solving problems such as data processing, finding the best route for navigation, scheduling, and data compression. One of the main advantages of DAG is that it eliminates the need for mining, unlike traditional blockchain technology. Instead, transactions are validated automatically and this results in safer, faster, and more instant transactions. Another advantage of DAG is that it helps to shorten the width of the network. In traditional blockchain, validating a transaction links it to the previous transaction, which can result in a widening of the network. In DAG, after validation, every transaction is linked to both a new and an existing transaction on the network. This helps to keep the network width under a certain range, which supports quicker transactions and validation. DAG also facilitates swift transactions as the transactions run directly into the network, making them quicker than those of blockchains based on Proof of Work (PoW) and Proof of Stake (PoS). Additionally, DAG addresses double-spending issues, as the validation of every transaction depends on the number of transactions supporting it. Some of the technologies based on DAG include IOTA, NANO, Byteball, and Hashgraph. Leading blockchain development company, Bitdeal, is actively involved in research and development of DAG, as they see it as the next form of development in blockchain technology.