**K. J. Somaiya College of Engineering, Mumbai-77**

**Department of Computer Engineering**

| | |
|---|---|
| **Batch: BCT-1** | **Roll No.: 1911031** |
| **Experiment No. 01** | |

**Title: Block chain Demo**

**Objective:** To explore the contents of blocks in a blockchain, get insights into the working of blockchain using online blockchain creation platforms and also access the test networks.

**Expected Outcome of Experiment:**

| CO | Outcome |
|---|---|
| CO1 | **Build your own Block chain businesses with acquired knowledge** |

**Books/ Journals/ Websites referred:**

1. **https://www.blockchain.com/explorer**
2. **https://www.blockchain.com/**
3. **https://etherscan.io/**
4. **https://www.ibm.com/in-en/topics/what-is-blockchain**
5. **https://en.wikipedia.org/wiki/Blockchain**

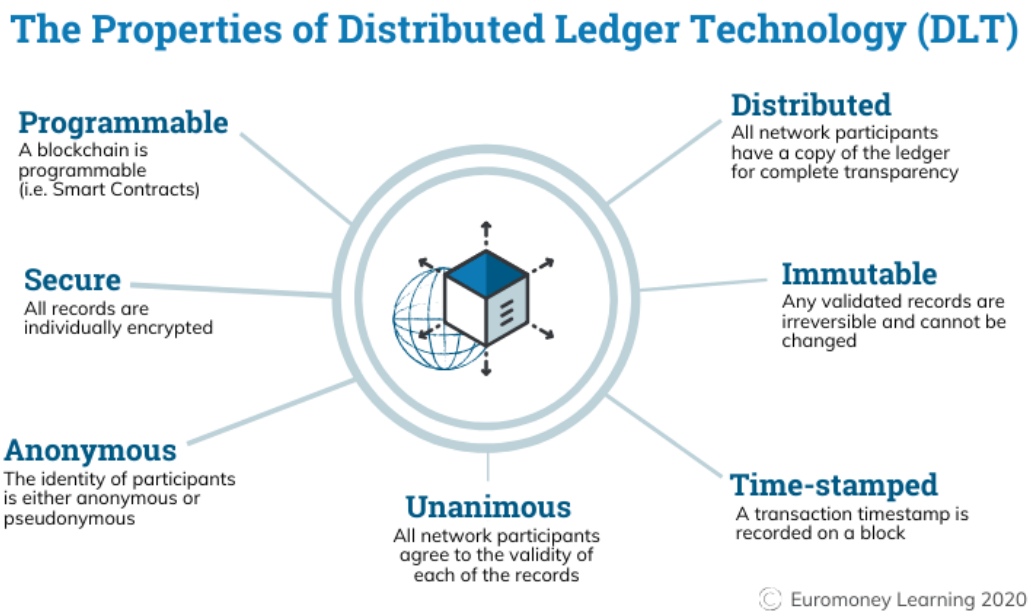
**Abstract**:-

**Blockchain defined:** Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.
An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

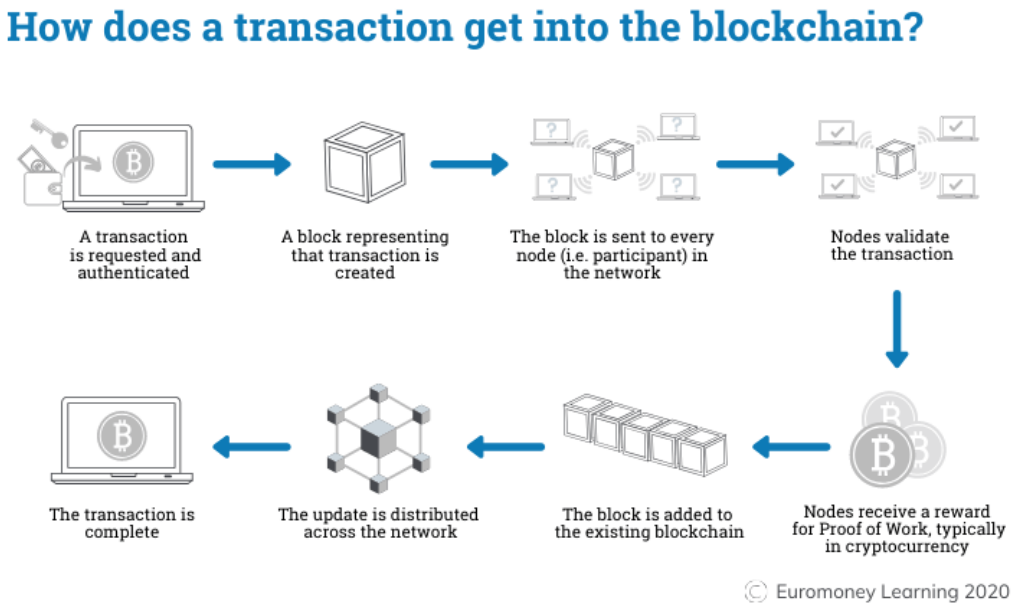
**Why blockchain is important:** Business runs on information. The faster it's received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members. A blockchain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you

can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.

**Related Theory: -**




There are several key steps a transaction must go through before it is added to the blockchain. Today, we're going to focus on authentication using cryptographic keys, authorisation via proof of work, the role of mining, and the more recent adoption of proof of stake protocols in later blockchain networks.




**Authentication**

The original blockchain was designed to operate without a central authority (i.e. with no bank or regulator controlling who transacts), but transactions still have to be authenticated.

This is done using cryptographic keys, a string of data (like a password) that identifies a user and gives access to their "account" or "wallet" of value on the system.

Each user has their own private key and a public key that everyone can see. Using them both creates a secure digital identity to authenticate the user via digital signatures and to 'unlock' the transaction they want to perform.

**Authorisation**

Once the transaction is agreed between the users, it needs to be approved, or authorized, before it is added to a block in the chain.

For a public blockchain, the decision to add a transaction to the chain is made by consensus. This means that the majority of "nodes" (or computers in the network) must agree that the transaction is valid. The people who own the computers in the network are incentivized to verify transactions through rewards. This process is known as 'proof of work'.

## Proof of Work

Proof of Work requires the people who own the computers in the network to solve a complex mathematical problem to be able to add a block to the chain. Solving the problem is known as mining, and 'miners' are usually rewarded for their work in cryptocurrency.

But mining isn't easy. The mathematical problem can only be solved by trial and error and the odds of solving the problem are about 1 in 5.9 trillion. It requires substantial computing power which uses considerable amounts of energy. This means the rewards for undertaking the mining must outweigh the cost of the computers and the electricity cost of running them, as one computer alone would take years to find a solution to the mathematical problem.

## The Power of Mining

The Cambridge Bitcoin Electricity Consumption Index estimates the bitcoin mining network consumes almost 70 terawatt-hours (TWh) of electricity per year, ranking it the 40th largest consumer of electricity by 'country'. By way of comparison, Ireland (ranked 68th) uses just over a third of Bitcoin's consumption, or 25 TWh, and Austria at number 42 consumes 64.6 TWh of electricity per year, according to 2016 data compiled by the CIA.

## The Problem with Proof of Work

To create economies of scale, miners often pool their resources together through companies that aggregate a large group of miners. These miners then share the rewards and fees offered by the blockchain network.

As a blockchain grows, more computers join to try and solve the problem, the problem gets harder and the network gets larger, theoretically distributing the chain further and making it ever more difficult to sabotage or hack. In practice though, mining power has become concentrated in the hands of a few mining pools. These large organisations have the vast computing and electrical power now needed to maintain and grow a blockchain network based around Proof of Work validation.

## Proof of Stake

Later blockchain networks have adopted "Proof of Stake" validation consensus protocols, where participants must have a stake in the blockchain - usually by owning some of the cryptocurrency - to be in with a chance of selecting, verifying & validating

transactions. This saves substantial computing power resources because no mining is required.

In addition, blockchain technologies have evolved to include “Smart Contracts” which automatically execute transactions when certain conditions have been met.

**Related Theory (contd...): -**

The basic application of the **blockchain** is to perform transactions in a secure network. That’s why people use blockchain and ledger technology in different scenarios. One can set up multichain to prevent unauthorized access to sensitive data. It is not available to the public, and can only be available to authorized entities in the organization. It depends on the organization which type it requires to choose for their work.
By using blockchain we can track orders and payments from end to end.

**Advantage using blockchain :**

1. It provides greater trust among users.
2. It provides greater security among data.
3. Reduce the cost of production.
4. Improve Speed.
5. Invocation and tokenization.
6. It provides immutable records.
7. Smart contracts

**Disadvantages using blockchain :**

1. Data modification is not possible.
2. It requires large storage for a large database.
3. The owner cannot access the private key again if they forget or lose it.

**Real life application of blockchain :**

Here is a list of real world problem where we can use blockchain :

1. In a secure and full-proof voting management system.
2. To supply chain management.
3. In healthcare management.
4. Real estate project.
5. NFT marketplace.
6. Avoid copyright and original content creation.
7. In the personal identity system
8. To make an immutable data backup.
9. Internet of Things

## Permissionless Blockchain

It is also known as trustless or public blockchains, are available to everyone to participate in the blockchains process that use to validate transactions and data. These are used in the network where high transparency is required.

**Characteristics:**

- Permissionless blockchain has no central authority.
- The platform is completely open-source.
- Full transparency of the transaction.
- Heavy use of tokens.
-

**Advantages:**

- Everyone can participate only requirement is good hardware and internet.
- Bring trust among users or entities.
- It has a high level of transparency as it's a larger network.
- Broader decentralization of access to more participants.

**Disadvantages:**

- Poor energy efficiency due to large network.
- Lower performance scalability.
- Less privacy as many of the things is visible.

## Permissioned Blockchain

These are the closed network only a set of groups are allowed to validate transactions or data in a given blockchain network. These are used in the network where high privacy and security are required.

**Characteristics:**

- A major feature is a transparency based on the objective of the organization.
- Another feature is the lack of anatomy as only a limited number of users are allowed.
- It does not have a central authority.
- Developed by private authority.

**Advantages:**

- This blockchain tends to be faster as it has some nodes for validations.
- They can offer customizability.
- Strong Privacy as permission is needed for accessing transaction information.
- As few nodes are involved performance and scalability are increased.

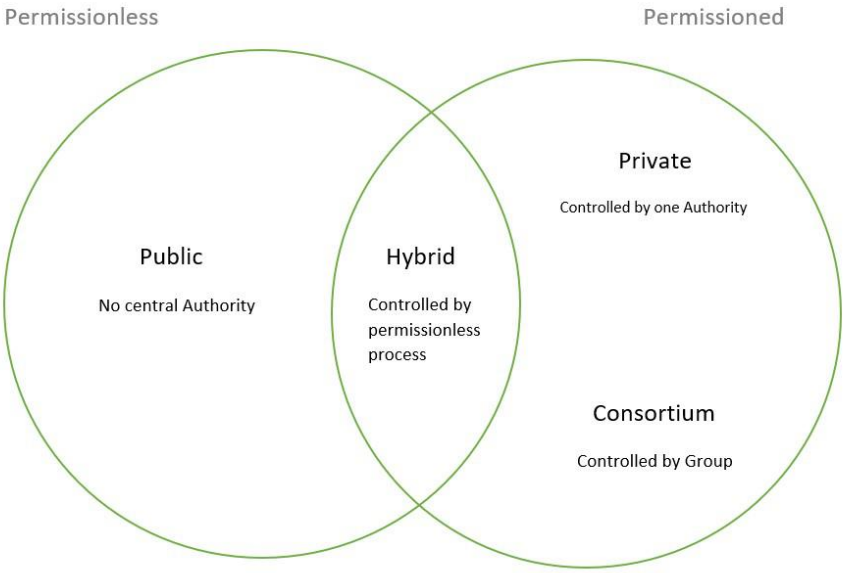
**Disadvantages:**

- Not truly decentralized as it requires permission
- Risk of corruption as only a few participants are involved.
- Anytime owner and operator can change the rules as per their need.

## Types of Blockchain

**There are 4 types of blockchain:**

- **Public Blockchain.**
- **Private Blockchain.**
- **Hybrid Blockchain.**
- **Consortium Blockchain.**




Let's discuss each of these topics in detail.

### 1. Public Blockchain

These blockchains are completely open to following the idea of decentralization. They don't have any restrictions, anyone having a computer and internet can participate in the network.

- As the name is public this blockchain is open to the public, which means it is not owned by anyone.
- Anyone having internet and a computer with good hardware can participate in this public blockchain.
- All the computer in the network hold the copy of other nodes or block present in the network
- In this public blockchain, we can also perform verification of transactions or records

**Advantages:**

- **Trustable:** There are algorithms to detect no fraud. Participants need not worry about the other nodes in the network
- **Secure:** This blockchain is large in size as it is open to the public. In a large size, there is greater distribution of records
- **Anonymous Nature:** It is a secure platform to make your transaction properly at the same time, you are not required to reveal your name and identity in order to participate.
- **Decentralized:** There is no single platform that maintains the network, instead every user has a copy of the ledger.

**Disadvantages:**

- **Processing:** The rate of the transaction process is very slow, due to its large size. Verification of each node is a very time-consuming process.
- **Energy Consumption:** Proof of work is high energy-consuming. It requires good computer hardware to participate in the network
- **Acceptance:** No central authority is there so governments are facing the issue to implement the technology faster.

**Use Cases:** Public Blockchain is secured with proof of work or proof of stake they can be used to displace traditional financial systems. The more advanced side of this blockchain is the smart contract that enabled this blockchain to support decentralization. Examples of public blockchain are Bitcoin, Ethereum.

**2. Private Blockchain**

These blockchains are not as decentralized as the public blockchain only selected nodes can participate in the process, making it more secure than the others.

- These are not as open as a public blockchain.
- They are open to some authorized users only.
- These blockchains are operated in a closed network.
- In this few people are allowed to participate in a network within a company/organization.

**Advantages:**

- **Speed:** The rate of the transaction is high, due to its small size. Verification of each node is less time-consuming.
- **Scalability:** We can modify the scalability. The size of the network can be decided manually.
- **Privacy:** It has increased the level of privacy for confidentiality reasons as the businesses required.
- **Balanced:** It is more balanced as only some user has the access to the transaction which improves the performance of the network.

**Disadvantages:**

- **Security**- The number of nodes in this type is limited so chances of manipulation are there. These blockchains are more vulnerable.

- **Centralized**- Trust building is one of the main disadvantages due to its central nature. Organizations can use this for malpractices.
- **Count**- Since there are few nodes if nodes go offline the entire system of blockchain can be endangered.

**Use Cases:** With proper security and maintenance, this blockchain is a great asset to secure information without exposing it to the public eye. Therefore companies use them for internal auditing, voting, and asset management. An example of private blockchains is Hyperledger, Corda.

**3. Hybrid Blockchain**

It is the mixed content of the private and public blockchain, where some part is controlled by some organization and other makes are made visible as a public blockchain.

- It is a combination of both public and private blockchain.
- Permission-based and permissionless systems are used.
- User access information via smart contracts
- Even a primary entity owns a hybrid blockchain it cannot alter the transaction

**Advantages:**

- **Ecosystem:** Most advantageous thing about this blockchain is its hybrid nature. It cannot be hacked as 51% of users don't have access to the network
- **Cost:** Transactions are cheap as only a few nodes verify the transaction. All the nodes don't carry the verification hence less computational cost.
- **Architecture:** It is highly customizable and still maintains integrity, security, and transparency.
- **Operations:** It can choose the participants in the blockchain and decide which transaction can be made public.

**Disadvantages:**

- **Efficiency:** Not everyone is in the position to implement a hybrid Blockchain. The organization also faces some difficulty in terms of efficiency in maintenance.
- **Transparency:** There is a possibility that someone can hide information from the user. If someone wants to get access through a hybrid blockchain it depends on the organization whether they will give or not.
- **Ecosystem:** Due to its closed ecosystem this blockchain lacks the incentives for network participation.

**Use Case:** It provides a greater solution to the health care industry, government, real estate, and financial companies. It provides a remedy where data is to be accessed publicly but needs to be shielded privately. Examples of Hybrid Blockchain are Ripple network and XRP token.

### 4. Consortium Blockchain

It is a creative approach that solves the needs of the organization. This blockchain validates the transaction and also initiates or receives transactions.

- Also known as Federated Blockchain.
- This is an innovative method to solve the organization's needs.
- Some part is public and some part is private.
- In this type, more than one organization manages the blockchain.

**Advantages:**

- **Speed:** A limited number of users make verification fast. The high speed makes this more usable for organizations.
- **Authority:** Multiple organizations can take part and make it decentralized at every level. Decentralized authority, makes it more secure.
- **Privacy:** The information of the checked blocks is unknown to the public view. but any member belonging to the blockchain can access it.
- **Flexible:** There is much divergence in the flexibility of the blockchain. Since it is not a very large decision can be taken faster.

**Disadvantages:**

- **Approval:** All the members approve the protocol making it less flexible. Since one or more organizations are involved there can be differences in the vision of interest.
- **Transparency:** It can be hacked if the organization becomes corrupt. Organizations may hide information from the users.
- **Vulnerability:** If few nodes are getting compromised there is a greater chance of vulnerability in this blockchain

**Use Cases:** It has high potential in businesses, banks, and other payment processors. Food tracking of the organizations frequently collaborates with their sectors making it a federated solution ideal for their use. Examples of consortium Blockchain are Tendermint and Multichain.

