Vivekanand Education Society's Institute of Technology, Chembur, Mumbai,
Department of Computer Engineering
Year : 2023-24 (ODD Sem)
MID TERM TEST

Class : BE	**Division: D17A/B/C**
Semester: VII	**Subject: Blockchain**
Date: 8th Sept 2023	**Time: 10.30 am - 11.30 am**

Q1 a. What is meant by mempool & mining Pool?

1. A mempool is the core component of how a blockchain moves transactions from a user's wallet to confirmation in a block. A blockchain creates a permanent collection of transactions, so once it is written, it can't be unwritten. So, a mechanism is needed to figure out the order of transactions to be added to a block.
2. Cryptocurrency mining pools are groups of miners who share their computational resources. Mining pools utilize these combined resources to strengthen the probability of finding a block or otherwise successfully mining for cryptocurrency. If the mining pool is successful and receives a reward, that reward is divided among participants in the pool.

Q1 b. Write a simple Solidity program to store value in a variable.

```
pragma solidity ^0.8.0;
contract SolidityTest {
  uint storedData;      // State variable
  constructor() public {
    storedData = 10;   // Using State variable
  }
}
```

Q1 c. Explain Limitations and Challenges of blockchain

While blockchain technology offers numerous benefits, it also faces limitations and challenges that can impact its widespread adoption and implementation. Some of the key limitations and challenges of blockchain are:

1. **Scalability:** One of the primary challenges of blockchain is scalability. Most blockchains, such as Bitcoin and Ethereum, have limitations on the number of transactions they can process per second. This can result in slower transaction times and higher transaction fees during peak periods, limiting the practicality of blockchain for high-volume transaction use cases.
2. E**nergy consumption:** Many blockchains, particularly those that rely on Proof of Work (PoW) consensus algorithms, require significant computing power and energy consumption for mining and validating transactions. This can have environmental impacts and raise concerns about the sustainability of blockchain technology.

3. **Governance and regulatory issues:** Blockchain's decentralized nature can make it challenging to establish governance and regulatory frameworks. The lack of a central authority can make it difficult to address issues such as disputes, fraud, and compliance with regulations, which can limit the adoption of blockchain in regulated industries.
4. **Interoperability:** Blockchain networks are often siloed and lack interoperability, making it challenging to transfer data and value between different blockchains. Interoperability is crucial for achieving seamless integration of blockchain with existing systems and other blockchain networks.
5. **Privacy and security:** While blockchain is often considered secure due to its cryptographic features, it is not completely immune to security breaches. Privacy can also be a concern, as transactions on many public blockchains are transparent and visible to all participants, potentially revealing sensitive information.
6. **User experience:** Blockchain technology can be complex and challenging for non-technical users. Issues such as private key management, transaction fees, and transaction confirmation times can impact the user experience, making it less user-friendly compared to traditional systems.
7. **Legal and regulatory uncertainty:** The legal and regulatory landscape surrounding blockchain is still evolving, with different jurisdictions having varying approaches and regulations. This can create uncertainty for businesses and individuals utilizing blockchain technology and may hinder its widespread adoption.
8. **Upgradability and backward compatibility:** Upgrading blockchain protocols can be challenging, as achieving consensus among network participants can be difficult. This can result in forks and fragmentation of the blockchain, leading to compatibility issues and potential disruptions.
9. **Ethical considerations:** As blockchain technology expands into various sectors, ethical concerns may arise, such as the potential for inequality, bias, and misuse of blockchain applications.

Q1 . d. What is a Merkle Tree ? What is its significance in a Blockchain?

A Merkle Tree, also known as a hash tree or binary hash tree, is a fundamental data structure used in cryptography and computer science. It's named after its inventor, Ralph Merkle. The main purpose of a Merkle Tree is to efficiently verify the integrity and consistency of large sets of data, particularly when dealing with distributed systems or data that might be too large to process all at once.

