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.

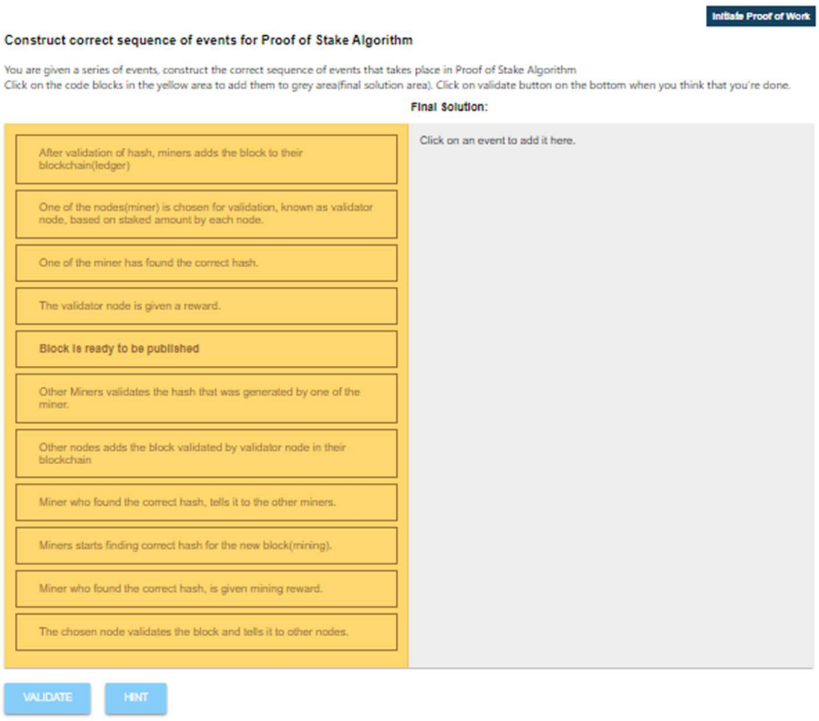
Procedure

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