**Implementation Details:**

**1. Enlist all the Steps followed and various options explored**

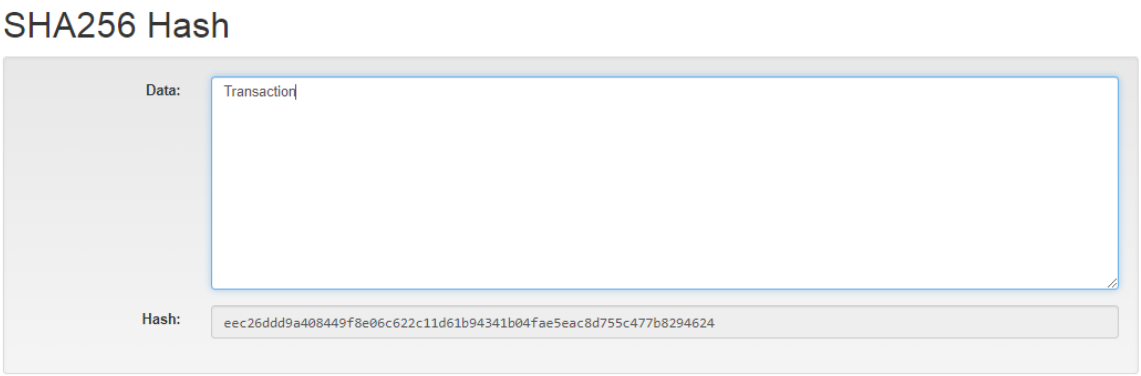
- Visit the blockchain demo website
- Understand how hash functions work by creating some hash for random data
- Now move to the next part where we try and understand how a block in a blockchain works and how the hash is calculated by changing the nonce until the predefined difficulty level is matched.
- When the data in the block is changed the block becomes invalid until the (block + nonce + data) is not hashed to create the desired difficulty level number of zeros.
- Explore all the other options which are provided on the website for understanding blockchain.

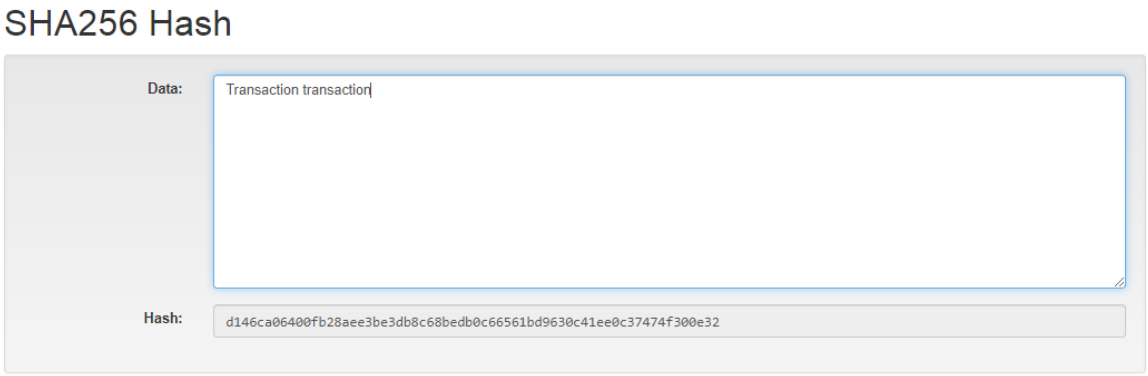
**Various options explored**

1. Block
2. Blockchain
3. Distributed blockchain
4. Tokens
5. Coinbase

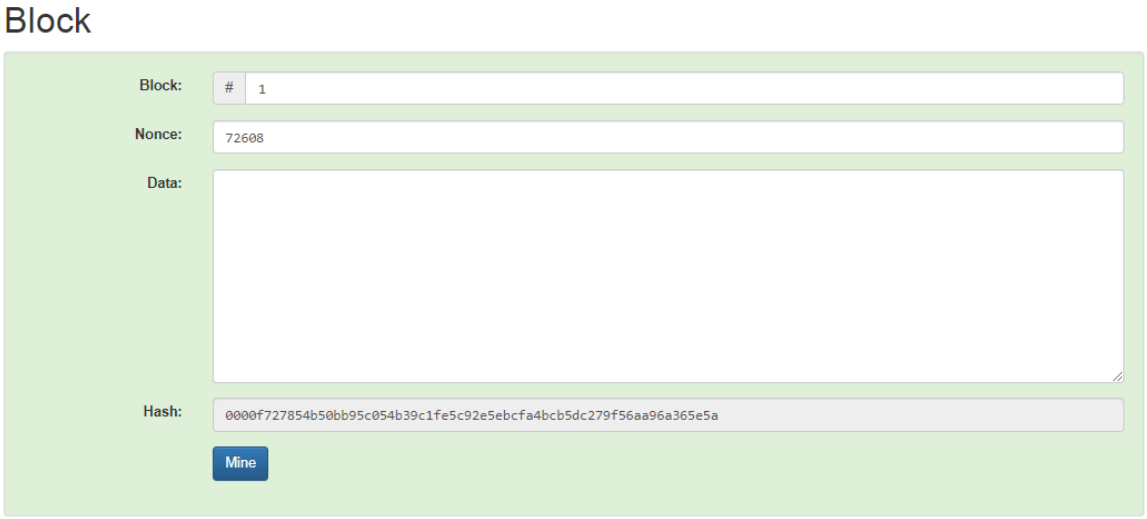
**2. Explain your program logic, classes and methods used.**

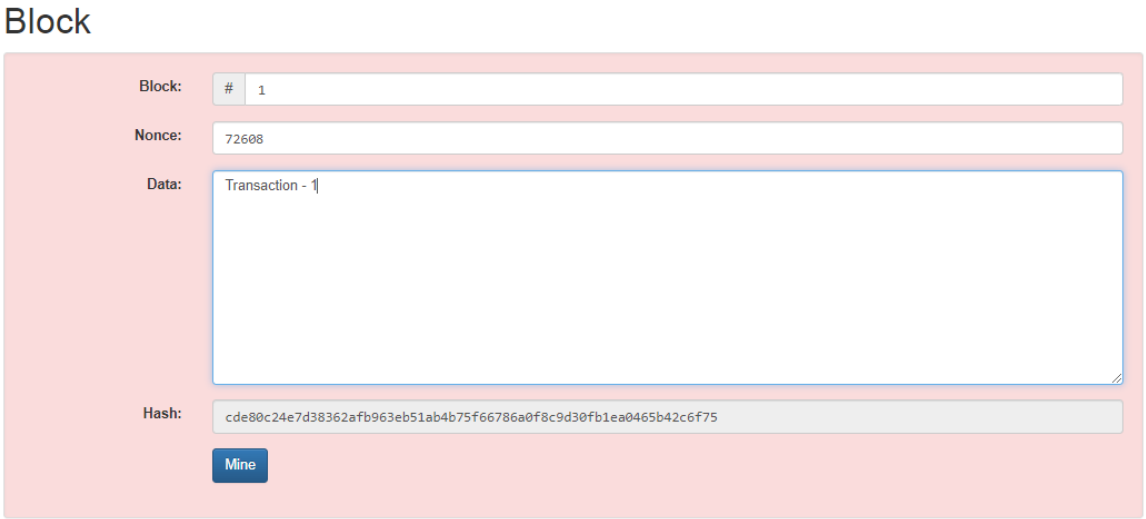
- Create a random hash to understand how hashing works



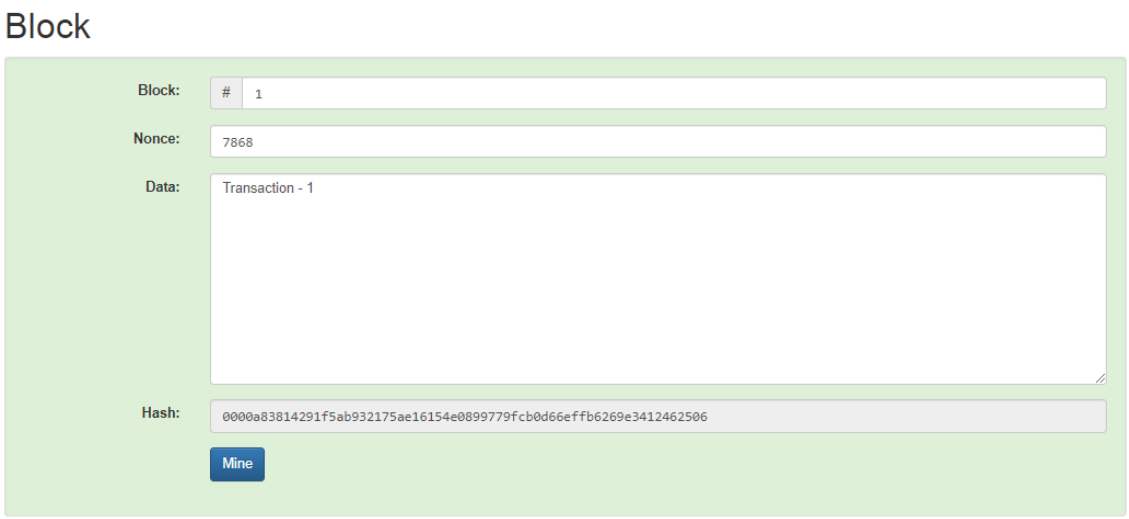



- Create a block in a blockchain and see how the hash changes on changing the data inside the block.

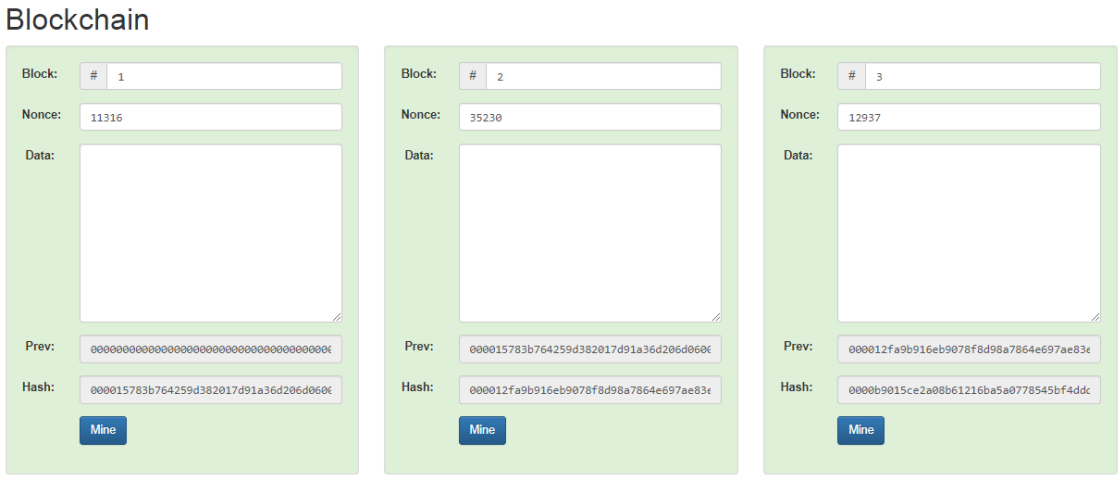


- After changing the value in a block the block becomes invalid which needs to be validated by mining the block, after which the hash changes and so does the state of the block.

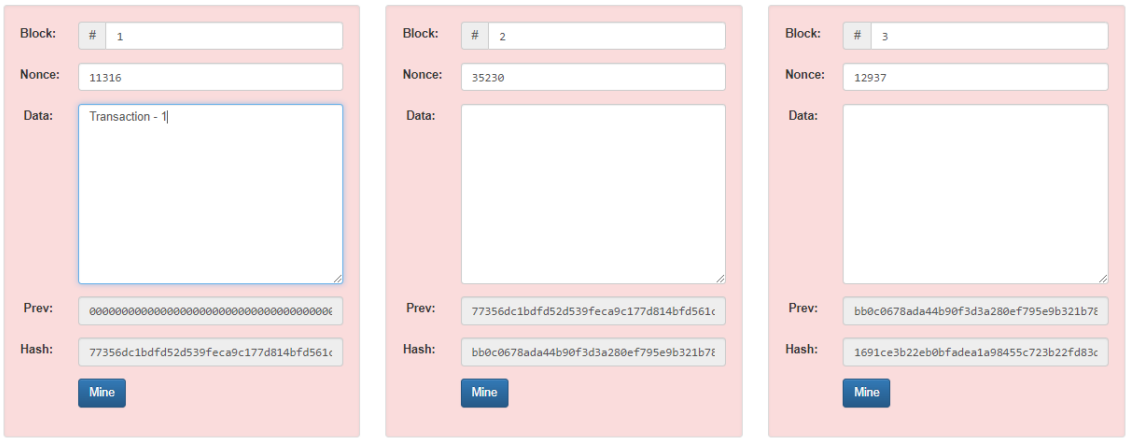



- Now explore the functionality of the blockchain.

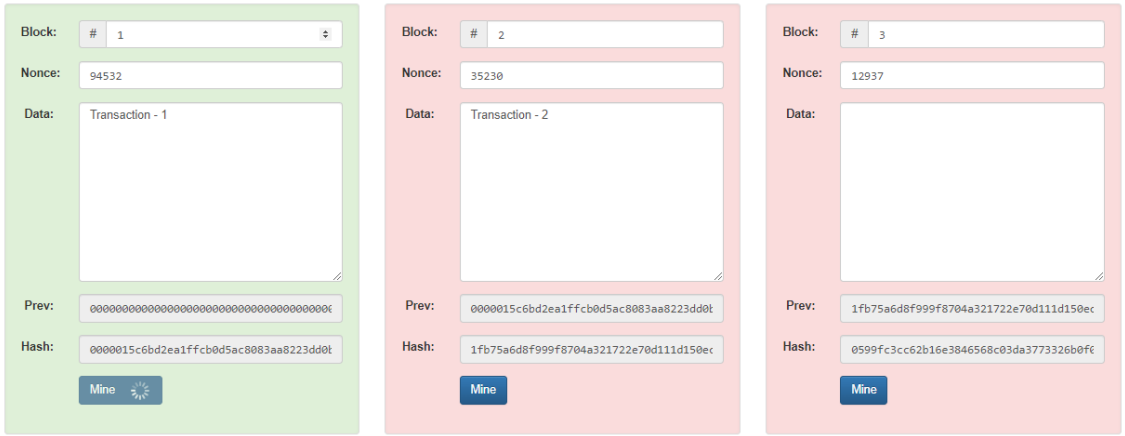



- On changing the data value of a block, all the blocks after the current block also become invalid. All these blocks need to be mined indivusally to make the blockchain completely valid again.

