DISTRIBUTED LEDGER IN BLOCKCHAIN TECHNOLOGY

Abstract

Distributed Ledger Technology (DLT) forms the cornerstone of blockchain systems, introducing a paradigm shift in data management, transparency, and security. This abstract provides a concise overview of the fundamental aspects of DLT within the context of blockchain technology, elucidating its key principles and applications.DLT is a decentralized and distributed database architecture that facilitates the secure and transparent recording of transactions across a network of nodes. By decentralizing control and consensus mechanisms, DLT mitigates single points of failure and enhances the robustness of data storage and verification.

Keywords: Distributed Ledger Technology (DLT), Consensus mechanisms, Robustness.

Authors

Shaik Mulla Almas
Assistant Professor
Department of Information Technology
Vasireddy Venkatadri Institute of Technology
Nambur, Andhra Pradesh, India.
mulla.almas@gmail.com

Pathan Mahamood Khan
Assistant Professor
Department of Electrical and Electronics Engineering
Vasireddy Venkatadri Institute of Technology
Nambur, Andhra Pradesh, India.
pathanmehemudkhan@gmail.com

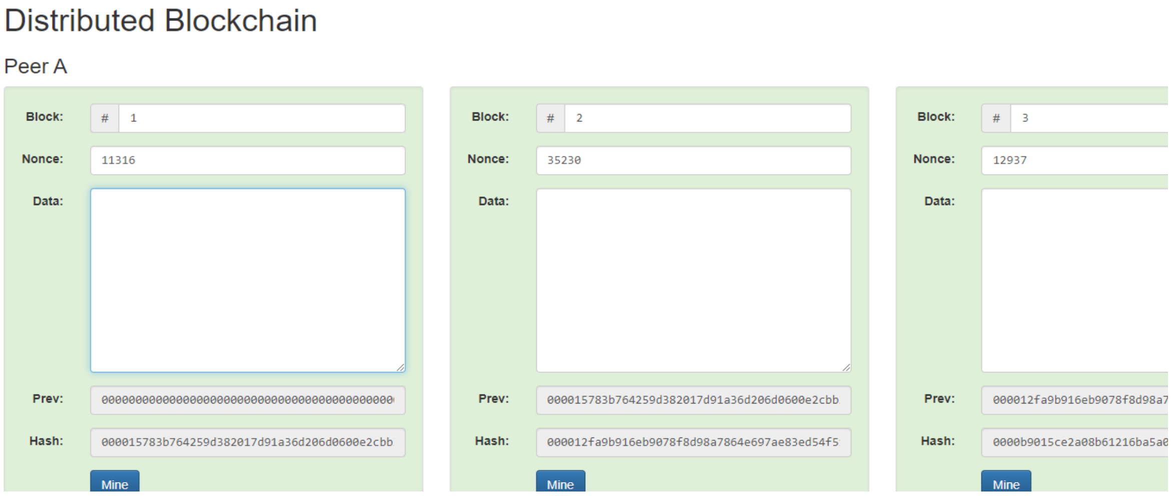
Dr. K. Kavitha
Associate Professor
Department of Computer Science Engineering
Annamalai University
Chidambaram, Tamil Nadu, India.
kavithacseau@gmail.com
.

I. DISTRIBUTED LEDGER

Distributed Ledger is databases that store the copy of all transactions that have happened. Every single person in the Blockchain network has a copy of the ledger.

Working of Distributed Ledger: Steps to perform

- Visithttps://andersbrownworth.com/blockchain/distributed
- Note the hash value of Node1 peer A
- Enter data in the data field of Peer A, click mine and note the hash value.
- Enter data and mine the other blocks of Peer A.
- Verify if the hash of the previous block is the same in the next block.
- All the peer nodes will have the same copy of blocks as shown in the figure 1, figure 2.