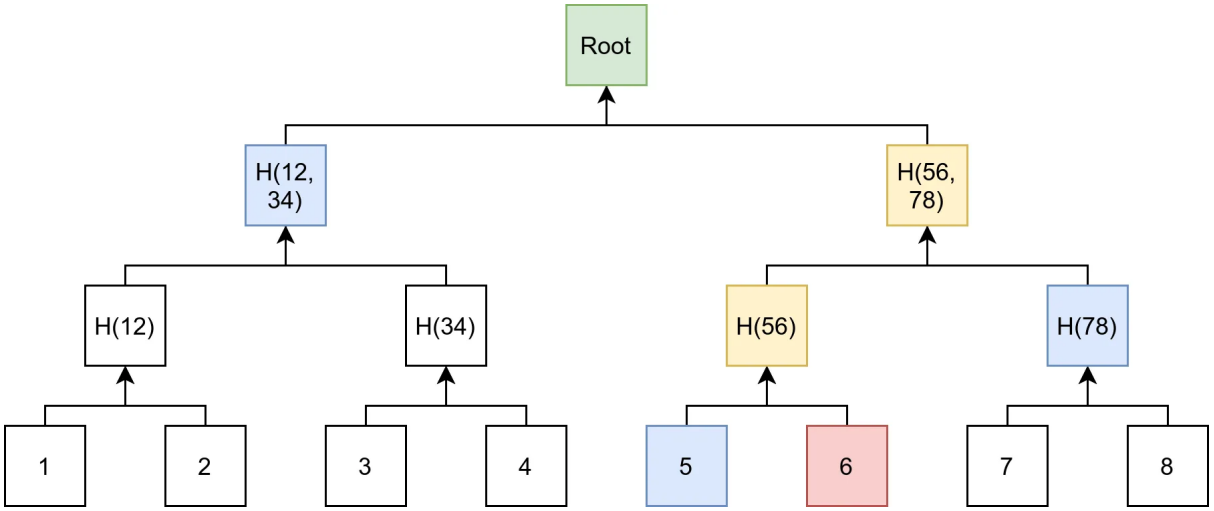
A Merkle Tree is constructed by recursively hashing data elements, typically in pairs, until a single root hash, known as the Merkle Root, is obtained. Here's a high-level explanation of how a Merkle Tree is constructed:

1. Start with a set of data elements (usually chunks of data, transactions, or blocks).

2. Hash each data element individually using a cryptographic hash function (like SHA-256).
3. If there's an odd number of hashes, duplicate the last hash to make an even number.
4. Pair adjacent hashes and concatenate them, then hash the concatenated result. This process is repeated until only one hash remains, which is the Merkle Root.

The significance of Merkle Trees in the context of blockchains is profound. Merkle Trees are used to provide efficiency and security in various aspects of blockchain technology:

1. **Efficient Data Verification:** In a blockchain, where data is distributed across many nodes, verifying the integrity of the entire dataset can be resource-intensive. Merkle Trees allow nodes to efficiently prove whether a specific data element is part of a larger dataset without needing to download and verify the entire dataset.
2. **Block Verification:** In a blockchain, transactions are grouped into blocks, and each block contains a Merkle Tree of its transactions. The Merkle Root of the transactions is stored in the block header. This enables quick verification that a specific transaction is part of a specific block without having to download and verify all transactions in that block.
3. **Efficient Light Clients:** Merkle Trees enable lightweight clients, such as mobile wallets, to interact with a blockchain without having to download the entire blockchain. These clients can request only the Merkle branch (a set of hashes) that proves the existence of a particular transaction within a block.
4. **Security:** Merkle Trees enhance the security of a blockchain by ensuring that any tampering or alteration of a single data element (transaction or block) will result in a completely different Merkle Root. This property makes it extremely difficult to manipulate historical data without being detected.



Vivekanand Education Society's Institute of Technology, Chembur, Mumbai,
Department of Computer Engineering
Year : 2023-24 (ODD Sem)
MID TERM TEST

Q1. e. Why is bytes32 preferred instead of string in Solidity?

In Solidity, which is the programming language used for writing smart contracts on the Ethereum blockchain, the bytes32 type is preferred over the string type for several reasons:

1. **Fixed Size:** bytes32 has a fixed size of 32 bytes, while the length of a string can vary. This fixed size is important for gas efficiency and storage optimization on the Ethereum blockchain. Operations involving fixed-size data are generally more predictable in terms of gas consumption.
2. **Gas Efficiency:** Manipulating bytes32 variables and performing operations on them is more gas-efficient than working with variable-length string types. Gas costs are a critical consideration on the Ethereum platform, as every operation requires a certain amount of gas, which users pay to execute transactions.
3. **EVM Limitations:** Ethereum Virtual Machine (EVM), the runtime environment for executing smart contracts, has limitations on its stack size and gas costs for operations. Using string types could lead to unpredictable and potentially high gas costs due to variable lengths.
4. **Packing Data:** In Solidity, data is often packed to optimize storage and memory usage. With bytes32, you can pack multiple pieces of data into a single bytes32 variable, whereas string types cannot be easily packed due to their variable length.
5. **Comparison and Hashing:** Comparing and hashing fixed-size data like bytes32 is straightforward and gas-efficient. On the other hand, comparing and hashing variable-length string types could be more complex and costly.
6. **Interoperability:** Many operations and libraries in Solidity and the Ethereum ecosystem are designed to work efficiently with fixed-size data types like bytes32. This makes interoperability and integration with other contracts and tools more seamless.