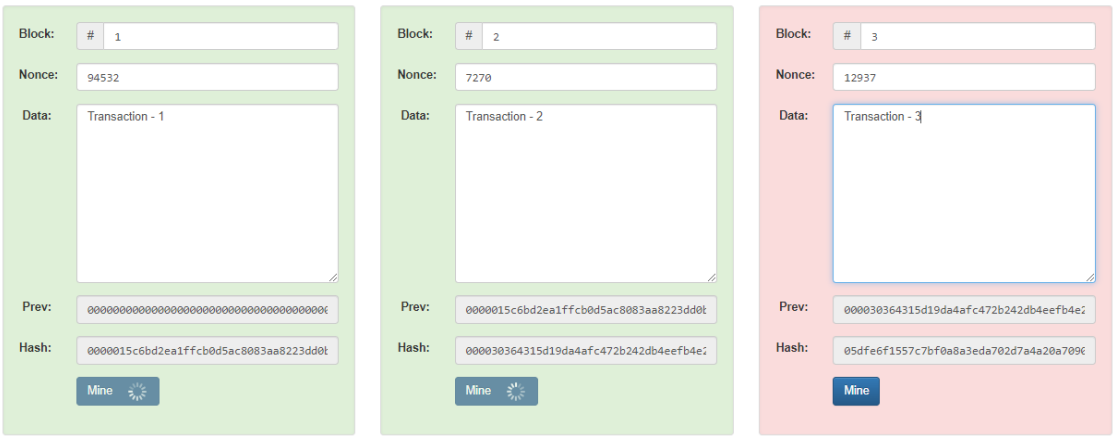
Blockchain

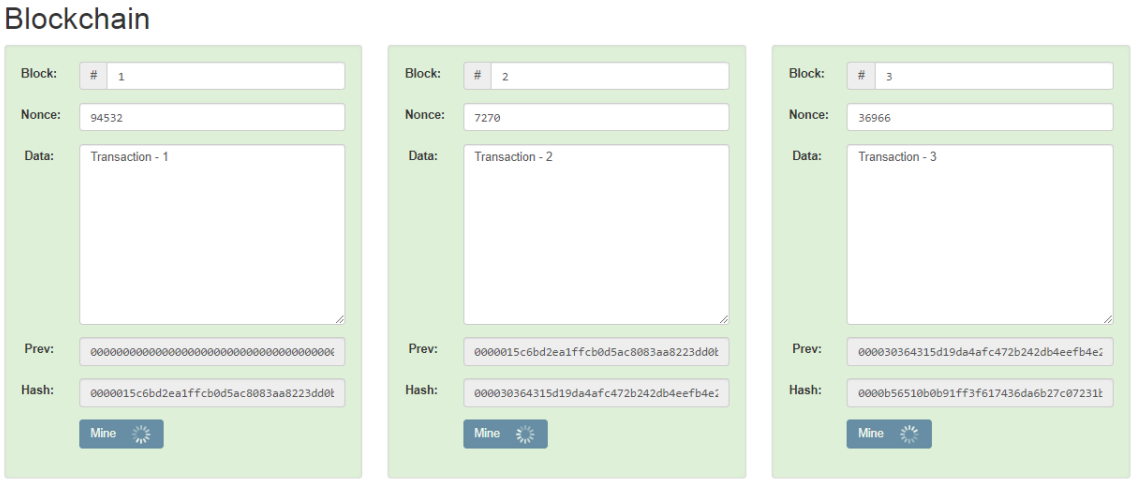



Blockchain

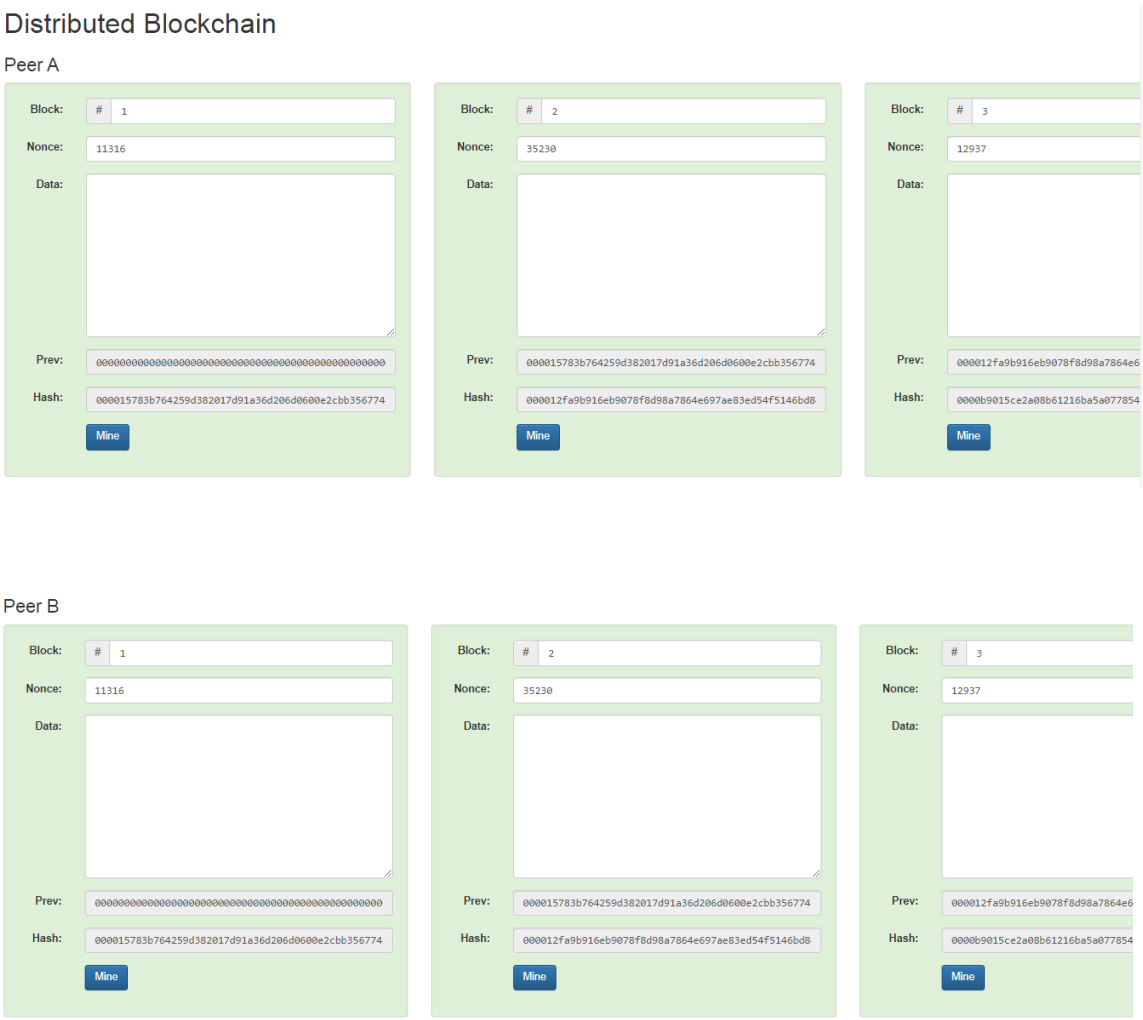



Blockchain

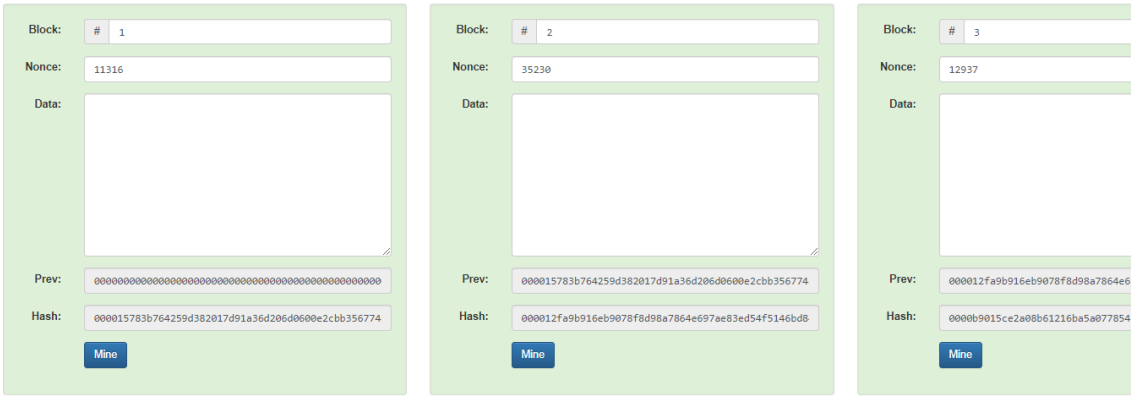





- Here the complete blockchain and all its blocks are stored at all the nodes participating in the blockchain.



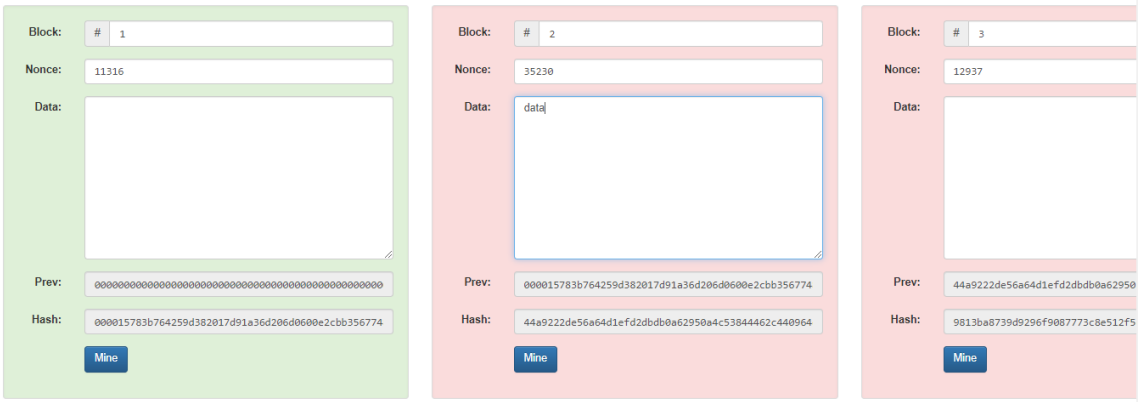
Peer C



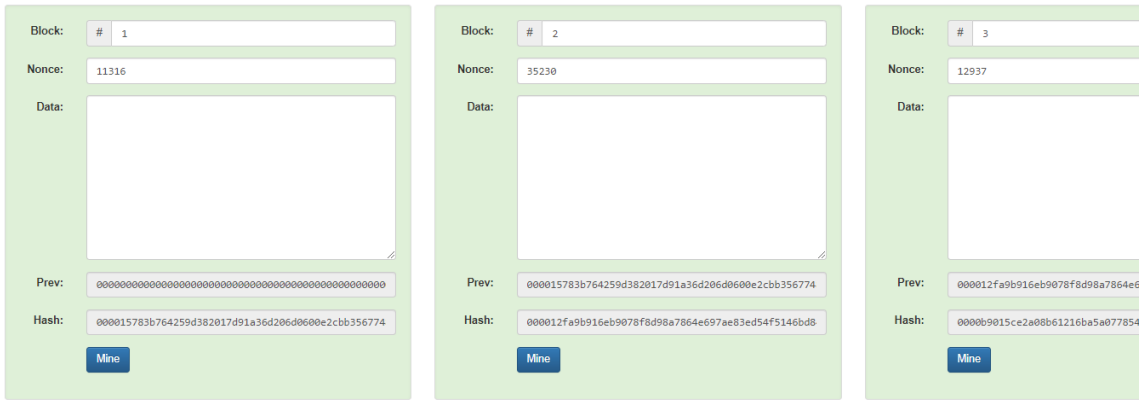

- If one block of a node becomes invalid, blocks in the other two nodes are not affected.

Distributed Blockchain

Peer A




Peer B



## Tokens

### Peer A

**Block: # 1**

Nonce: 139358

| Tx: | | | | | |
|---|---|---|---|---|---|
| $ 25.00 | From: | Darcy | -> | Bingley |
| $ 4.27 | From: | Elizabeth | -> | Jane |
| $ 19.22 | From: | Wickham | -> | Lydia |
| $ 106.44 | From: | Lady Cath | -> | Collins |
| $ 6.42 | From: | Charlotte | -> | Elizabeth |

Prev: 00000000000000000000000000000000000000000000000000000000000000000

Hash: 00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfb

Mine

**Block: # 2**

Nonce: 39207

| Tx: | | | | | |
|---|---|---|---|---|---|
| $ 97.67 | From: | Ripley | -> | Lambert |
| $ 48.61 | From: | Kane | -> | Ash |
| $ 6.15 | From: | Parker | -> | Dallas |
| $ 10.44 | From: | Hicks | -> | Newt |
| $ 88.32 | From: | Bishop | -> | Burke |
| $ 45.00 | From: | Hudson | -> | Gorman |
| $ 92.00 | From: | Vasquez | -> | Apone |

Prev: 00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfb

Hash: 000078be183417844c14a9251ca246fb15df1074019873f5d

Mine

**Block: # 3**

Nonce: 13804

| Tx: | | | | | |
|---|---|---|---|---|---|
| $ 10.00 | From: | Emily | | |
| $ 5.00 | From: | Madison | | |
| $ 20.00 | From: | Lucas | | |

Prev: 000078be183417844c14a9251ca246f

Hash: 0000c2c95f54a49b4f2bee7056a7dc3

Mine



### Peer B

**Block: # 1**

Nonce: 139358

| Tx: | | | | | |
|---|---|---|---|---|---|
| $ 25.00 | From: | Darcy | -> | Bingley |
| $ 4.27 | From: | Elizabeth | -> | Jane |
| $ 19.22 | From: | Wickham | -> | Lydia |
| $ 106.44 | From: | Lady Cath | -> | Collins |
| $ 6.42 | From: | Charlotte | -> | Elizabeth |

Prev: 00000000000000000000000000000000000000000000000000000000000000000

Hash: 00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfb

Mine

**Block: # 2**

Nonce: 39207

| Tx: | | | | | |
|---|---|---|---|---|---|
| $ 97.67 | From: | Ripley | -> | Lambert |
| $ 48.61 | From: | Kane | -> | Ash |
| $ 6.15 | From: | Parker | -> | Dallas |
| $ 10.44 | From: | Hicks | -> | Newt |
| $ 88.32 | From: | Bishop | -> | Burke |
| $ 45.00 | From: | Hudson | -> | Gorman |
| $ 92.00 | From: | Vasquez | -> | Apone |

Prev: 00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfb

Hash: 000078be183417844c14a9251ca246fb15df1074019873f5d

Mine

**Block: # 3**

Nonce: 13804

| Tx: | | | | | |
|---|---|---|---|---|---|
| $ 10.00 | From: | Emily | | |
| $ 5.00 | From: | Madisor | | |
| $ 20.00 | From: | Lucas | | |

Prev: 000078be183417844c14a9251ca246f

Hash: 0000c2c95f54a49b4f2bee7056a7dc3

Mine

## Tokens

### Peer A

**Block: # 1**

Nonce: 26485

| Tx: | | | | | |
|---|---|---|---|---|---|
| $ 25.00 | From: | Darcy | -> | Nayan |
| $ 4.27 | From: | Elizabeth | -> | Jane |
| $ 19.22 | From: | Wickham | -> | Lydia |
| $ 106.44 | From: | Lady Cath | -> | Collins |
| $ 6.42 | From: | Charlotte | -> | Elizabeth |

Prev: 00000000000000000000000000000000000000000000000000000000000000000

Hash: 00006f4ce1e02102b82cf3ab107c27218d7beb8584c137fba

Mine

**Block: # 2**

Nonce: 39207

| Tx: | | | | | |
|---|---|---|---|---|---|
| $ 97.67 | From: | Ripley | -> | Lambert |
| $ 48.61 | From: | Kane | -> | Ash |
| $ 6.15 | From: | Parker | -> | Dallas |
| $ 10.44 | From: | Hicks | -> | Newt |
| $ 88.32 | From: | Bishop | -> | Burke |
| $ 45.00 | From: | Hudson | -> | Gorman |
| $ 92.00 | From: | Vasquez | -> | Apone |

Prev: 00006f4ce1e02102b82cf3ab107c27218d7beb8584c137fba

Hash: 1101e6538b7f4cef9842858abece7d920d2f70d5b4217e8c3

Mine

**Block: # 3**

Nonce: 13804

| Tx: | | | | | |
|---|---|---|---|---|---|
| $ 10.00 | From: | Emily | | |
| $ 5.00 | From: | Madison | | |
| $ 20.00 | From: | Lucas | | |

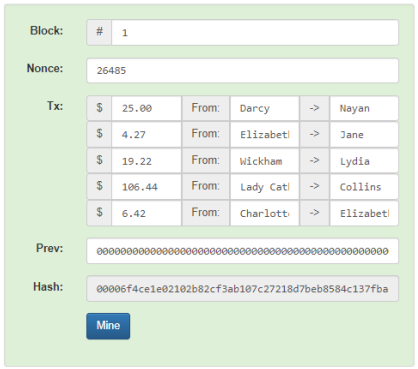
Prev: 1101e6538b7f4cef9842858abece7d9

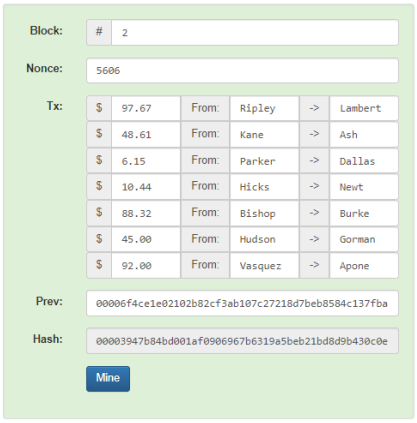
Hash: 20501e5eb440eb969d608a6cf95e740

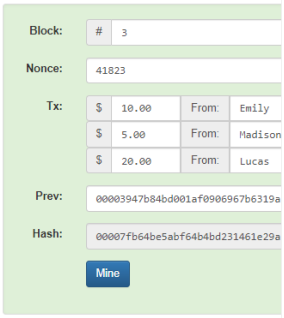
Mine

## Tokens

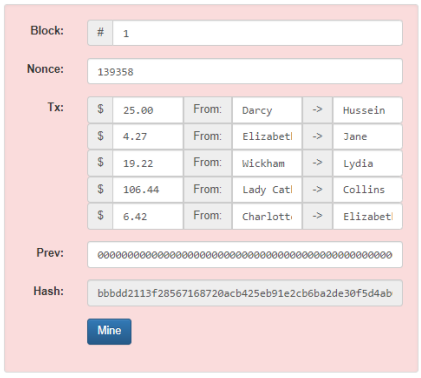
### Peer A

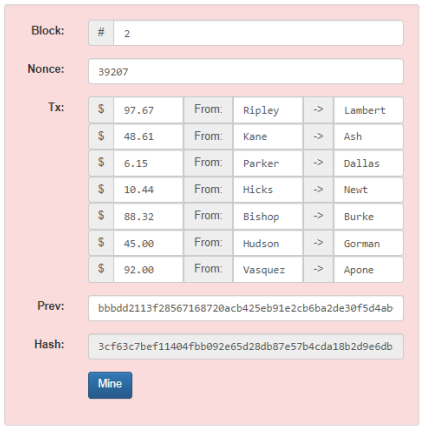


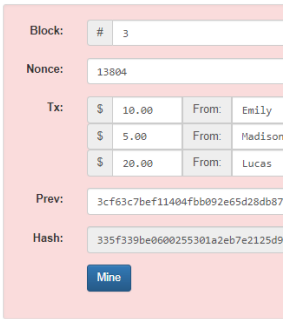



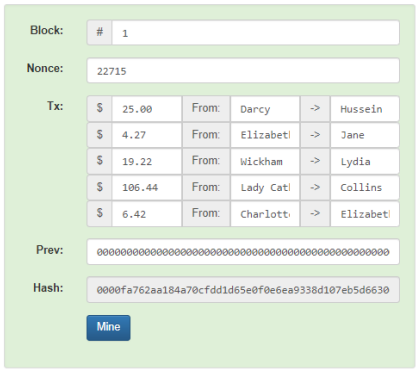

### Peer B

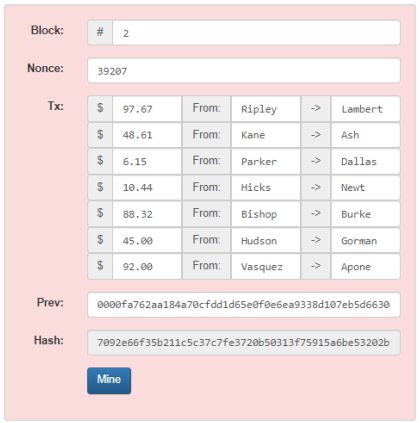


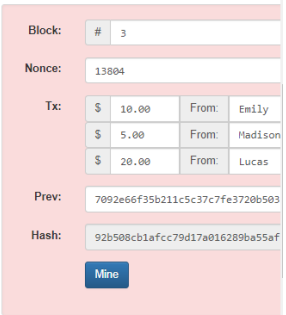




### Peer B



Peer B

| Block: | # | 1 | | | | |
|---|---|---|---|---|---|---|
| Nonce: | 22715 | | | | | |
| Tx: | $ | 25.00 | From: | Darcy | -> | Hussein |
| | $ | 4.27 | From: | Elizabet | -> | Jane |
| | $ | 19.22 | From: | Wickham | -> | Lydia |
| | $ | 106.44 | From: | Lady Cat | -> | Collins |
| | $ | 6.42 | From: | Charlott | -> | Elizabet |
| Prev: | 00000000000000000000000000000000000000000000000000000000 | | | | | |
| Hash: | 0000fa762aa184a70cfdd1d65e0f0e6ea9338d107eb5d6630 | | | | | |