Distributed Blockchain

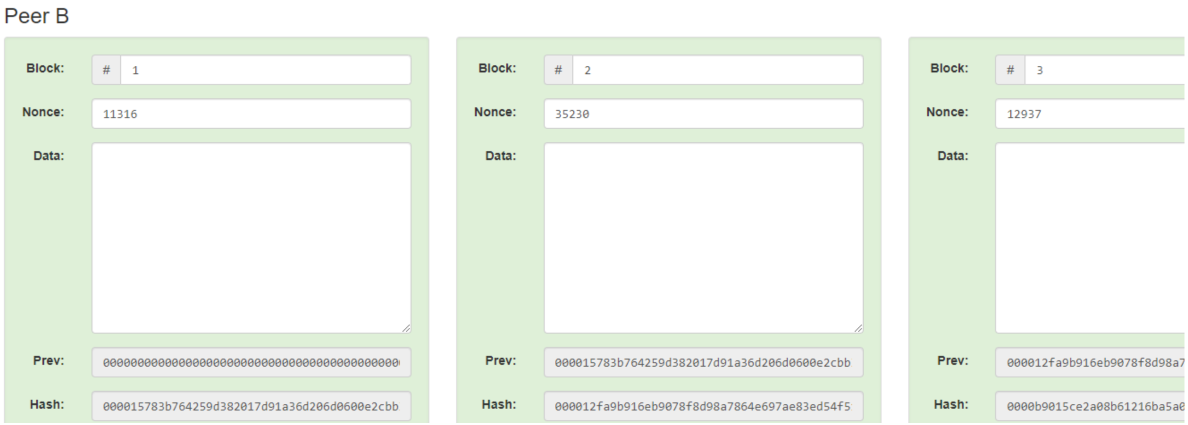
Peer A

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cbb
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7
Hash: 0000b9015ce2a08b61216ba5a0

Figure 1



Peer B

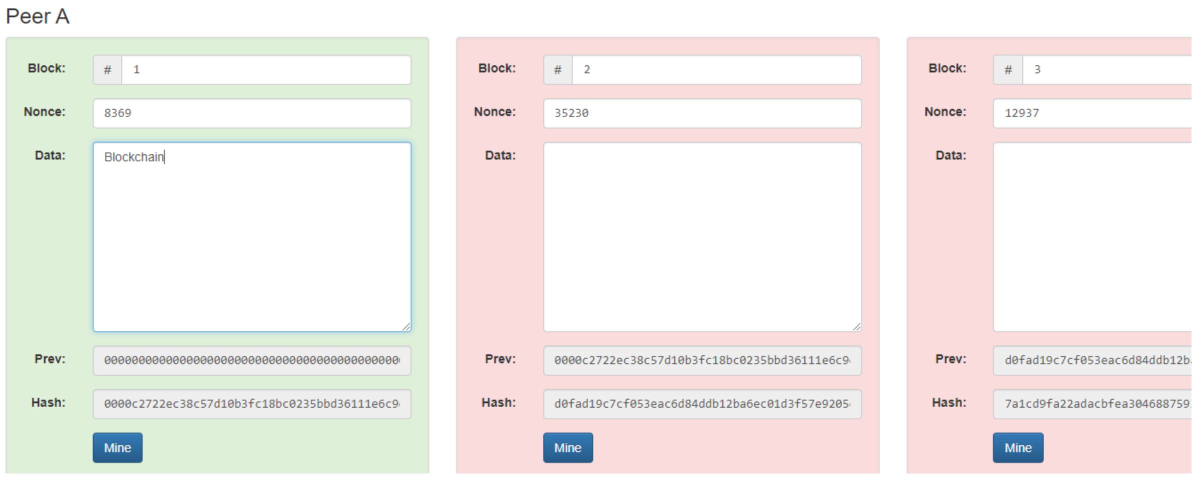
Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cbb
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7
Hash: 0000b9015ce2a08b61216ba5a0

Figure 2

Once after entering the data value in the data field and clicking mine the hash value is changed in the current block and in the next block also. Shown in figure 3