Q1 f. What is SegWit?

Segregated Witness (SegWit) refers to a change in Bitcoin's transaction format where the witness information was removed from the input field of the block. The stated purpose of Segregated Witness is to prevent non-intentional Bitcoin transaction malleability and allow for more transactions to be stored within a block. SegWit was also intended to solve a blockchain size limitation problem that reduced Bitcoin transaction speed. The main benefits of SegWit include:

1. **Increased Transaction Capacity:** By separating the signature data from the transaction data, the block size limit effectively increased, allowing more transactions to fit within a single block. This helped alleviate the network's congestion during periods of high transaction activity.
2. **Fee Reduction:** With more space available in each block, users could include more transactions with lower fees, making it more affordable to send Bitcoin.

3. **Security Improvements:** SegWit also introduced fixes to certain vulnerabilities in the Bitcoin protocol, enhancing the security of the network.
4. **Lightning Network Compatibility:** SegWit was a necessary step for the development and implementation of the Lightning Network, a layer-2 scaling solution that enables fast and low-cost Bitcoin transactions by conducting most transactions off-chain.
5. **Malleability Fix:** SegWit also addressed a transaction malleability issue, which was a quirk in Bitcoin's protocol that allowed third parties to slightly modify transaction IDs without changing the transaction's content. This malleability fix was essential for the development of more complex smart contracts and second-layer solutions like the Lightning Network.

Q2. a. Compare Public, Private and Consortium Blockchain

Public, private, and consortium blockchains are three distinct types of blockchain networks, each with its own characteristics, use cases, and levels of decentralization.

Public Blockchain:

1. Decentralization: Public blockchains are fully decentralized networks that are open to anyone. They are maintained by a distributed network of nodes operated by various individuals and organizations.
2. Accessibility: Anyone can participate in a public blockchain network by becoming a node, mining, or validating transactions. Public blockchains are permissionless, meaning no central entity controls who can join or participate.
3. Examples: Bitcoin, Ethereum, and other similar cryptocurrencies.
4. Use Cases: Public blockchains are commonly used for cryptocurrency transactions, smart contracts, and decentralized applications (DApps) that require a high level of security and transparency.

Private Blockchain:

1. Decentralization: Private blockchains are controlled by a single entity or a consortium of entities. They are not fully decentralized like public blockchains. Access and participation are controlled by the entity that owns and operates the network.
2. Accessibility: Participation in a private blockchain is typically restricted and permissioned. Only approved participants can become nodes, validate transactions, and access the blockchain's data.
3. Examples: Some enterprise use cases and industry-specific applications, such as supply chain management and internal record-keeping systems.
4. Use Cases: Private blockchains are often used by organizations that want to leverage blockchain technology for improved efficiency, security, and transparency within their internal processes or collaborative efforts.

Vivekanand Education Society's Institute of Technology, Chembur, Mumbai,
Department of Computer Engineering
Year : 2023-24 (ODD Sem)
MID TERM TEST

Characteristics	Public Blockchain	Private Blockchain	Consortium Blockchain
Permission Read	Public Class	Could be public or restricted	May be public or restricted
Determination of Consensus	All miners	Only one organization	Designated set of nodes
Efficiency	Low	High	High
Immutability	Impossible to tamper	Could be tampered	Could be tampered
Centralized	No	Yes	Partial
Consensus	Permissionless	Permissioned	Permissioned

Consortium Blockchain:

1. Decentralization: Consortium blockchains are a hybrid between public and private blockchains. They are managed by a consortium or a group of organizations that jointly control the network's operations.
2. Accessibility: Consortium blockchains are permissioned, meaning participants are approved by the consortium members. These participants usually represent organizations with a shared interest in the blockchain's use cases.
3. Examples: R3 Corda and Hyperledger Fabric are examples of consortium blockchain platforms.
4. Use Cases: Consortium blockchains are suitable for scenarios where multiple organizations need to collaborate while maintaining a degree of control and privacy. They are often used in industries like finance, supply chain, and healthcare.