Mine

| Block: | # | 2 | | | | |
|---|---|---|---|---|---|---|
| Nonce: | 9306 | | | | | |
| Tx: | $ | 97.67 | From: | Ripley | -> | Lambert |
| | $ | 48.61 | From: | Kane | -> | Ash |
| | $ | 6.15 | From: | Parker | -> | Dallas |
| | $ | 10.44 | From: | Hicks | -> | Newt |
| | $ | 88.32 | From: | Bishop | -> | Burke |
| | $ | 45.00 | From: | Hudson | -> | Gorman |
| | $ | 92.00 | From: | Vasquez | -> | Apone |
| Prev: | 0000fa762aa184a70cfdd1d65e0f0e6ea9338d107eb5d6630 | | | | | |
| Hash: | 000090261995d5e6a6263b2117c17cba169b02a99b853577c | | | | | |

Mine

| Block: | # | 3 | | | | |
|---|---|---|---|---|---|---|
| Nonce: | 13804 | | | | | |
| Tx: | $ | 10.00 | From: | Emily | | |
| | $ | 5.00 | From: | Madison | | |
| | $ | 20.00 | From: | Lucas | | |
| Prev: | 000090261995d5e6a6263b2117c17cb | | | | | |
| Hash: | 23e8223f69a0b289e781abb28d69f72 | | | | | |

Mine

Peer B

| Block: | # | 1 | | | | |
|---|---|---|---|---|---|---|
| Nonce: | 22715 | | | | | |
| Tx: | $ | 25.00 | From: | Darcy | -> | Hussein |
| | $ | 4.27 | From: | Elizabet | -> | Jane |
| | $ | 19.22 | From: | Wickham | -> | Lydia |
| | $ | 106.44 | From: | Lady Cat | -> | Collins |
| | $ | 6.42 | From: | Charlott | -> | Elizabet |
| Prev: | 00000000000000000000000000000000000000000000000000000000 | | | | | |
| Hash: | 0000fa762aa184a70cfdd1d65e0f0e6ea9338d107eb5d6630 | | | | | |

Mine

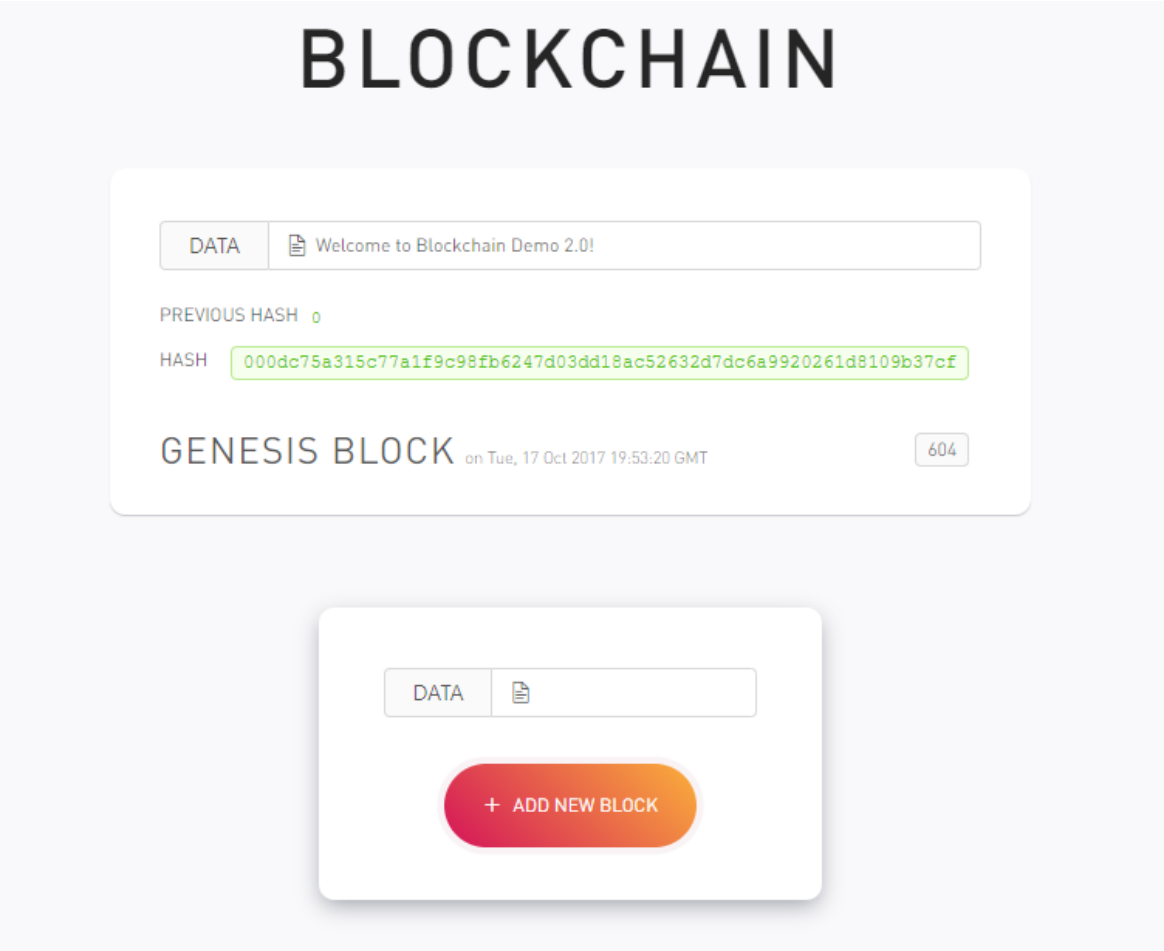
| Block: | # | 2 | | | | |
|---|---|---|---|---|---|---|
| Nonce: | 9306 | | | | | |
| Tx: | $ | 97.67 | From: | Ripley | -> | Lambert |
| | $ | 48.61 | From: | Kane | -> | Ash |
| | $ | 6.15 | From: | Parker | -> | Dallas |
| | $ | 10.44 | From: | Hicks | -> | Newt |
| | $ | 88.32 | From: | Bishop | -> | Burke |
| | $ | 45.00 | From: | Hudson | -> | Gorman |
| | $ | 92.00 | From: | Vasquez | -> | Apone |
| Prev: | 0000fa762aa184a70cfdd1d65e0f0e6ea9338d107eb5d6630 | | | | | |
| Hash: | 000090261995d5e6a6263b2117c17cba169b02a99b853577c | | | | | |

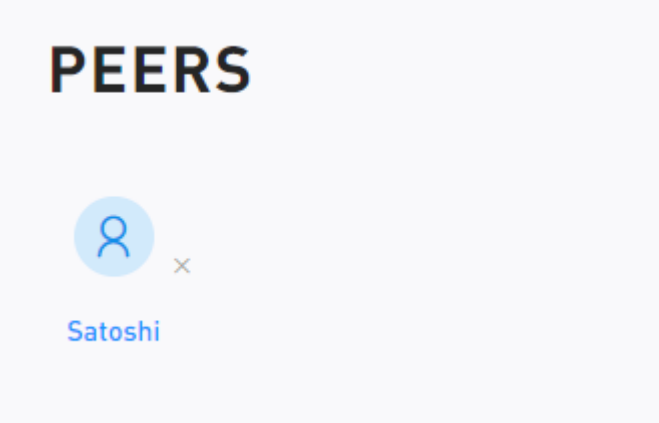
Mine

| Block: | # | 3 | | | | |
|---|---|---|---|---|---|---|
| Nonce: | 67612 | | | | | |
| Tx: | $ | 10.00 | From: | Emily | | |
| | $ | 5.00 | From: | Madison | | |
| | $ | 20.00 | From: | Lucas | | |
| Prev: | 000090261995d5e6a6263b2117c17cb | | | | | |
| Hash: | 0000675a320649ffe47135b861c4627 | | | | | |

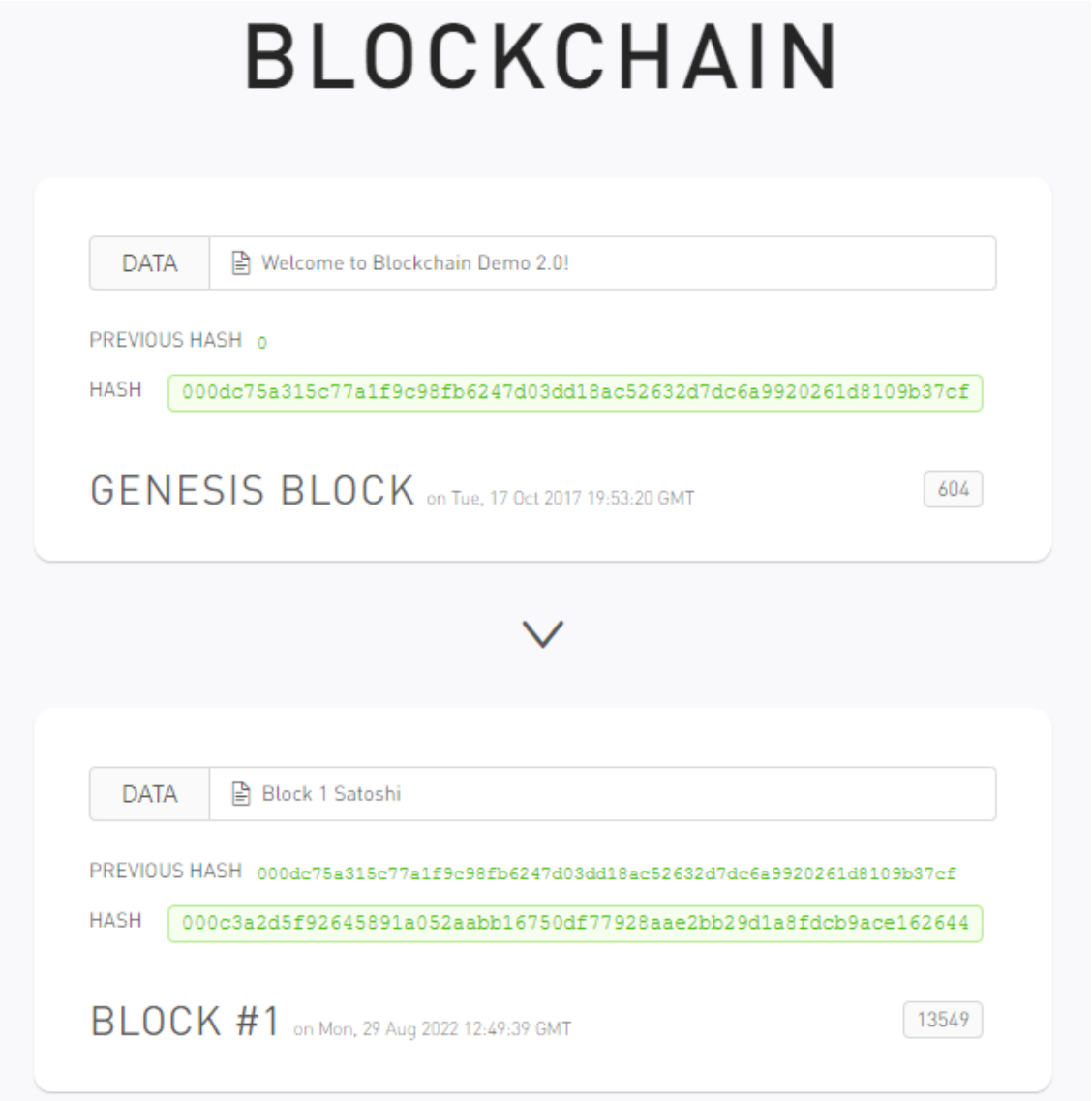
Mine

This is a peer to peer blockchain network where two or more peers can communicate and all the messages and data is stored on the blockchain itself.

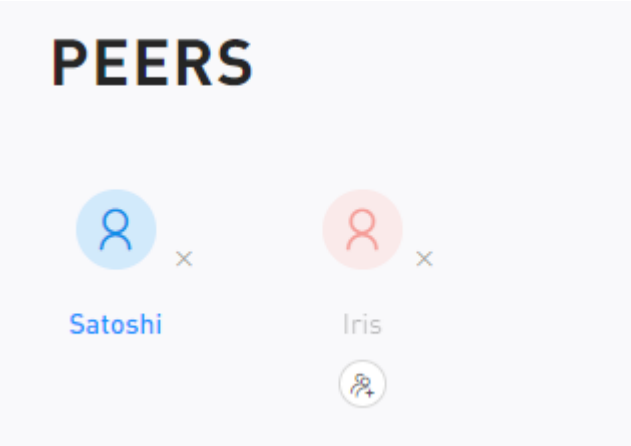


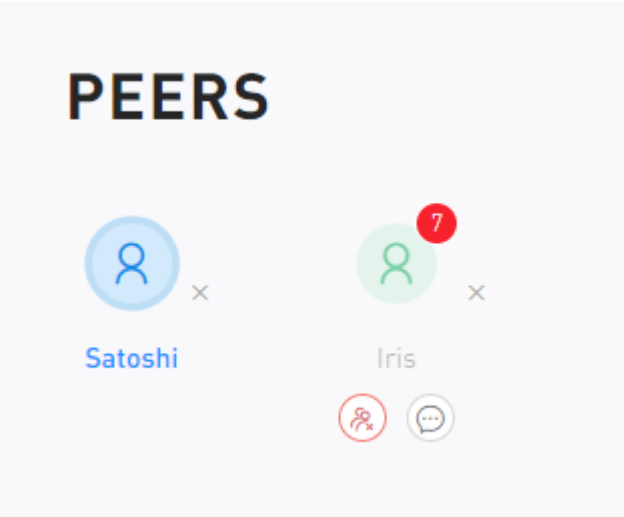



- Here the peer named **Satoshi** adds a block on the network which has the following data “Block 1 satoshi”