Peer A

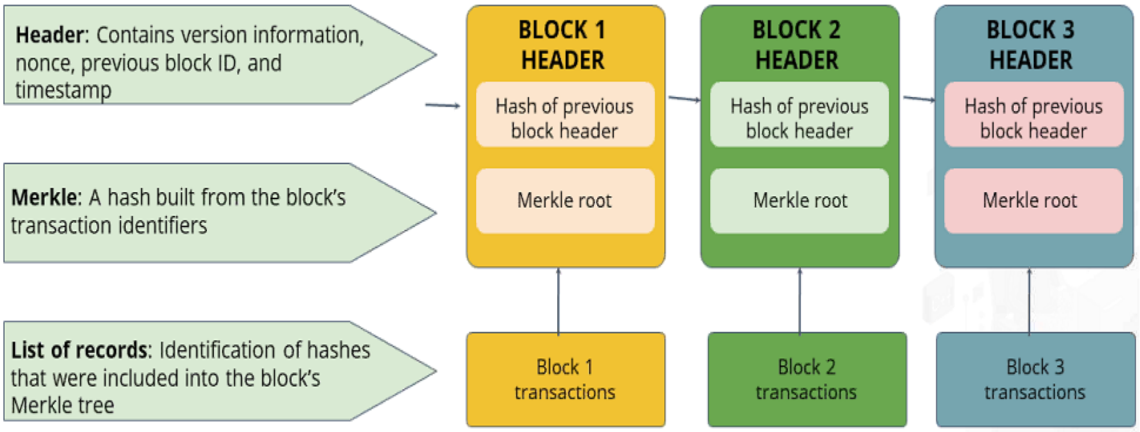
Block: # 1
Nonce: 8369
Data: Blockchain
Prev: 0000000000000000000000000000000000000000000
Hash: 0000c2722ec38c57d10b3fc18bc0235bbd36111e6c9

Block: # 2
Nonce: 35230
Data:
Prev: 0000c2722ec38c57d10b3fc18bc0235bbd36111e6c9
Hash: d0fad19c7cf053eac6d84ddb12ba6ec01d3f57e9205

Block: # 3
Nonce: 12937
Data:
Prev: d0fad19c7cf053eac6d84ddb12b
Hash: 7a1cd9fa22adacbfea304688759

Figure 3

1. **Block Structure:** Block in Blockchain is made up of two parts: Block Header, Block Body.



Header: Contains version information, nonce, previous block ID, and timestamp
Merkle: A hash built from the block's transaction identifiers
List of records: Identification of hashes that were included into the block's Merkle tree
BLOCK 1 HEADER
Hash of previous block header
Merkle root
Block 1 transactions
BLOCK 2 HEADER
Hash of previous block header
Merkle root
Block 2 transactions
BLOCK 3 HEADER
Hash of previous block header
Merkle root
Block 3 transactions

Figure 4

2. **Block Header:** Block header consist of the critical terms as shown in the figure:5

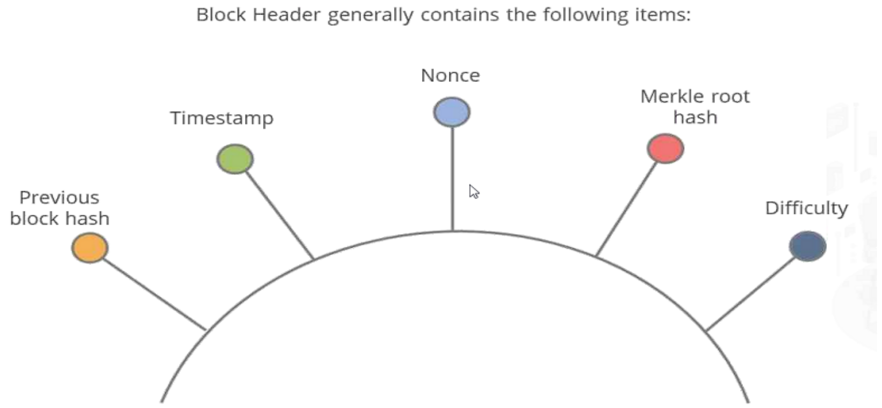


Figure 5: Block Header Description

3. **Previous Block Hash**: Hash value of a previous block is stored in the current block.

   - **Timestamp**: The time when the block is created is called as timestamp of a block.

   - **Difficulty Target**: Consider if person A performs some transaction with person B, that transaction generates Hash Value. After hash value is been generated, if the prefix of the hash value is 0's,that indicates the difficulty level for mining a block. The number of 0's in the prefix tells us that the difficulty level of the network. Every node in the network will solve the puzzle; the puzzle is to get the 0's in the prefix of the Hash Value.

   - **Nonce**: The random number which generates 0's at the prefix of the hash values are called Nonce.

