Sipna College of Engineering & Technology, Amravati.
Department of Computer Science & Engineering
Session 2022-2023

Branch :- Computer Sci. & Engg. **Class :- Final Year**
Subject :-Block Chain Fundamentals Lab manual **Sem :- VII**
Teacher Manual

PRACTICAL NO 9

AIM: To learn about Blockchain and its three pillars that are decentralization, transparency & immutability by using simulator

S/W REQUIRED: Virtual lab

A blockchain is basically a living list of records, called as "blocks". These blocks are connected to each other by the diverse cryptographic mechanisms. In the category of data structures, this can be related to the concept of a Linked List. In Blockchain, the initial block is known as the "Genesis Block". This naming convention is basically a major commendation to Satoshi Nakamoto. The domain of crypto-currency was pioneered by a bogus naming convention. It can be related to a random scenario of a person or a group of persons, represented by a peculiar name "Satoshi Nakamoto". In the year 2008, for the purpose of Bitcoin this name was utilized. The technology that was used behind the Bitcoin spectrum was "Block-Chain". Initially the structure of a block has basically 3 components namely data, hash of current block and hash of previous block. As an illustration in general, the concept of block-chain can be depicted with "m" blocks forming a chain where m can be any random positive integer.

Three pillars of blockchain

- Decenttralization

  The true meaning of decentralization is not having a central unit. Now if we take this concept in Blockchain it means that blockchain is autonomous and does not have a central governing unit.

- Transparency

  Transparency in real life means something with zero opacity. Now if we take this concept in Blockchain, it means that blockchain has zero privacy to be exact when we talk about transactions, all the transactions are public and can be viewed by anyone on the network.

- Immutability
  Here immutable means exactly what the word means in any real life i.e. something that cannnot be altered. So when we talk about blockchain it means that once a transaction is pushed into blockchain it cannot be altered.

Functioning of Blockchain Technology

Decentralization, Transparency, Immutability are the three pillars of blockchain technology. Efficiency as well as cost can be optimised using this approach. The use as well as request of softwares or applications that are made on blockchain architecture will only advance. A hash can be compared with a fingerprint (that is totally unique). A very popular cryptographic approach that is Secure Hash Algorithm (256) is used to formulate the hash value. Hash Value is basically the amalgamation of the numeric and the alphabetical data. This generation of hash is the primitive approach to understand blockchain. At that instant,when a block is generated, a hash has been produced for the same, and if any change has been done in the block, it will certainly affect the hash value too. With the mechanism of hashing, the changes are easily identified.

The ultimate verdict within the block is the hash value from a predecessor. Fortunately, by the means of this a chain of blocks is created that is the strategy behind blockchain's architecture.

Procedure

Steps of simulator

1. First complete the recall task as per the instructions given on the page.Then click on next button on the top of the page.
2. To Understand the concept of open ledger, Enter the Name and Amount of the sender as well as the recipient in the placeholder.
3. Click on the Submit button to complete the details of a particular user. Complete the same process for the next user.
4. In the canvas section, the illustration will take place according to the inputs given by the user.
5. Click on the Next Experiment button to proceed further.
6. The next section is of Distributed ledger where the concept of decentralization is implemented.
7. Click on the desired block in the ledger, then click on the desired user where you need to place that block.
8. The same process is done for the next two users.
9. Click on the validate button to validate your transaction.
10. The next concept is of immutability, where the user wil click on the toggle button, to display or delete a block.
11. Click on the validate button to complete the concept of Immutability.

Output:

CONCLUSION: Thus we have gained knowledge about Blockchain and its three pillars that are decentralization, transparency & immutability by using simulator

Sipna College of Engineering & Technology, Amravati.
Department of Computer Science & Engineering
Session 2022-2023

Branch :- Computer Sci. & Engg. **Class :- Final Year**
Subject :-Block Chain Fundamentals Lab manual **Sem :- VII**

Teacher Manual

PRACTICAL NO 10

AIM: To learn about mining in blockchain i.e. how a transaction is validated and added into a blockchain through simulator.