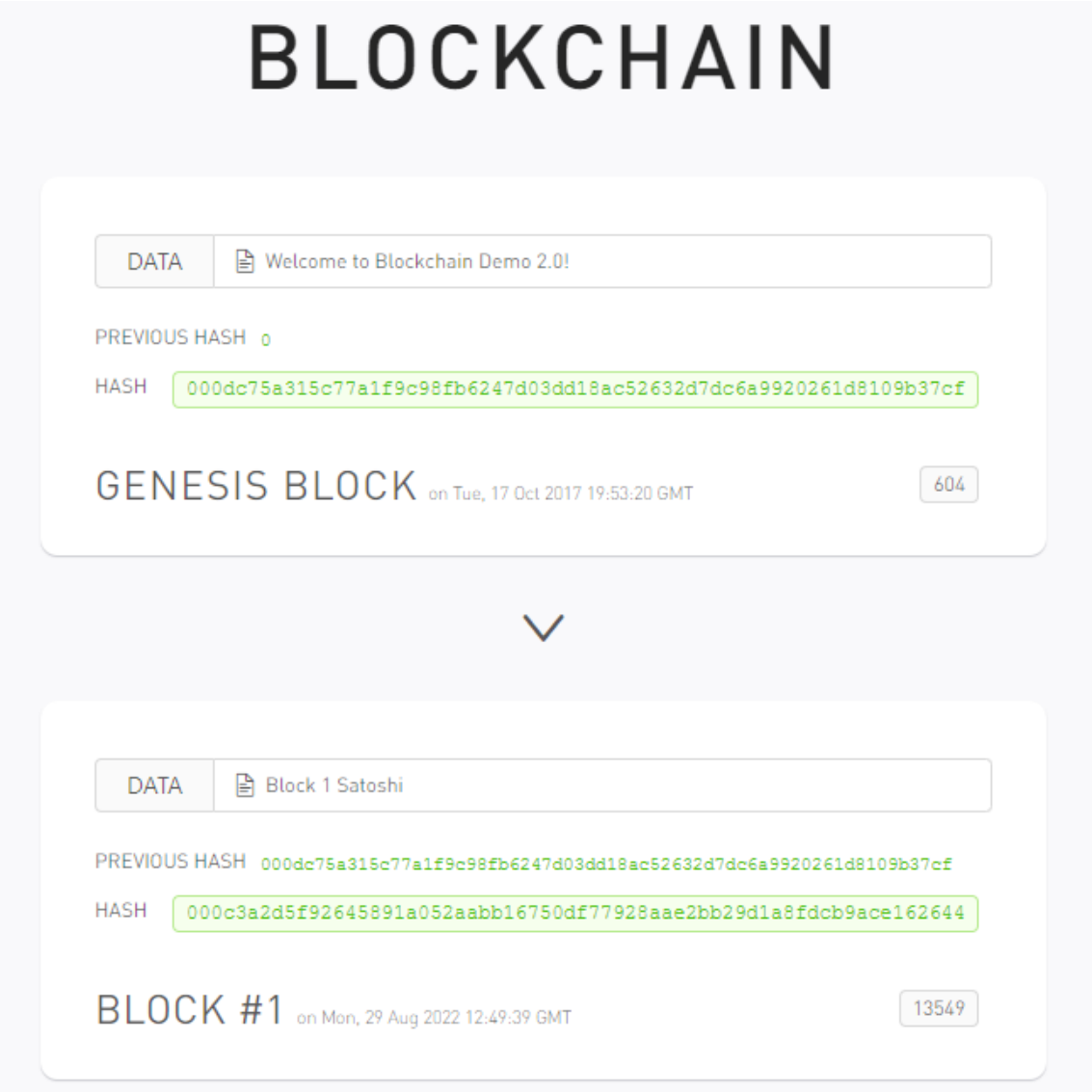


- Here we create a new peer named **Iris** who then goes on to connect with the peer **satoshi** on the same network.



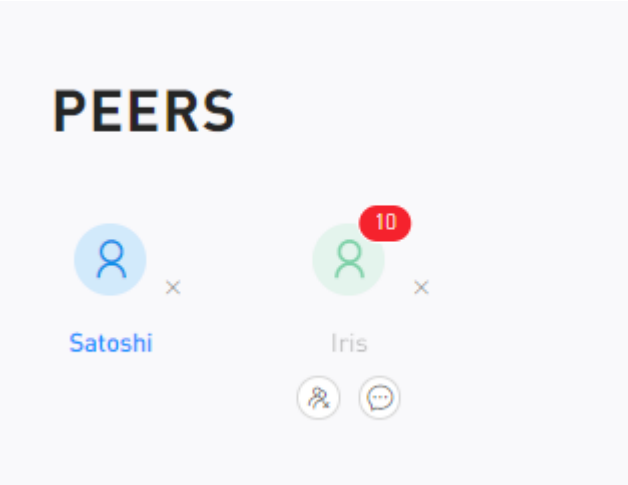



- Now on seeing the network copy stored on **Iris** machine it can be seen that the message which **Satoshi** has added on the network is visible.



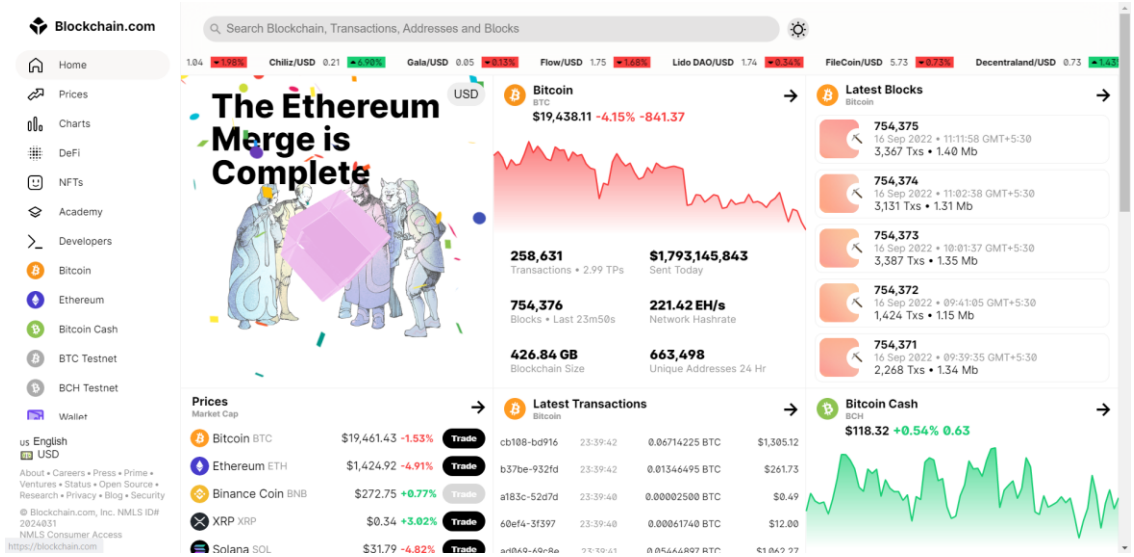
- Now we add block from **Iris** peer and see whether that block can be seen from the network copy on **Satoshi** peers device.


DATA
Block 1 Satoshi
PREVIOUS HASH 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf
HASH 000c3a2d5f92645891a052aabb16750df77928aae2bb29d1a8fdcb9ace162644
BLOCK #1 on Mon, 29 Aug 2022 12:49:39 GMT
13549
DATA
Block 2 iris
PREVIOUS HASH 000c3a2d5f92645891a052aabb16750df77928aae2bb29d1a8fdcb9ace162644
HASH 00081a8f8a1bb1c35aa933f6a6b218e78e5528adb4f09f317366f09fedf48205
BLOCK #2 on Mon, 29 Aug 2022 12:54:23 GMT
472


PEERS
10
Satoshi
Iris

**Block explorer – Bitcoin: Link**

1) Bitcoin blockchain is a very wide network consists of thousands of block linked one after another. Despite of this huge network every information related to a particular block is easily using block explorers. Transactions, block numbers, bitcoins transferred, etc everything can be easily checked by usign the blockchain explorers available.




2) As seen from the results of the search the description of block number 0 is visible. The date when it is added to the chain and by whom it is added is also seen in the description. It also contains the number of blocks added in the chain after the first i.e. the genesis block. Reward received by the miner after adding this block in the bitcoin network is also available with the description of amount transferred to miners address.


3) A table will be displayed at the bottom containing more information related to the block that is searched. Hash shows the has of the block header, confirmations shows the number of blocks added after the block, timestamps shows the time at which the block is inserted, height shows the number of blocks before this block, name of the miner, number of transations, nonce used to calculate block hash to satisfy proof of work, block reward, etc.

| | |
|---|---|
| Hash | 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f |
| Confirmations | 754,376 |
| Timestamp | 2009-01-03 23:45 |
| Height | 0 |
| Miner | Unknown |
| Number of Transactions | 1 |
| Difficulty | 1.00 |
| Merkle root | 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b |
| Version | 0x1 |
| Bits | 486,604,799 |
| Weight | 1,140 WU |
| Size | 285 bytes |
| Nonce | 2,083,236,893 |
| Transaction Volume | 0.00000000 BTC |
| Block Reward | 50.00000000 BTC |

4) At the bottom of the page all the transactions present in the block can be seen. As seen from the information given some bitcoins are transferred from one address to another. Green symbol besides amount shows that the bitcoin are unspent and can be used for making another transactions.

**Block Transactions**

| | | | |
|---|---|---|---|
| Fee | 0.00000000 BTC<br>(0.000 sat/B - 0.000 sat/WU - 204 bytes) | | 50.00000000 BTC |
| Hash | 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b | | 2009-01-03 23:45 |
| | COINBASE (Newly Generated Coins) | 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa | 50.00000000 BTC |

5) By navigating to any of the address information related to the account (address) can be easily found. As seen qr code associated with the address, format, number of transactions, total amount of bitcoins received, total amount of bitcoin sent and the final balance.

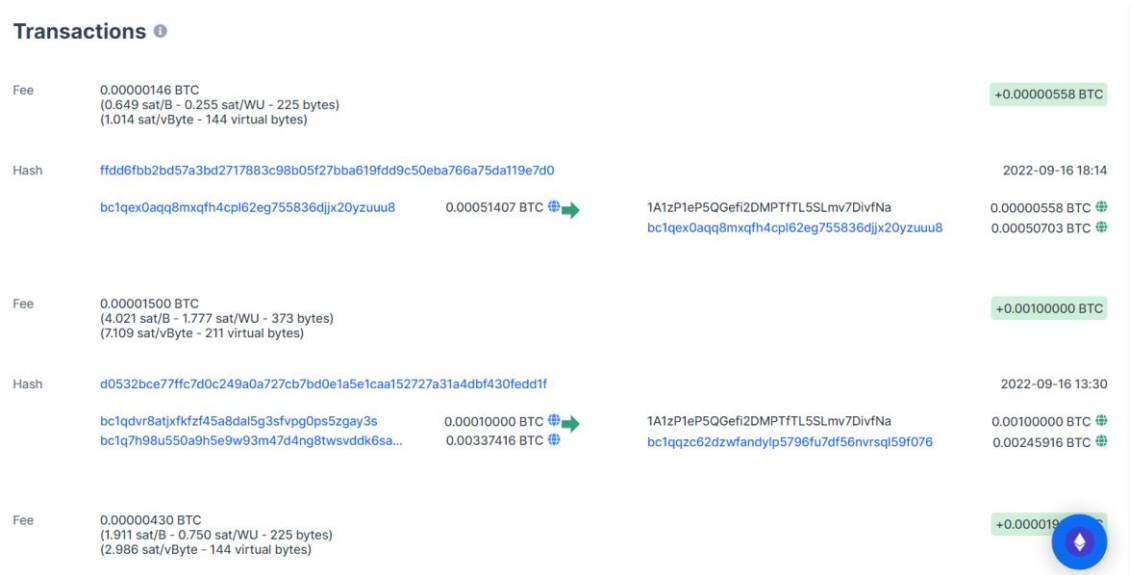
**Address** USD BTC

This address has transacted 3,453 times on the Bitcoin blockchain. It has received a total of 68.55312301 BTC ($1,332,866.03) and has sent a total of 0.00000000 BTC ($0.00). The current value of this address is 68.55312301 BTC ($1,332,866.03).

| | |
|---|---|
| Address | 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa |
| Format | BASE58 (P2PKH) |
| Transactions | 3,453 |
| Total Received | 68.55312301 BTC |
| Total Sent | 0.00000000 BTC |
| Final Balance | 68.55312301 BTC |

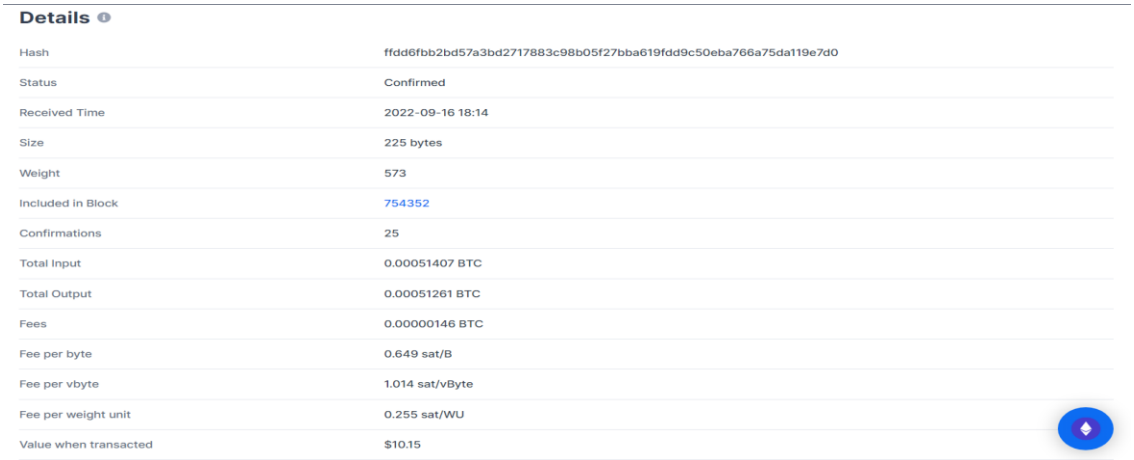
Total amount received from this address over time

6) All the transactions related to this address can also been at the bottom of the page. All the transactions with its transaction fees, amount of btc's transferred, from and to address of the transaction and the date of the transation can also be visible.




7) Information related to any transaction can also be seen by navigating to any of the transaction hashes. Transaction fees, amount of btc's transferred, addresses of transactions, date, the number of confirmations on this transaction, etc.


8) Other details can also be seen at the bottom including size, status, value of the transaction when it was made, etc.




9) Input associated with the transaction and the output can also be seen at the end of the page.

**Inputs** ⓘ HEX ASM

| | | | |
|---|---|---|---|
| Index | 0 | Details | Output |
| Address | bc1qex0aqq8mxqfh4cpl62eg755836djjx20yzuuu8 | Value | 0.00051407 BTC |
| Pkscript | OP_0<br>c99fd000fb30137ae03fd2b28f52878e9b29194f | | |
| Sigscript | | | |
| Witness | 3044022017bd023c1c073d463ebea129e7e2a8bffabb24c0695a344bdc4fba8e4304cbda02205f0175a05108757a0cc35a455645a1a6f1d047b13ec3aea348617a6bb2e5dba401<br>031f6fa906bb52f3e1bdc59156a5659ce1aa251eaf26f411413c76409360ef7205 | | |

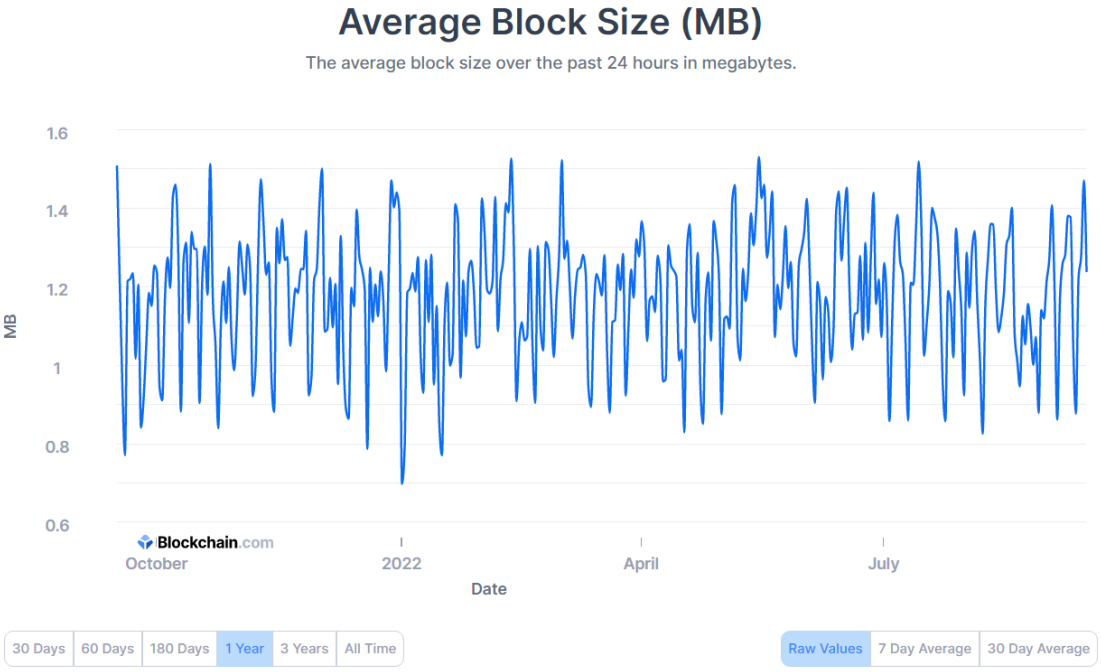
10) Output contains addresses, public key scripts and the amount of bitcoints spent/unspent.