   Once this is done by the node, the proof will be submitted to the network and node will be eligible to mine the particular records and add new block to the Blockchain network. There is a possibility that network may increase or decrease difficulty target. For example, consider time taken to mine a block is 10 minutes, if one of the block in a network is been mined within 8 minutes then difficulty target level will be increased. In the same way if the time taken for a block to get mined is 12 minutes the difficulty target level of the network is decreased. This is not done by anyone explicitly, the software is designed in such a way.

4. **Merkle Root Hash (MRH):** Merkle root Hash shows how the transactions are stored in the blockchain. If we consider hash values of Transactions a, b, c, d as Ha, Hb, Hc, Hd respectively. The below figure shows how they are paired up with each other to form a Merkle root hash Habcd.

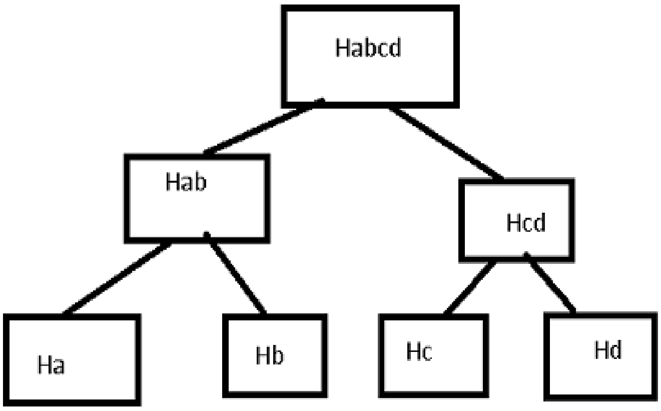


Figure 6: Merkle Root Hash

5. **Block Body:** Block body consists of a list of transactions in the block. The point to be remembered here is no benchmark exists here for the number of transactions a block contains. Sometime a block can contain 100 transactions, sometimes 1000 transactions which depend upon the traffic going on in the block chain network and how many transactions miner has taken.

6. **Block Transactions:** Consider Joe wants to transfer money or one bit coin to the mark , once it is transferred, the transaction is stored to the block that is to the new block which is created and is been broadcasted to the network. If the transaction gets approved by 51% of the nodes in the network, then the block is added to the block chain and the transaction will be done successfully to mark.

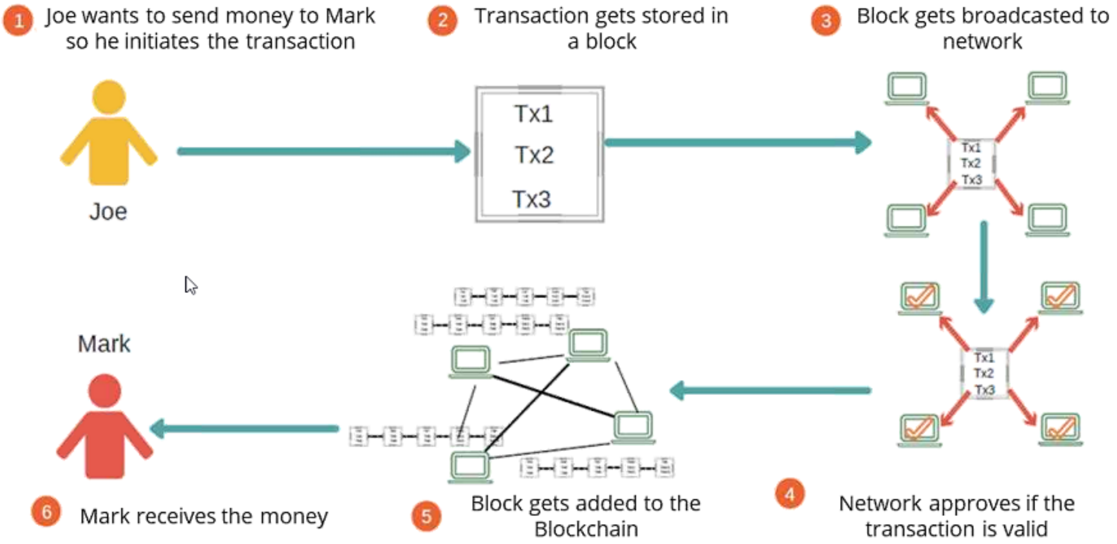
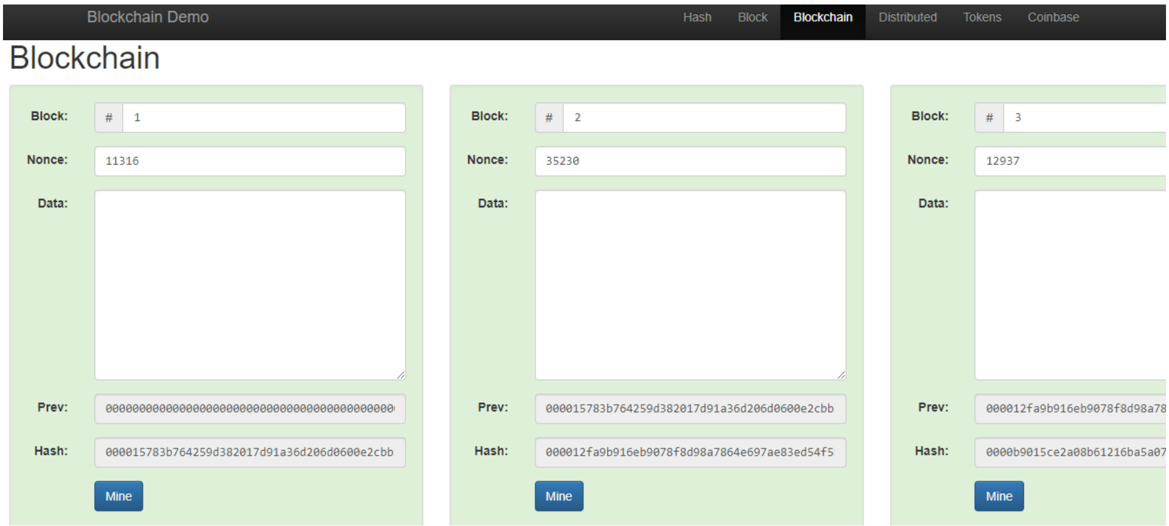