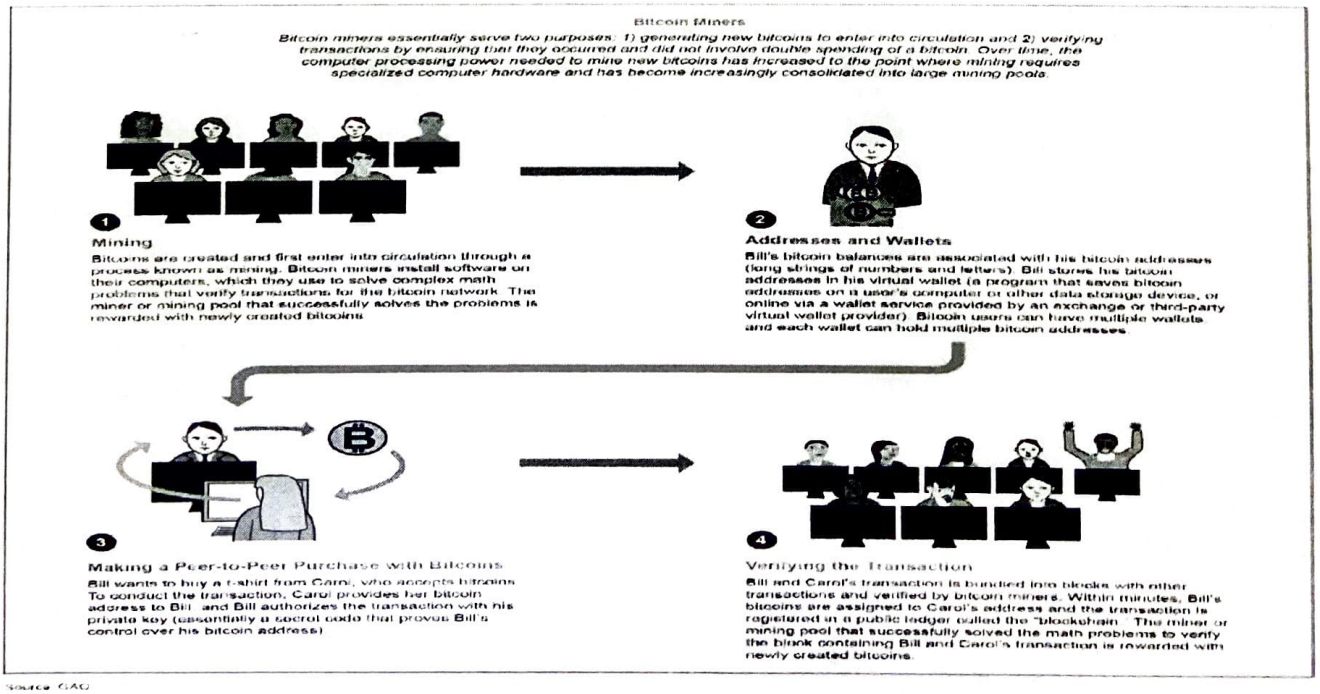
S/W REQUIRED: Virtual lab

Blockchain Technology

A blockchain is basically a living list of records, called as "blocks". These blocks are connected to each other by the diverse cryptographic mechanisms. In the category of data structures, this can be related to the concept of a Linked List. In Blockchain, the initial block is known as the "Genesis Block". This naming convention is basically a major commendation to Satoshi Nakamoto. The domain of crypto-currency was pioneered by a bogus naming convention. It can be related to a random scenario of a person or a group of persons, represented by a peculiar name "Satoshi Nakamoto". In the year 2008, for the purpose of Bitcoin this name was utilized. The technology that was used behind the Bitcoin spectrum was "Block-Chain". Initially the structure of a block has basically 3 components namely data, hash of current block and hash of previous block.

Mining

In terms of the block chain domain, mining is the procedure of appending transactions to an enormous distributed ledger of extant transactions. This concept is well suited for the bitcoin approach but the diverse technologies that uses the block chain approach can also perform the approach of mining as well. It allows the creation of a hash for a block of transactions that cannot be changed easily protecting the integrity approach of the block chain. The concept of mining goes really well with the other two approaches that are open ledger and distributed ledger.