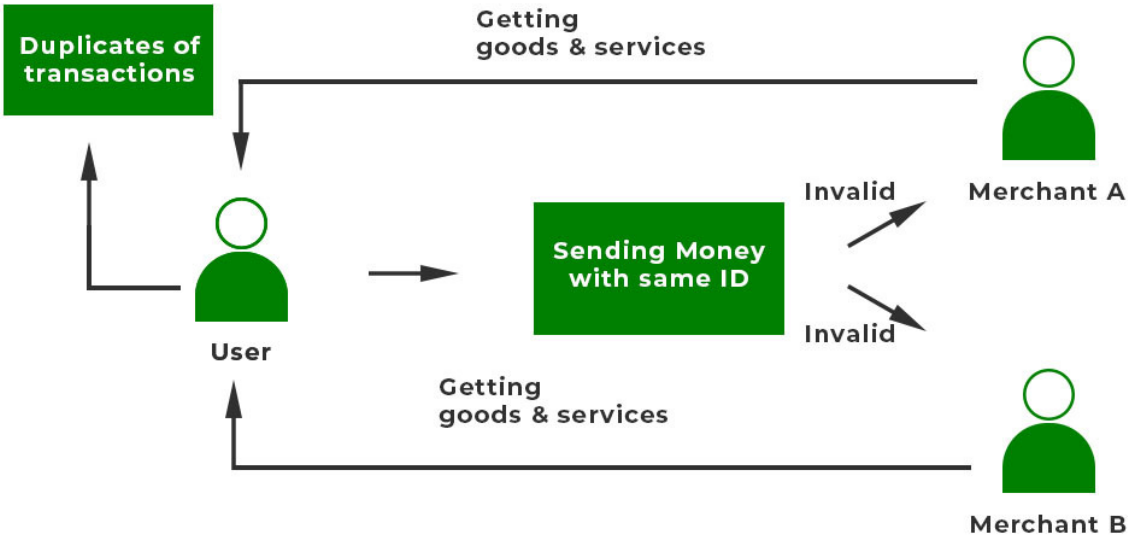
Q2. b. Explain the concept of Double Spending with a suitable example

Double spending means the expenditure of the same digital currency twice or more to avail the multiple services. It is a technical flaw that allows users to duplicate money. Since digital currencies are nothing but files, a malicious user can create multiple copies of the same currency file and can use it in multiple places. This issue can also occur if there is an alteration in the network or copies of the currency are only used and not the original one. There are also double spends that allow hackers to reverse transactions so that transaction happens two times. By doing this, the user loses money two times: one for the fake block

created by the hacker and for the original block as well. The hacker gets incentives as well for the fake blocks that have been mined and confirmed.

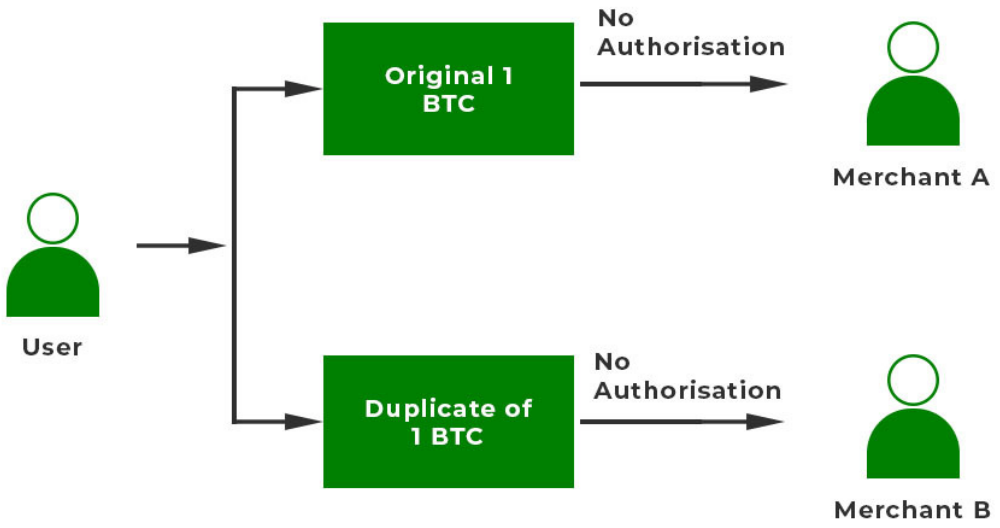
Double spending can never arise physically. It can happen in online transactions. This mostly occurs when there is no authority to verify the transaction. It can also happen if the user's wallet is not secured. Suppose a user wants to avail of services from Merchant 'A' and Merchant 'B'.