1 Joe wants to send money to Mark so he initiates the transaction
2 Transaction gets stored in a block
3 Block gets broadcasted to network
Joe
Tx1
Tx2
Tx3
Tx1
Tx2
Tx3
Tx1
Tx2
Tx3
Mark
6 Mark receives the money
5 Block gets added to the Blockchain
4 Network approves if the transaction is valid

Figure 7: Block Transactions

7. **Working of Blockchain Transaction:** Below is the example showing the working of block chain transaction where the initial block is known as Genesis block. The previous hash value of this genesis block is all 0’s because it is the first block and no other block is there previous to it. The hash value of this block is fed to the next block as shown in the figure 8.The hash algorithm that is used is SHA 256 algorithm.



Blockchain

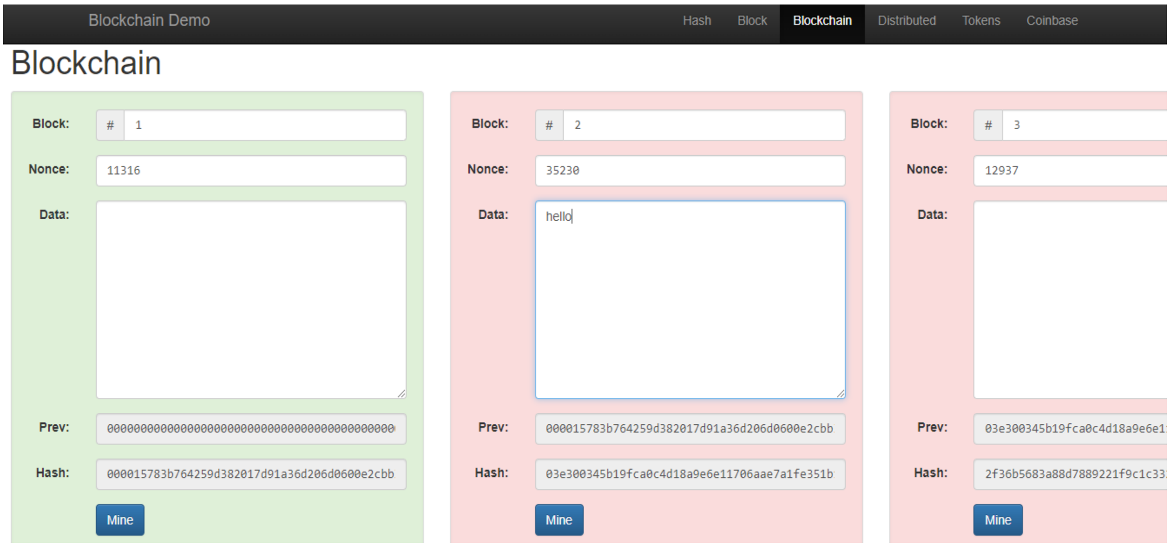
Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb
Mine