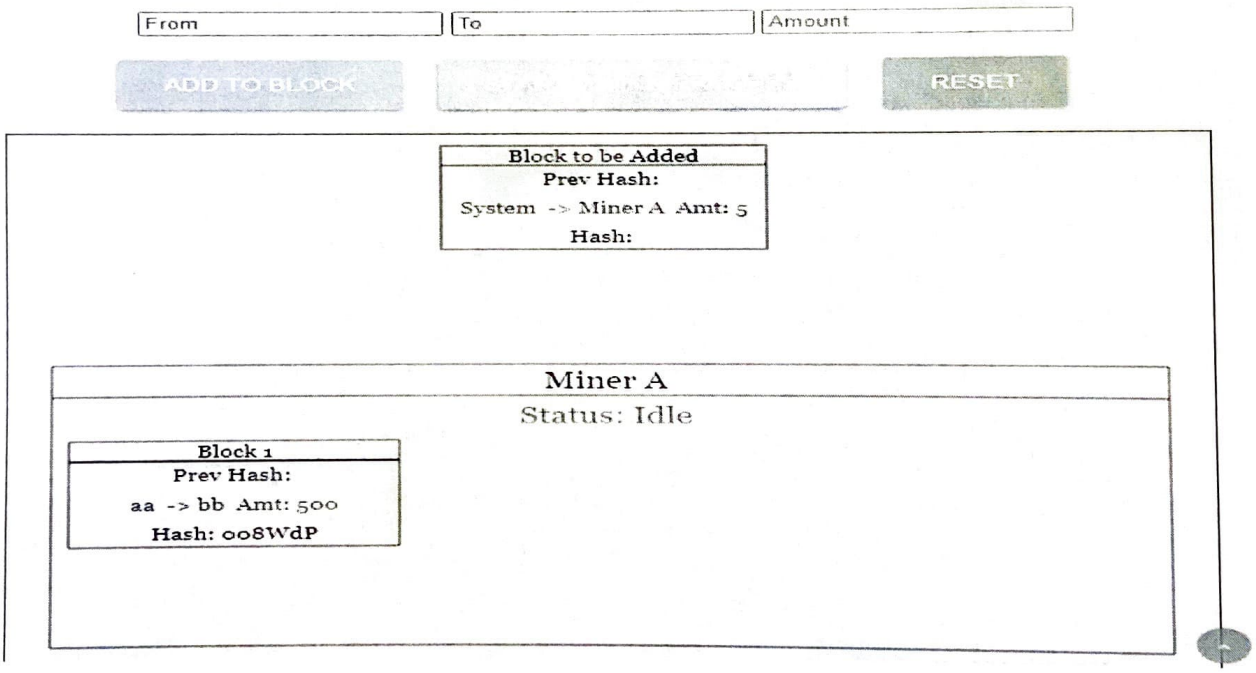
Source: GAO

Procedure

Steps of simulator

- Start with the task regarding concept of mining.(If previously known, otherwise skip)
- Match the following with the correct answer.
- Select the first block on left side(Step number).
- Now, select the block in right in such a way that it is the correct position on left.
- Do the same procedure for the rest of the steps.
- Now, after you've done matching click on "VALIDATE" button.
- If all the answers are correct,then a popup will appear saying "Valid!".
- If popup shows "Not Valid!" then reset the test by cicking on "RESET" button to restart the test.
- Now click on initiate mining process to go to the next part.
- Enter the Name and Amount (Cryptocurrency) of the sender as well as the recipient in the placeholder.
- Click on the 'Add to block' button to complete the details of a particular user. As soon as the button is clicked, the details will get added to the block.
- The illustration will take place according to the inputs given by the user.
- Complete the same process for the next user.
- Click on the start mining process button, to start the mining process.
- Click on the reset button to reset all the details that were entered by the user.
- The instruction pane will also be there to make the user understand about the basic process that is happening in the simulator.

Output:



CONCLUSION: Thus we have gained knowledge of how mining is been performed in blockchain.

Sipna College of Engineering & Technology, Amravati.
Department of Computer Science & Engineering
Session 2022-2023

Branch :- Computer Sci. & Engg. **Class :- Final Year**
Subject :-Block Chain Fundamentals Lab manual **Sem :- VII**

Teacher Manual

PRACTICAL NO 11

AIM: To learn Proof of Work (PoW) & Proof of Stake (PoS) by using simulator

S/W REQUIRED: Virtual lab

Consensus Mechanism

A consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies. It is useful in record-keeping, among other things.

Consensus Model

This model basically deals with the soundness as well as safety of the blockchain. The primitive condition to be followed for this is to be consistent across the shared state. Consensus is a vital approach because without a medial power, the users must follow the protocols and how to solicit them.

Mining

In terms of the block chain domain, mining is the procedure of appending transactions to an enormous distributed ledger of extant transactions. This concept is well suited for the bitcoin approach but the diverse technologies that uses the blockchain approach can also perform the approach of mining as well. It allows the creation of a hash for a block of transactions that cannot be changed easily protecting the integrity approach of the block chain. The concept of mining goes really well with the other two approaches that are open ledger and distributed ledger.

Proof of Work

This consensus algorithmic rule deals with the prevention of raw facts & figures, in blocks from tampering. By this mechanism, the blocks can be appended into a chain in a perpetual manner. Hashing as well as linking are the domains of safety in blockchain. A brief idea, of the hashing algorithmic rules have been understood by the user in the previous experiment (experiment no.2). For appending the blocks in the blockchain, the miners are provided with some tricky mathematical puzzles. The first miner to solve the puzzle, gets a reward that is based on some policy. One must understand that there should be enough computational power to solve that tricky mathematical puzzle. After the solving of the puzzle, the blocks get added to chain thus forming blockchain.

Proof of work is a consensus algorithm in blockchain technology. In Blockchain, miners use this algorithm to confirm transactions and create new blocks in the blockchain. With proof of work, miners try and compete against others to confirm the transaction in less time to get rewarded. For that miners have to solve a complex mathematical puzzle. Bitcoin is the most famous application of proof of work. In Blockchain it takes 10 minutes for the creation of Blockchain.