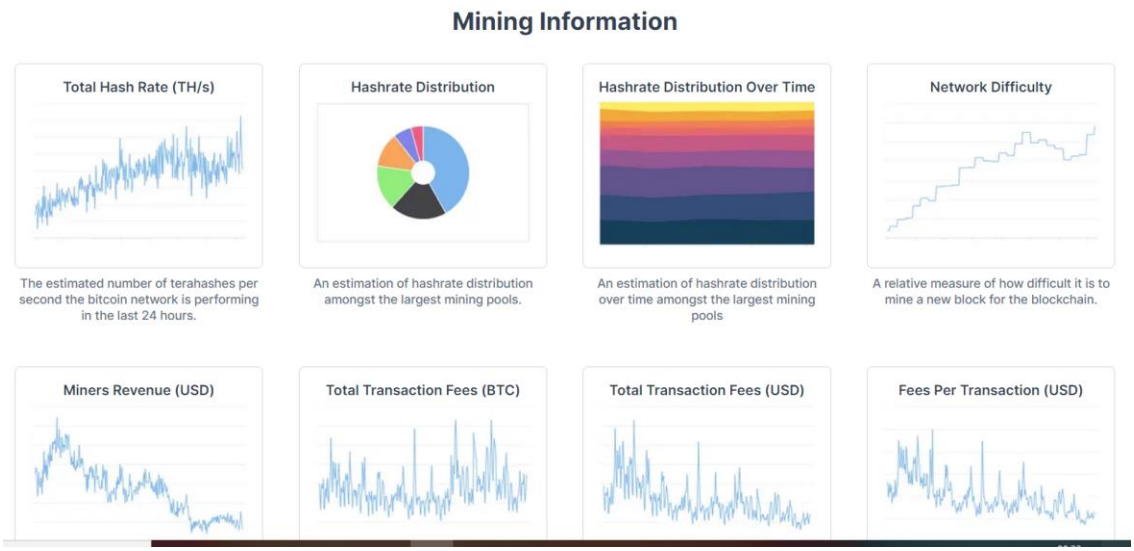
**Outputs** ⓘ

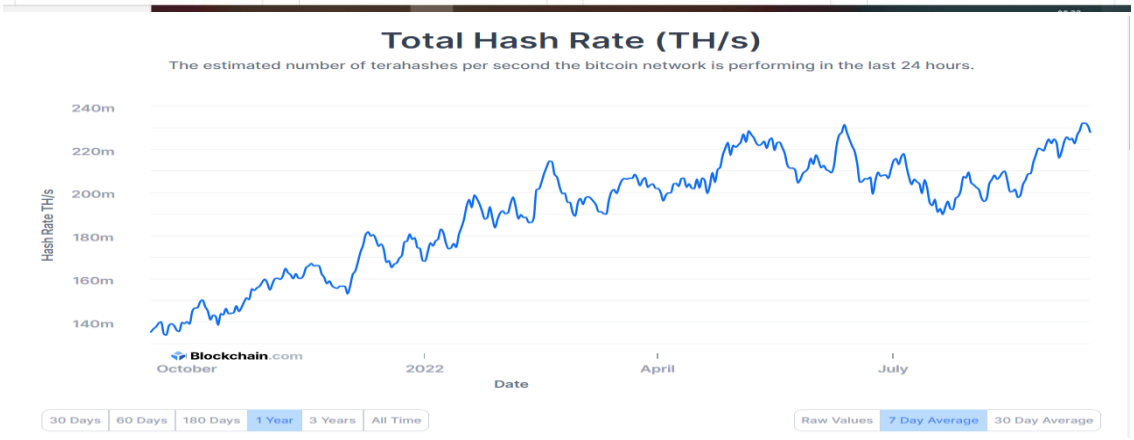
| | | | |
|---|---|---|---|
| Index | 0 | Details | Unspent |
| Address | 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa | Value | 0.00000558 BTC |
| Pkscript | OP_DUP<br>OP_HASH160<br>62e907b15cbf27d5425399ebf6f0fb50ebb88f18<br>OP_EQUALVERIFY<br>OP_CHECKSIG | | |
| Index | 1 | Details | Unspent |
| Address | bc1qex0aqq8mxqfh4cpl62eg755836djjx20yzuuu8 | Value | 0.00050703 BTC |
| Pkscript | OP_0<br>c99fd000fb30137ae03fd2b28f52878e9b29194f | | |

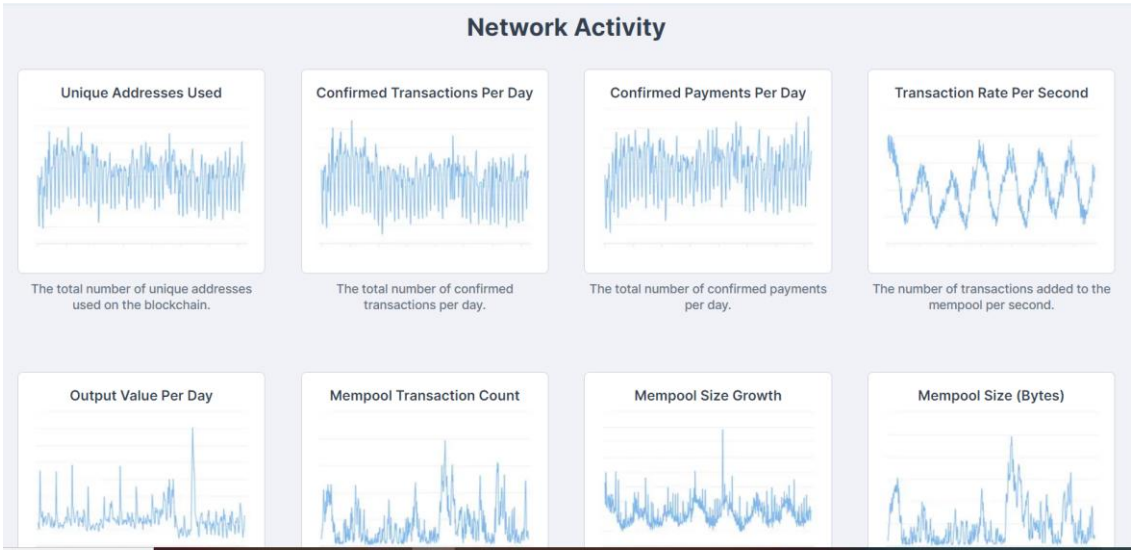
11) Overview of the current statistics containts the price related information related to the bitcoin. Individual charts can also be seen by navigating to any of the available charts.

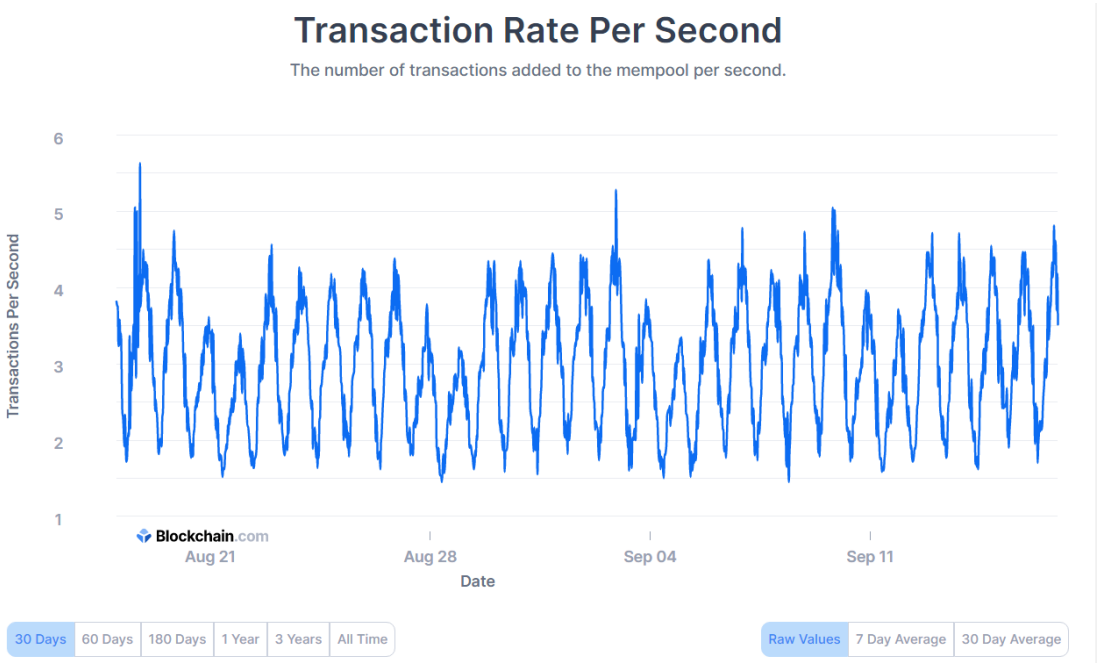
12) Following are all the charts which are available on the bitcoin explorer.

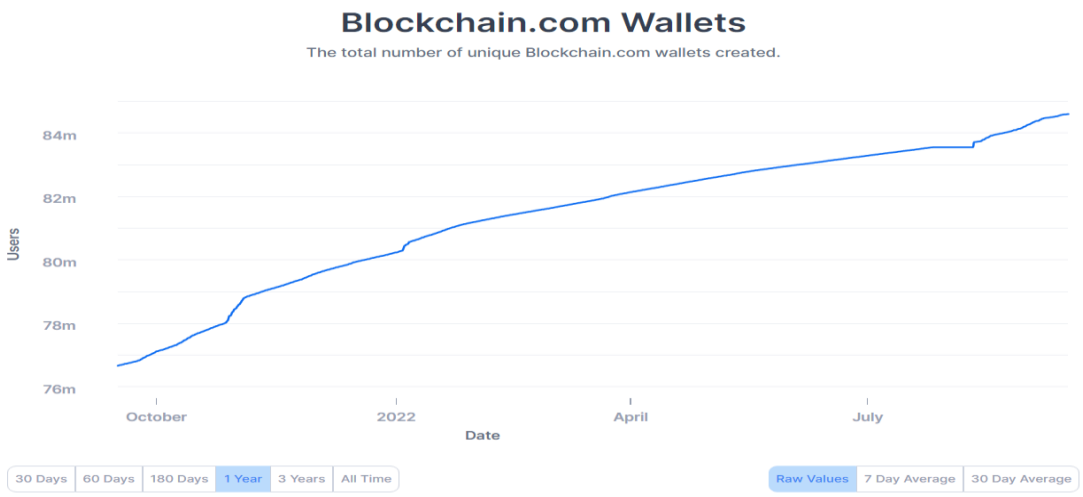




Mining Information
Total Hash Rate (TH/s)
Hashrate Distribution
Hashrate Distribution Over Time
Network Difficulty
The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.
An estimation of hashrate distribution amongst the largest mining pools.
An estimation of hashrate distribution over time amongst the largest mining pools
A relative measure of how difficult it is to mine a new block for the blockchain.
Miners Revenue (USD)
Total Transaction Fees (BTC)
Total Transaction Fees (USD)
Fees Per Transaction (USD)


Total Hash Rate (TH/s)
The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.
240m
220m
200m
180m
160m
140m
Hash Rate TH/s
Blockchain.com
October
2022
April
July
Date
30 Days
60 Days
180 Days
1 Year
3 Years
All Time
Raw Values
7 Day Average
30 Day Average

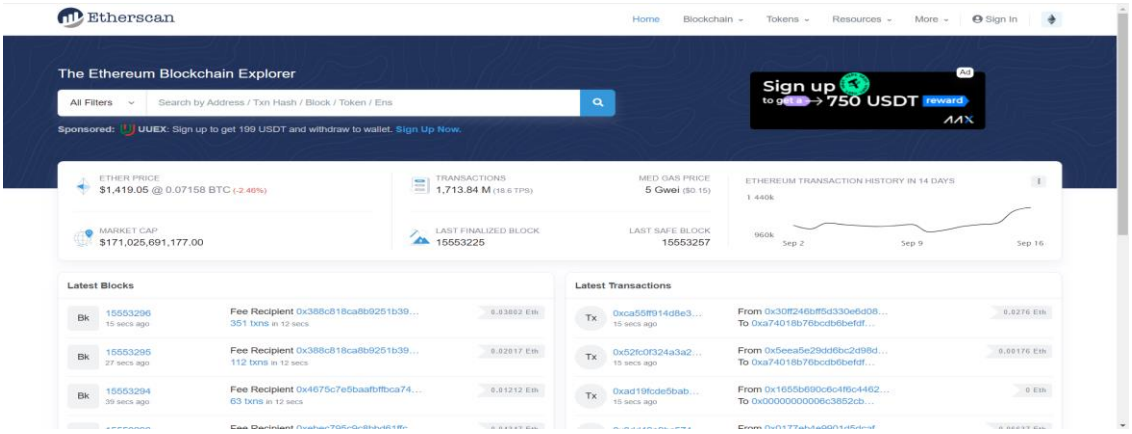

Network Activity
Unique Addresses Used
Confirmed Transactions Per Day
Confirmed Payments Per Day
Transaction Rate Per Second
The total number of unique addresses used on the blockchain.
The total number of confirmed transactions per day.
The total number of confirmed payments per day.
The number of transactions added to the mempool per second.
Output Value Per Day
Mempool Transaction Count
Mempool Size Growth
Mempool Size (Bytes)


Transaction Rate Per Second
The number of transactions added to the mempool per second.
Transactions Per Second
6
5
4
3
2
1
Blockchain.com
Aug 21
Aug 28
Sep 04
Sep 11
Date
30 Days
60 Days
180 Days
1 Year
3 Years
All Time
Raw Values
7 Day Average
30 Day Average

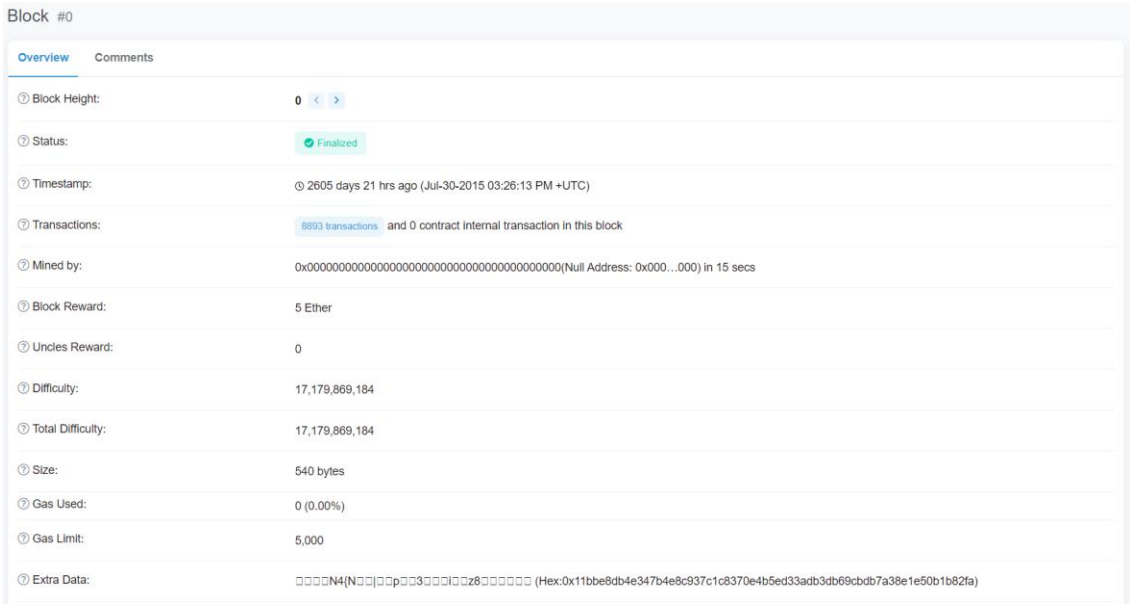

Blockchain.com Wallets
The total number of unique Blockchain.com wallets created.
Users
84m
82m
80m
78m
76m
October
2022
April
July
Date
30 Days
60 Days
180 Days
1 Year
3 Years
All Time
Raw Values
7 Day Average
30 Day Average

**Block explorer – Ethereum: [Link]**

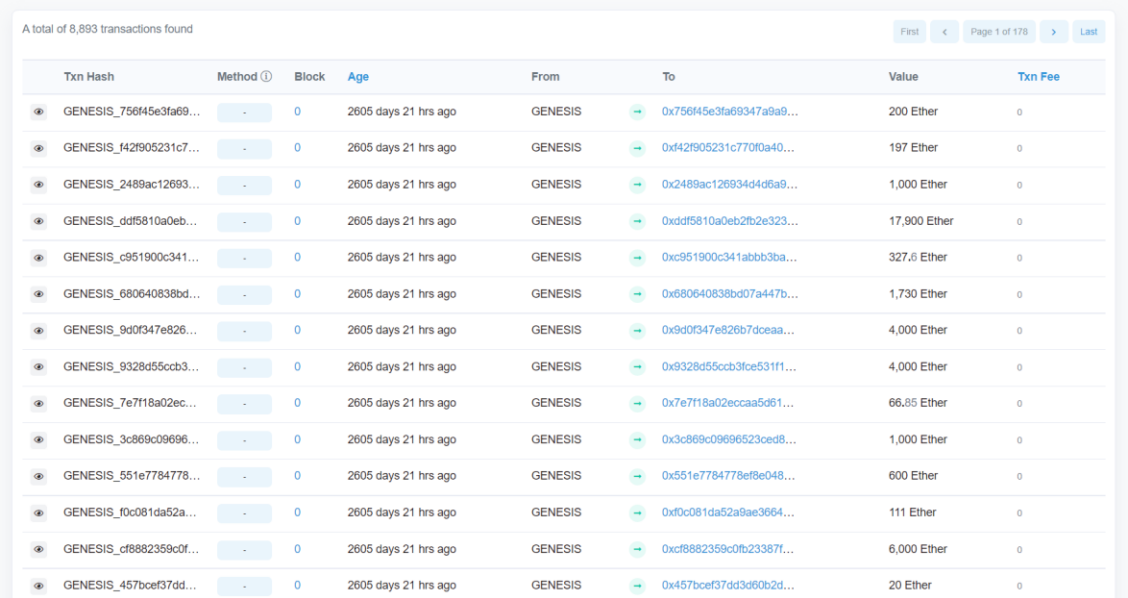
1) One of the most used cyrptocurrency is ethereum and etherscan.io provides details corresponding to ethereum blockchain.