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cbb
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5
Mine

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a78
Hash: 0000b9015ce2a08b61216ba5a07
Mine

Figure 8

As blockchain is an immutable. If any hacker tries to update the transactions in the block, it is clearly identified as blocks which are affected will be turned into pink colour as shown in figure 9



Blockchain

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb

Block: # 2
Nonce: 35230
Data: hello
Prev: 000015783b764259d382017d91a36d206d0600e2cbb
Hash: 03e300345b19fca0c4d18a9e6e11706aae7a1fe351b

Block: # 3
Nonce: 12937
Data:
Prev: 03e300345b19fca0c4d18a9e6e1
Hash: 2f36b5683a88d7889221f9c1c33

Figure 9: Immutable Block chain

II. CONSENSUS MECHANISM

1. Objectives of Blockchain Consensus Model:

- **Coming to an Agreement:** This is a mechanism that gathers all the agreements from the group as much as it can.
  Example:

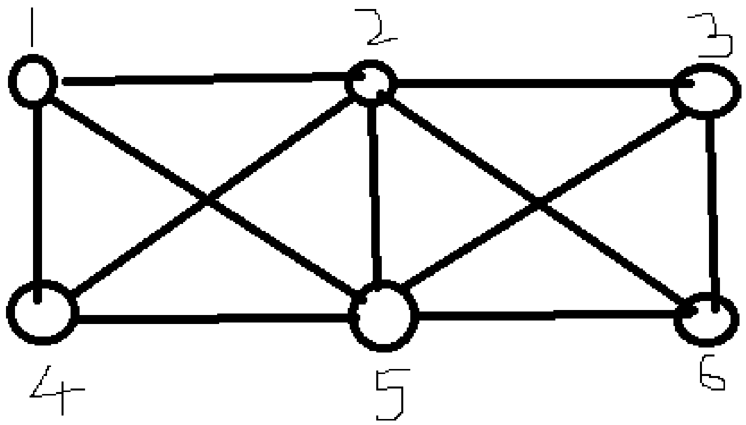


Figure10: Connectivity of Nodes in Blockchain

Suppose in the above diagram node-3 confirms a transaction, this means that every other node should accept that node-3 has been ethically mined in a particular transaction. This is the conclusion that we come through.

- **Collaboration:** Every one of the groups aims towards a better agreement that results in the groups "Interest as a whole. That is everyone cooperates with the other node without any competition.