Proof of Stake

It is an alternative measure to the proof of Work (Pow). To achieve the objective of the distributed consensus this algorithmic rule can be used. In this mechanism, also the validation of blocks takes place. Pos is somehow, less risky in comparison to the other protocol mentioned. Everything under this mechanism, holds a principle that "Proportions of Coins held by the miner".It is an alternative measure to the proof of Work (Pow). To achieve the objective of the distributed consensus this algorithmic rule can be used. In this mechanism, also the validation of blocks takes place. Pos is somehow, less risky in comparison to the other

protocol mentioned. Everything under this mechanism, holds a principle that "Proportions of Coins held by the miner".

The proof of stake (PoS) seeks to address this issue by attributing mining power to the proportion of coins held by a miner. This way, instead of utilizing energy to answer PoW puzzles, a PoS miner is limited to mining a percentage of transactions that is reflective of his or her ownership stake.With a PoS, the attacker would need to obtain 51% of the cryptocurrency to carry out a 51% attack. The Proof of Stake avoids this by making it disadvantageous for a miner with a 51% stake in a cryptocurrency to attack the network.

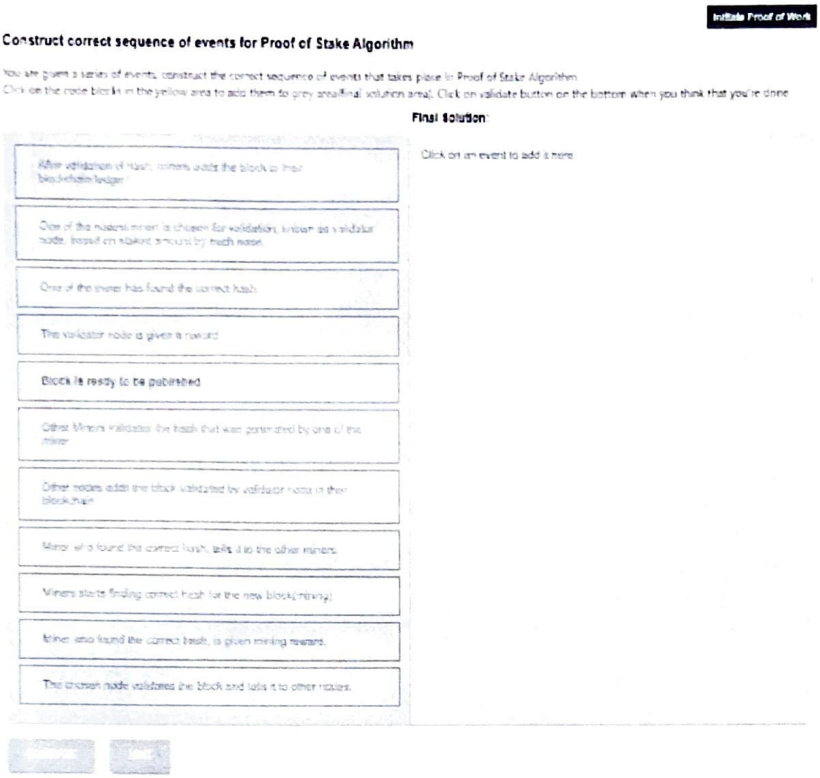
Procedure

Steps of simulator

1. Start with the task regarding concept of Proof of Work.
2. Click on the block to add it into the final solution block.
3. After adding all the blocks correctly as per the instructions, click on validate button.
4. Click in the hint button to get the hint of the wrong question if any and repeat the above process to get all the right answers.
5. Now click on the "Initiate proof of stake task" button to start task regarding concept of Proof of Stake.
6. Click on the block to add it into the final solution block.
7. After adding all the blocks correctly as per the instructions, click on validate button.
8. Click in the hint button to get the hint of the wrong question if any and repeat the above process to get all the right answers.
9. Now click on the "Initiate Proof of Work" button to move on to the PoW page.
10. To Understand the concept of proof of work, Enter the Name and Amount (Cryptocurrency) of the sender as well as the recipient in the placeholder.
11. Click on the 'Add to block' button to complete the details of a particular user. As soon as the button is clicked, the details will get added to the block.
12. Complete the same process for the next user.
13. Now enter the name of the miner to be added.
14. Click on the 'Add Miner' button to add the miner.
15. Complete the same process to add more miners to the block.
16. Click on the start mining process button, to start the mining process.
17. Click on the reset button to reset all the details that were entered by the user.
18. Now click on the "Initiate Proof of Stake" button to move on to the PoS page.

Output:

Simulation



CONCLUSION: Thus we have gained knowledge of Proof of Work (PoW) & Proof of Stake (PoS) by using simulator