2) Ethers blockchain contains fields such as height, timestamp, transactions, mined by, block reward, etc but it also contains other fields like uncles reward which is obtained if 2 miners are mining the same transactions, difficulty level (proof of work now changed to proof of stake), gas used which is the amount of energy required to insert the block into the ethereum main net.




3) By navigating to all the transactions inside the block we can see all the information related to all the transactions in the block under consideration. From and to addresses of transfer of ether are also available with the number of ethers transferred.

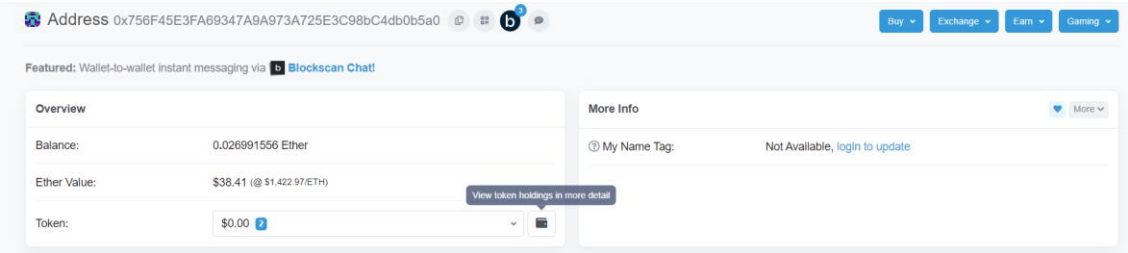


A total of 8,893 transactions found

First | Page 1 of 178 | Last

| Txn Hash | Method | Block | Age | From | To | Value | Txn Fee |
|---|---|---|---|---|---|---|---|
| GENESIS_756f45e3fa69... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0x756f45e3fa69347a9a9... | 200 Ether | 0 |
| GENESIS_f42f905231c7... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0xf42f905231c770f0a40... | 197 Ether | 0 |
| GENESIS_2489ac12693... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0x2489ac126934d4d6a9... | 1,000 Ether | 0 |
| GENESIS_ddf5810a0eb... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0xddf5810a0eb2fb2e323... | 17,900 Ether | 0 |
| GENESIS_c951900c341... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0xc951900c341abbb3ba... | 327.6 Ether | 0 |
| GENESIS_680640838bd... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0x680640838bd07a447b... | 1,730 Ether | 0 |
| GENESIS_9d0f347e826... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0x9d0f347e826b7dceaa... | 4,000 Ether | 0 |
| GENESIS_9328d55ccb3... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0x9328d55ccb3fce531f1... | 4,000 Ether | 0 |
| GENESIS_7e7f18a02ec... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0x7e7f18a02eccaa5d61... | 66.85 Ether | 0 |
| GENESIS_3c869c09696... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0x3c869c09696523ced8... | 1,000 Ether | 0 |
| GENESIS_551e7784778... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0x551e7784778ef8e048... | 600 Ether | 0 |
| GENESIS_f0c081da52a... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0xf0c081da52a9ae3664... | 111 Ether | 0 |
| GENESIS_cf8882359c0f... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0xcf8882359c0fb23387f... | 6,000 Ether | 0 |
| GENESIS_457bcef37dd... | - | 0 | 2605 days 21 hrs ago | GENESIS | 0x457bcef37dd3d60b2d... | 20 Ether | 0 |

4) By navigating to a particular address all the information associated with that address can also be seen such as balance, value in terms of dollars, tokens and name if available.



Address 0x756F45E3FA69347A9A973A725E3C98bC4db0b5a0

Buy | Exchange | Earn | Gaming

Featured: Wallet-to-wallet instant messaging via Blockscan Chat!

Overview

Balance: 0.026991556 Ether

Ether Value: $38.41 (@ $1,422.97/ETH)

Token: $0.00

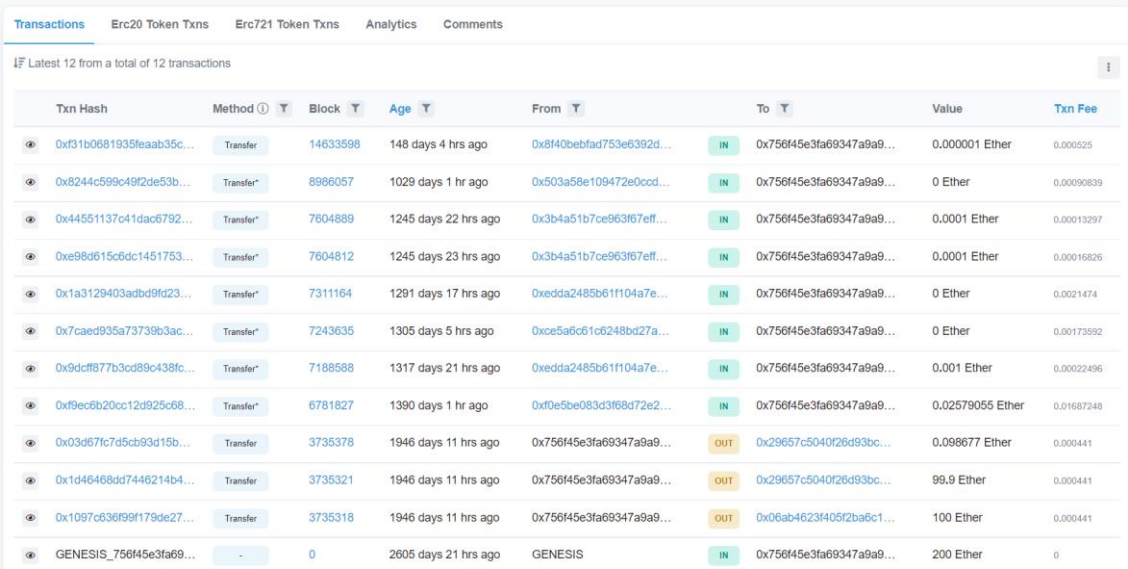
View token holdings in more detail

More Info

More

My Name Tag: Not Available, login to update

5) All the transactions associated with the particular address can also be seen at the bottom of the page with fields such as the method, transaction hash, block numbers, age (time elapsed from the time transaction has made to now), from and too addresses, amount of ethers transferred and the transaction fees applied while making the transactions.

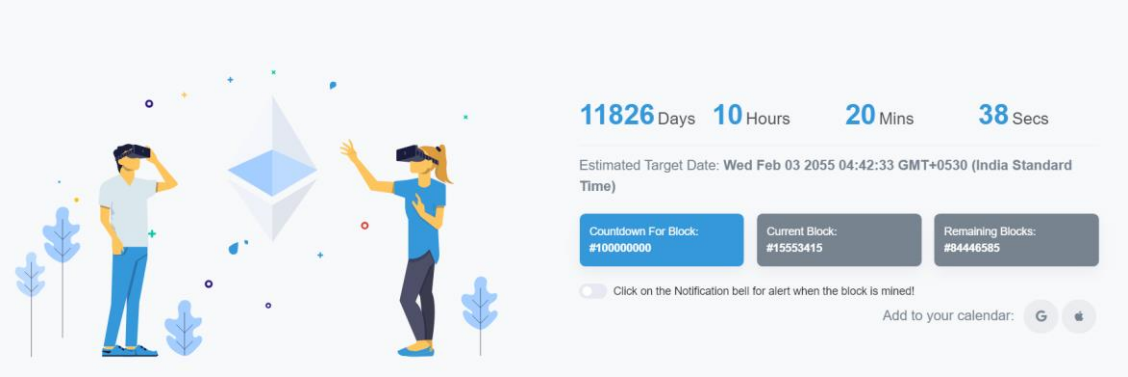


Transactions | Erc20 Token Txns | Erc721 Token Txns | Analytics | Comments

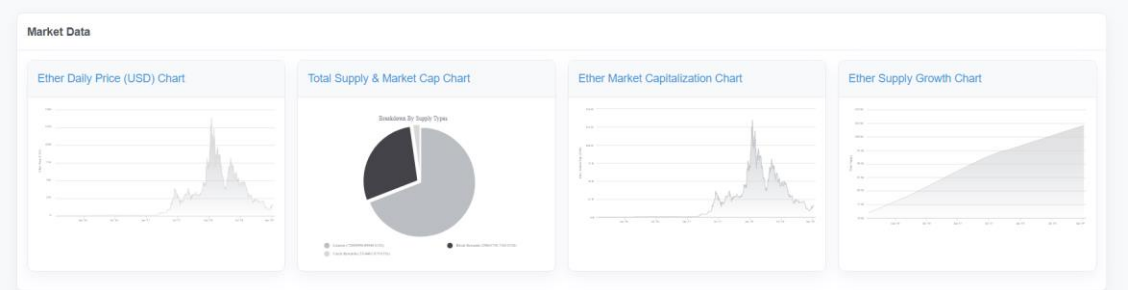
Latest 12 from a total of 12 transactions

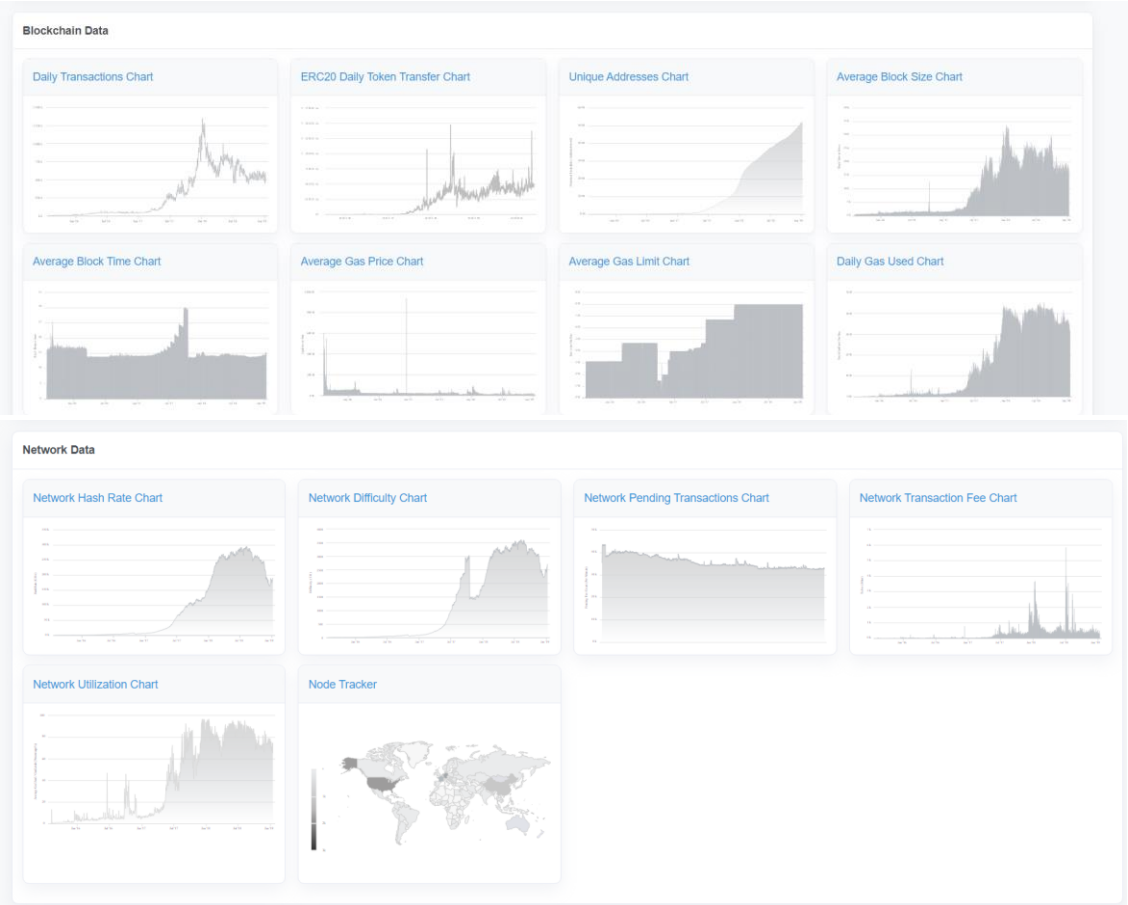
| Txn Hash | Method | Block | Age | From | | To | Value | Txn Fee |
|---|---|---|---|---|---|---|---|---|
| 0xf31b0681935feaab35c... | Transfer | 14633598 | 148 days 4 hrs ago | 0x8f40bebfad753e6392d... | IN | 0x756f45e3fa69347a9a9... | 0.000001 Ether | 0.000525 |
| 0x8244c599c49f2de53b... | Transfer | 8986057 | 1029 days 1 hr ago | 0x503a58e109472e0ccd... | IN | 0x756f45e3fa69347a9a9... | 0 Ether | 0.00090839 |
| 0x44551137c41dac6792... | Transfer | 7604889 | 1245 days 22 hrs ago | 0x3b4a51b7ce963f67eff... | IN | 0x756f45e3fa69347a9a9... | 0.0001 Ether | 0.00013297 |
| 0xe98d615c6dc1451753... | Transfer | 7604812 | 1245 days 23 hrs ago | 0x3b4a51b7ce963f67eff... | IN | 0x756f45e3fa69347a9a9... | 0.0001 Ether | 0.00016826 |
| 0x1a3129403adbd9fd23... | Transfer | 7311164 | 1291 days 17 hrs ago | 0xedda2485b61f104a7e... | IN | 0x756f45e3fa69347a9a9... | 0 Ether | 0.0021474 |
| 0x7caed935a73739b3ac... | Transfer | 7243635 | 1305 days 5 hrs ago | 0xce5a6c61c6248bd27a... | IN | 0x756f45e3fa69347a9a9... | 0 Ether | 0.00173592 |
| 0x9dcff877b3cd89c438fc... | Transfer | 7188588 | 1317 days 21 hrs ago | 0xedda2485b61f104a7e... | IN | 0x756f45e3fa69347a9a9... | 0.001 Ether | 0.00022496 |
| 0xf9ec6b20cc12d925c68... | Transfer | 6781827 | 1390 days 1 hr ago | 0xf0e5be083d3f68d72e2... | IN | 0x756f45e3fa69347a9a9... | 0.02579055 Ether | 0.01687248 |
| 0x03d67fc7d5cb93d15b... | Transfer | 3735378 | 1946 days 11 hrs ago | 0x756f45e3fa69347a9a9... | OUT | 0x29657c5040f26d93bc... | 0.098677 Ether | 0.000441 |
| 0x1d46468dd7446214b4... | Transfer | 3735321 | 1946 days 11 hrs ago | 0x756f45e3fa69347a9a9... | OUT | 0x29657c5040f26d93bc... | 99.9 Ether | 0.000441 |
| 0x1097c636f99f179de27... | Transfer | 3735318 | 1946 days 11 hrs ago | 0x756f45e3fa69347a9a9... | OUT | 0x06ab4623f405f2ba6c1... | 100 Ether | 0.000441 |
| GENESIS_756f45e3fa69... | - | 0 | 2605 days 21 hrs ago | GENESIS | IN | 0x756f45e3fa69347a9a9... | 200 Ether | 0 |

6) This is a special feature available in ethereum block explorer which is the amount of time required to make number of blocks which is mentioned by the user. If the block number enterd by the user is greater than the number of blocks in the blockchain then this explorer will give you the details of when the particular block will be available in the ethereum mainnet.

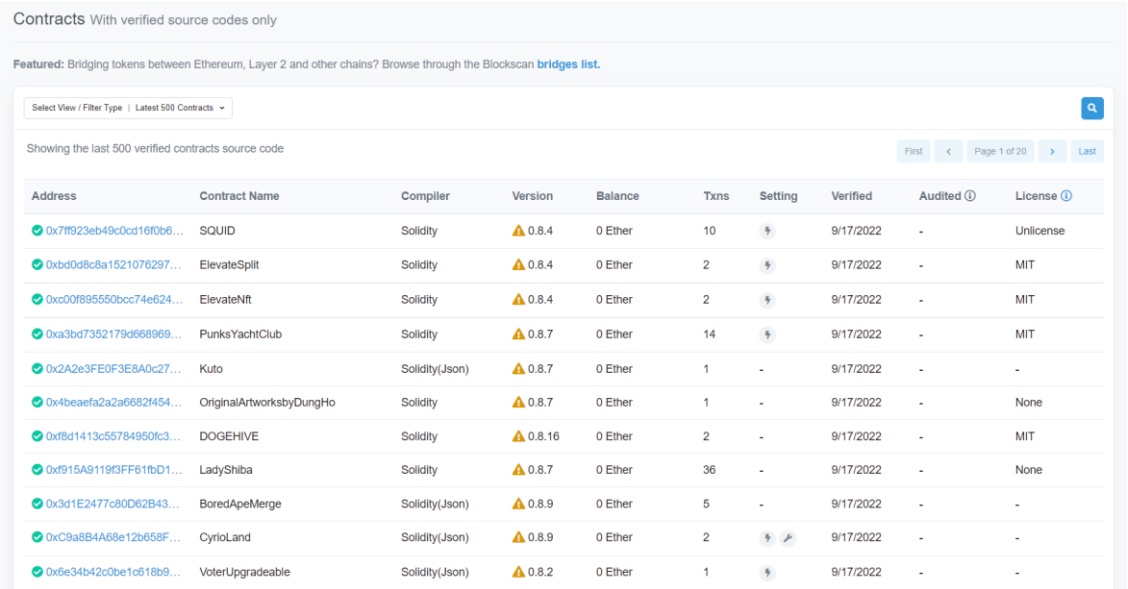



7) Ethereum block explorer also provides the hsitorical data of the ethereum in terms of charts which can be seen in the charts section.