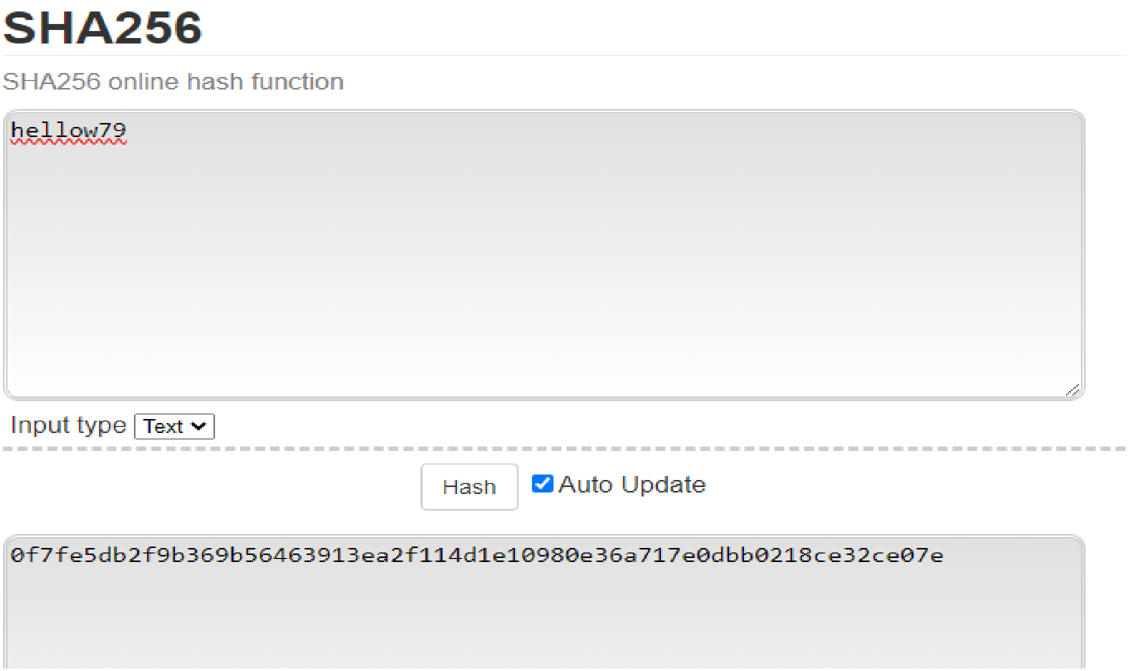
- **Co-operation:** Other nodes will not think of benefits in collaboratively working together.

- **Equal Rights:** Every single participant has the same value in voting. This means that every person's vote is important. There is nothing like master and slave.

- **Participation:** Everyone inside the network needs to participate in the voting. No one will be left out or can stay out without a vote.

- **Activity:** Every member of the group is equally active. There is no one with more responsibility in the group.

- **Proof of Work Consensus Algorithm:** Proof of work is used to validate whether the user has put enough effort (such as computing power) or done some work for solving a mathematical problem of a given complexity before sending the request. Go to any online SHA-256 calculator tool and tr using a random number with the text "Hello World". If the difficulty target is set as the hash value starting with one zero, you could see that the random number 10 results in the hash value starting with zero.



SHA256

SHA256 online hash function

```
hellow79
```

Input type Text

```
0f7fe5db2f9b369b56463913ea2f114d1e10980e36a717e0dbb0218ce32ce07e
```

Figure 11: Difficulty Target Level

Nonce value is hellow79 to get the prefix of hash value to get single zero.

III. ADVANTAGES OF POW

1. **Security and Immutability:** PoW is noted for its high level of security and immutability. An attacker would need to possess the majority of the network's processing power to edit a transaction or alter the block chain’s history, which gets increasingly difficult as the network expands. As a result, the block chain is immune to tampering and has a high degree of immutability.

2. **Proven Track Record:** PoW has been proven to be effective for more than a decade, particularly in the instance of Bitcoin. Its security and dependability have withstood the test of time, increasing faith in the system.

3. **Resistance to Sybil Attack:** PoW requires users to contribute real-world resources in the mining process, such as energy and hardware. This makes it difficult for a single entity to produce a large number of bogus identities and assault the network (Sybil attacks).

4. **Proven Security Model:** Over the years, the concept of PoW has been thoroughly investigated and modified, leading to a greater understanding of its security implications.

IV. DIS-ADVANTAGES OF POW

1. **Energy Consumption:** To validate transactions, PoW players, known as miners, must solve hard mathematical puzzles. This method is computationally demanding and requires a lot of energy. As a result, PoW-based cryptocurrencies such as Bitcoin have come under fire for their large carbon footprint and environmental impact.

2. **Centralization of Mining Power:** PoW mining has become increasingly competitive and resource-intensive over time. As a result, mining power has been concentrated in the hands of a few major mining pools or corporations that can pay the requisite gear and energy expenditures. This centralized approach contradicts the decentralized nature of blockchain technology.

3. **Hardware and Energy Costs:** PoW mining necessitates the use of specialized hardware such as powerful graphics cards or ASICs (Application-Specific Integrated Circuits). Individuals who do not have the financial capacity to invest in such equipment and infrastructure face a barrier to entry.

4. **Lack of Upgrade Mechanism:** Because of the decentralized nature of the network, changing the consensus method or protocol of a PoW blockchain might be difficult. This can make it difficult to carry out necessary modifications or improvements.