1. The user first made a digital transaction with Merchant 'A'.
2. The copy of the cryptocurrency is stored on the user's computer.
3. So the user uses the same cryptocurrency to pay Merchant 'B'
4. Now both the merchants have the illusion that the money has been credited since the transactions were not confirmed by the miners.



Example: Suppose a user has 1 BTC. He/She wants to avail of services from merchant A and merchant B. The user creates multiple copies of the same BTC and stores it. The user first sends the original BTC to Merchant A and gets the service. Simultaneously, the user sends the copied version of 1 BTC to Merchant B. Since the second transaction was not confirmed by other miners, the merchant accepts the bitcoin and sends the service. But the cryptocurrency that was sent is invalid. This is the case of Double Spending.

Vivekanand Education Society's Institute of Technology, Chembur, Mumbai,
Department of Computer Engineering
Year : 2023-24 (ODD Sem)
MID TERM TEST



Types Of Double Spending Attacks

1. Finney Attack: Finney Attack is a type of Double spending Attack. In this, a merchant accepts an unauthorized transaction. The original block is eclipsed by the hacker using an eclipse attack. The transaction is performed on an unauthorized one. After that, the real block shows up and again the transaction is done automatically for the real block. Thus the merchant loses money two times.
2. Race attack: is an attack in which there is a 'race' between two transactions. The attacker sends the same money using different machines to two different merchants. The merchants send their goods but transactions get invalid.
3. 51% Attack: This type of attack is prevalent in small blockchains. Hackers usually take over 51% of the mining power of blockchain and therefore can do anything of their own will.

Bitcoin is one of the most popular blockchains. To combat Double spending it uses some security measures. There are two types of examples of double spending in BTC.

1. The first case is making duplicates of the same bitcoin and sending it to multiple users.
2. The second case is performing the transaction and reversing the already sent transaction after getting the service.

To tackle these double-spending issues, some security measures are taken. They are:

- Validation: Validation of transactions by a maximum number of nodes in the network. Once a block is created, it is added to a list of pending transactions. Users send validation for the block. If the verifications are done then only the block is added to the blockchain.

- Timestamp: The confirmed transactions are timestamped, therefore they are irreversible. If a transaction is involved with a bitcoin it is verified and done. But in the future, if other transactions are made with the same bitcoin, the transactions will be canceled.
- Block Confirmations: Merchants get block confirmations so that they are assured that there was no case of double spending. In bitcoin, a minimum of 6 confirmations are done.
- Saving copies: A copy of each transaction is kept at each node so in case of network failure the whole network does not go down.

These security features have reduced double spending to a large extent. There are many disadvantages of blockchain concerning Double Spending:

- Control of the blockchain: The biggest disadvantage is if the hackers manage to take control of 51% computation power, they can do any transaction of their own will and can steal other users' money. Therefore there is a threat to security as millions and millions of money are involved in transactions.
- Alteration of information: Transaction information can also be altered by hackers. They can mine blocks and hide the original blocks using attacks like Eclipse attack, Finney Attack, etc.
- No authority: The third major problem is no central authority is present to verify the transactions. But these problems will be eliminated if companies take proper security measures and users are also aware of the measures.

Q3. a. Explain the process of adding transactions in the Blockchain

The process of adding transactions to a blockchain can vary depending on the specific consensus algorithm and blockchain architecture being used. However, in general, the process involves several key steps:

1. **Transaction Creation:** A user initiates a transaction by creating a transaction request, specifying the sender's address, the recipient's address, and the amount of cryptocurrency or other data being transferred.
2. **Transaction Propagation:** The transaction is then propagated through the peer-to-peer network of nodes that make up the blockchain network. Each node receives the transaction and verifies its validity, typically by checking the transaction format, digital signatures, and other relevant transaction details.
3. **Transaction Verification:** Miners or validators in the blockchain network then verify the transaction. This verification process typically involves checking the transaction against a set of predefined rules or consensus rules, which may vary depending on the blockchain's specific protocol. For example, in a Proof of Work (PoW) blockchain, miners may need to solve a complex mathematical puzzle to validate the transaction.

4. **Transaction Inclusion in a Block:** Once the transaction is verified, it is included in a block. A block is a group of transactions that are bundled together and cryptographically linked to the previous block in the blockchain, forming a chain of blocks. The process of adding a transaction to a block may involve adding a transaction record to the block's data structure, updating the block's header, and recalculating the block's hash value.
5. **Block Propagation and Consensus:** The validated block containing the transaction is then propagated through the network of nodes, and the consensus algorithm used in the blockchain determines which miner or validator gets to add the block to the blockchain. This process may involve additional verification and consensus steps, depending on the specific consensus algorithm being used.
6. **Block Confirmation:** Once the block is added to the blockchain and the consensus is reached, the transaction is considered confirmed. The confirmation process provides assurance that the transaction is immutable and cannot be altered without consensus from the network.
7. **Transaction Finality:** As more blocks are added to the blockchain, the transaction becomes increasingly secure and final. In most blockchains, a transaction is considered final after it has been confirmed by a certain number of subsequent blocks, which varies depending on the blockchain's confirmation time and security requirements.

It's important to note that the exact process of adding transactions to a blockchain can vary depending on the specific blockchain implementation, consensus algorithm, and other factors. Different blockchains may have different transaction fees, confirmation times, and security measures. Additionally, the process of adding transactions to a blockchain may evolve over time as blockchain technology continues to develop and mature

Q3 . b Differentiate between PoW, PoS, PoB & PoET

PoW, PoS, PoB, and PoET are different consensus algorithms used in blockchain networks to achieve agreement on the state of the blockchain. Here's a brief overview of each:

1. Proof of Work (PoW): PoW is the original and most widely used consensus algorithm, used in blockchains like Bitcoin and Ethereum. In PoW, miners compete to solve complex mathematical puzzles, and the first miner to solve the puzzle gets to validate the next block of transactions and is rewarded with new cryptocurrency. PoW requires significant computational power and energy consumption to secure the network, and the miner with the most computational power (hash rate) has a higher chance of winning the block validation.
2. Proof of Stake (PoS): PoS is a consensus algorithm used in blockchains like Cardano and Tezos. In PoS, instead of miners competing with computational power, validators (often referred to as "stakers") are chosen to validate blocks based on the amount of

cryptocurrency they "stake" or lock up as collateral. Validators are selected randomly or based on their stake, and they validate transactions and create new blocks. PoS typically requires less computational power and energy compared to PoW, as the block validation process is based on ownership of cryptocurrency rather than computational work.

3. Proof of Burn (PoB): PoB is a consensus algorithm used in some lesser-known blockchains. In PoB, users prove ownership of a certain amount of cryptocurrency by "burning" or destroying a certain amount of that cryptocurrency, making it unspendable. The users who burn the most cryptocurrency are selected to validate blocks and are rewarded with transaction fees or newly created cryptocurrency.
4. Proof of Elapsed Time (PoET): PoET is a consensus algorithm used in the Hyperledger Sawtooth blockchain. In PoET, validators are selected to create blocks based on a randomized lottery, but instead of using computational power or cryptocurrency ownership as a basis for selection, validators "wait" for a certain amount of time, and the first validator to finish waiting gets to create the next block. PoET aims to be more energy-efficient compared to PoW and PoS, as it does not require high computational power or cryptocurrency ownership.

Proof of work (PoW)	Proof of stake (PoS) [11]	Proof of Burn (PoB)	PoET
Used for industries working on financial level	Used for industries working on financial level	Used for industries working on financial level	Used for industries working on financial level
Using public key encryption (i.e. Bitcoin)	Using RSA algorithm for encryption	RSA algorithm for encryption	RSA algorithm for encryption
Miners having higher work done after investing higher power will have higher probability to mine the new block	It is some election type selection of miners for next block to be mined	PoB acquires some cryptocurrencies (wealth) to mine new block using virtual resource	Person spends some time and power to mine new block who finishes first the prior task will be the next miner
Power inefficient	Power efficient	Power efficient	Power efficient
Open environment	Open environment	Open environment	Open environment
Bitcoin script is used	Mostly Golong is used	Mostly Golong is used	

++++++++++++++++++++++**Happy Learning!!!**++++++++++++++++++++++