8) There is a concept of smart contracts, which is a set of rules that determine the way the network functions, in ethereum, information related to that is also available with the name of the compiler, version, balance, transactions, date of verification, license, etc.



Contracts With verified source codes only

**Featured:** Bridging tokens between Ethereum, Layer 2 and other chains? Browse through the Blockscan **bridges list.**

Select View / Filter Type | Latest 500 Contracts

Showing the last 500 verified contracts source code

First | Page 1 of 20 | Last

| Address | Contract Name | Compiler | Version | Balance | Txns | Setting | Verified | Audited | License |
|---|---|---|---|---|---|---|---|---|---|
| 0x7ff923eb49c0cd16f0b6... | SQUID | Solidity | 0.8.4 | 0 Ether | 10 | | 9/17/2022 | - | Unlicense |
| 0xbd0d8c8a1521076297... | ElevateSplit | Solidity | 0.8.4 | 0 Ether | 2 | | 9/17/2022 | - | MIT |
| 0xc00f895550bcc74e624... | ElevateNft | Solidity | 0.8.4 | 0 Ether | 2 | | 9/17/2022 | - | MIT |
| 0xa3bd7352179d668969... | PunksYachtClub | Solidity | 0.8.7 | 0 Ether | 14 | | 9/17/2022 | - | MIT |
| 0x2A2e3FE0F3E8A0c27... | Kuto | Solidity(Json) | 0.8.7 | 0 Ether | 1 | - | 9/17/2022 | - | - |
| 0x4beaefa2a2a6682f454... | OriginalArtworksbyDungHo | Solidity | 0.8.7 | 0 Ether | 1 | - | 9/17/2022 | - | None |
| 0xf8d1413c55784950fc3... | DOGEHIVE | Solidity | 0.8.16 | 0 Ether | 2 | - | 9/17/2022 | - | MIT |
| 0xf915A9119f3FF61fbD1... | LadyShiba | Solidity | 0.8.7 | 0 Ether | 36 | - | 9/17/2022 | - | None |
| 0x3d1E2477c80D62B43... | BoredApeMerge | Solidity(Json) | 0.8.9 | 0 Ether | 5 | - | 9/17/2022 | - | - |
| 0xC9a8B4A68e12b658F... | CyrioLand | Solidity(Json) | 0.8.9 | 0 Ether | 2 | | 9/17/2022 | - | - |
| 0x6e34b42c0be1c618b9... | VoterUpgradeable | Solidity(Json) | 0.8.2 | 0 Ether | 1 | | 9/17/2022 | - | - |

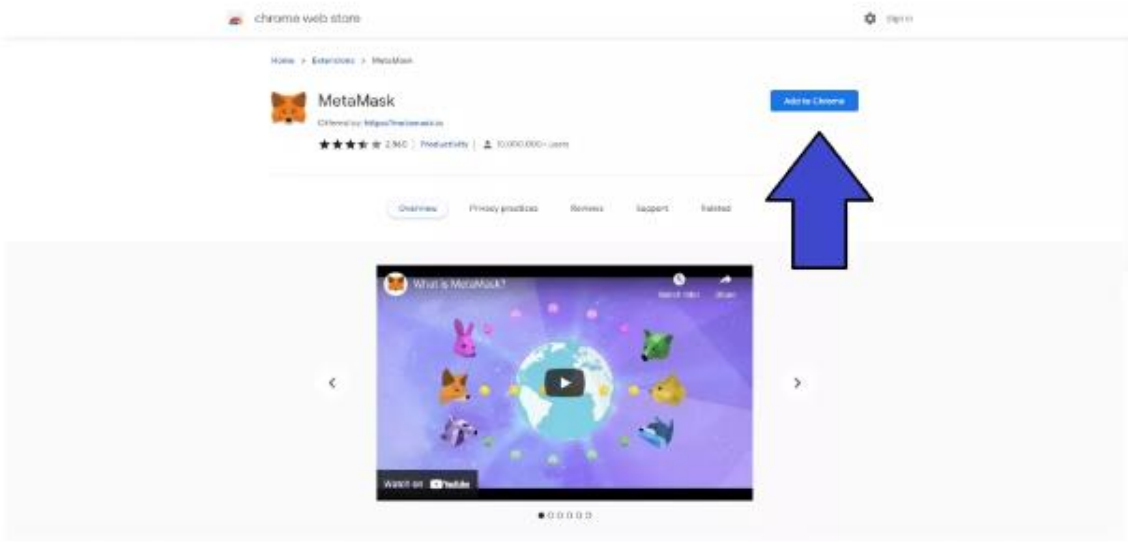
### 3. Explain the Importance of the approach followed by you

Blockchain technology is something that cannot be understood without actually watching a demo of its working, so online platforms providing these services are of great importance while working with blockchain. Some other advantages include:

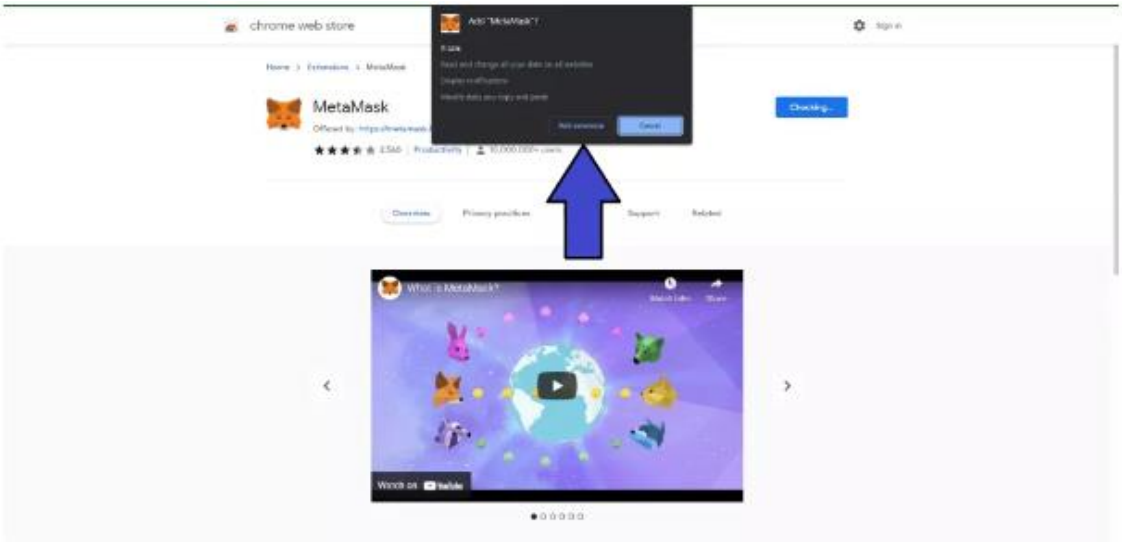
- Online platforms for learning blockchain provide good UI/UX, which is very useful for any beginner to begin learning blockchain.
- Some platforms also provide some kind of demo in video format to make users comfortable with the use of the platform. All the platforms used to complete this experiment contain a demo in video format.
- To test any blockchain network, we need some fake entities to test the blockchain, and online platforms provide that also.
- Before learning blockchain, the concepts used under blockchain have to be learned first. All the prerequisite information can also be gathered from the platforms used above.
- To explore all the things possible with blockchain, we need to go through tonnes of websites, but platforms describing blockchain contain all the information related to blockchain.

## Metamask

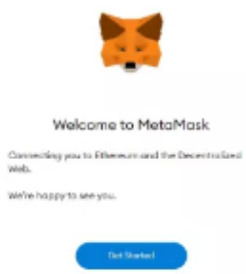
1. Go to Metamask's official website here and click on **"Install Metamask for Chrome."**
2. You should now be on Metamask's Chrome Web Store page. Click on **"Add to Chrome."**




3. A pop-up entitled "Add 'Metamask?'" should appear. Click on **"Add Extension."**



4. A new tab will appear. Click on **"Get Started."**




5. Click on **"Create a New Wallet"** under "Yes, let's get set up!"

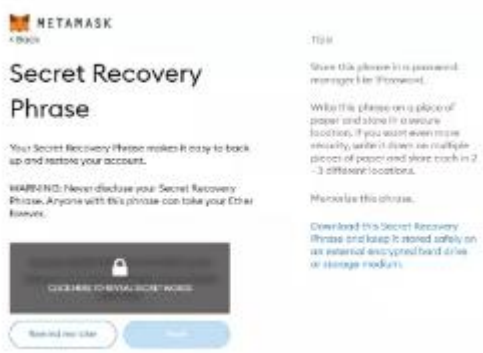

6. Metamask will then ask whether it can gather your usage data. If you accept, click, **"I Agree."** If not, click, **"No Thanks."** Selecting the latter will not affect your ability to move forward in the set up process.

How to use Metamask (Image credit: Future)

7. Create a password for Metamask. I'd suggest using a password you haven't used for other accounts. I'd also recommend using a long, complicated password. Next, tick the **"I have read and agree to the Terms of Use"** box.
8. You'll be guided to watch a short video on how to secure your Metamask wallet, which involves a writing down and storing a secret recovery phrase (a string of 12

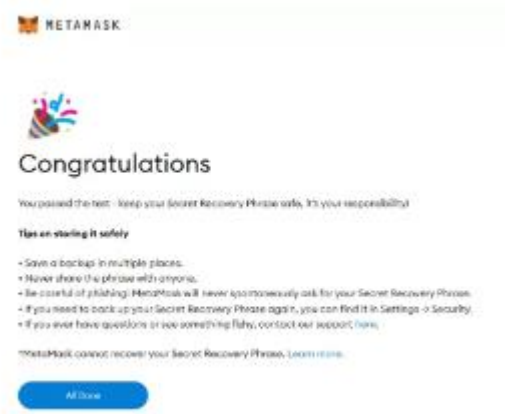
words that gives you, or anyone else who has it, access to your Metamask wallet and its contents). Hit "**Next.**"

9. You'll land on a page that has your 12-word recovery phrase. Click on the greyed out area to reveal it. Once you've written it down, hit **"Next."**




10. Confirm your secret recovery phrase by putting the 12 words in the right order. Click **"Confirm."**

11. Once you've completed step 10, you'll land on a page that says, **"Congratulations!"** You officially have a Metamask wallet that's ready to go. Click on **"All done."**



## Virtual Labs

## Virtual lab 1 – Three Pillars of Blockchain: Link

Three Pillars of Blockchain

### Aim

In this experiment, the user will learn about Blockchain and its three pillars that are decentralization, transparency & immutability. The simulator will also demonstrate the relation between blocks and chain. Apart from that, he/she will also be able to explain and apply the concepts of blockchain with the help of open and distributed ledger.

### Theory

#### 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. 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.

# Pre Test

**What is a blockchain?**

- a : A type of cryptocurrency
- b : A distributed ledger on a peer to peer network
- c : An exchange
- d : A centralized ledger

**Who created Bitcoin?**

- a : Samsung
- b : John Mcafee
- c : Satoshi Nakamoto
- d : None of the above

**What is a miner?**

- a : Computers that validate and process blockchain transactions
- b : A person doing calculations to verify a transaction
- c : A type of blockchain
- d : An algorithm that predicts the next part of the chain

**What is a genesis block?**

- a : A famous block that hardcoded a hash of the Book of Genesis onto the blockchain
- b : The 2nd transaction of a blockchain
- c : The first block of a Blockchain
- d : None of the above

**According to the blockchain mechanism, which statement is true?**

- a : All the people receive transactions simultaneously
- b : Only the person receives the transaction
- c : Both are correct
- d : None of these

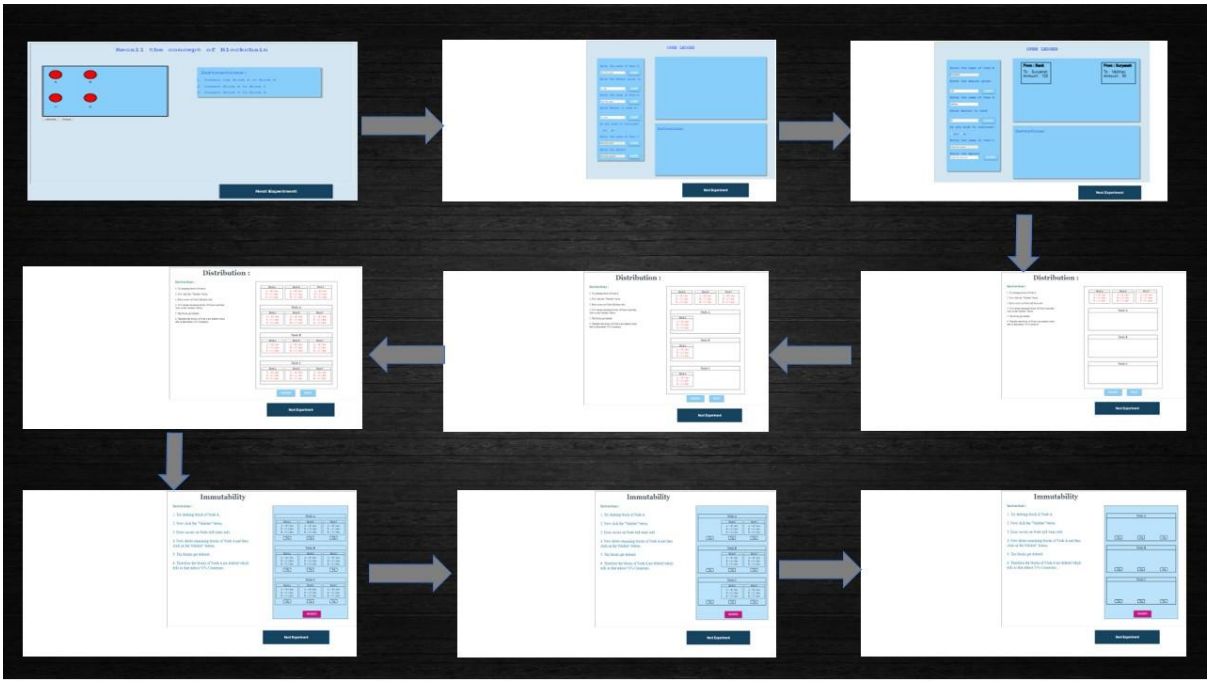
Submit Quiz

5 out of 5

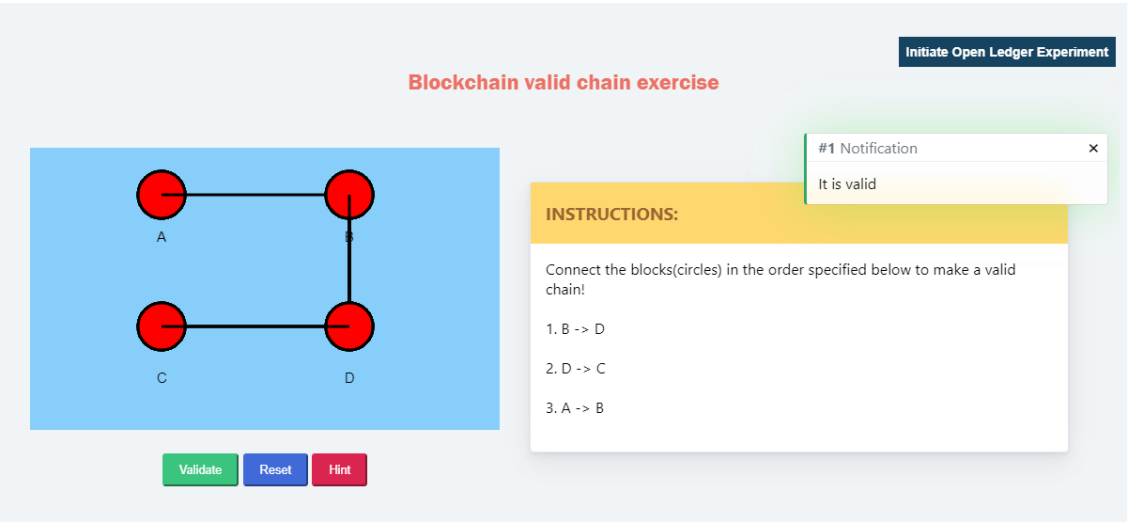
## Procedure

**Steps of simulator**

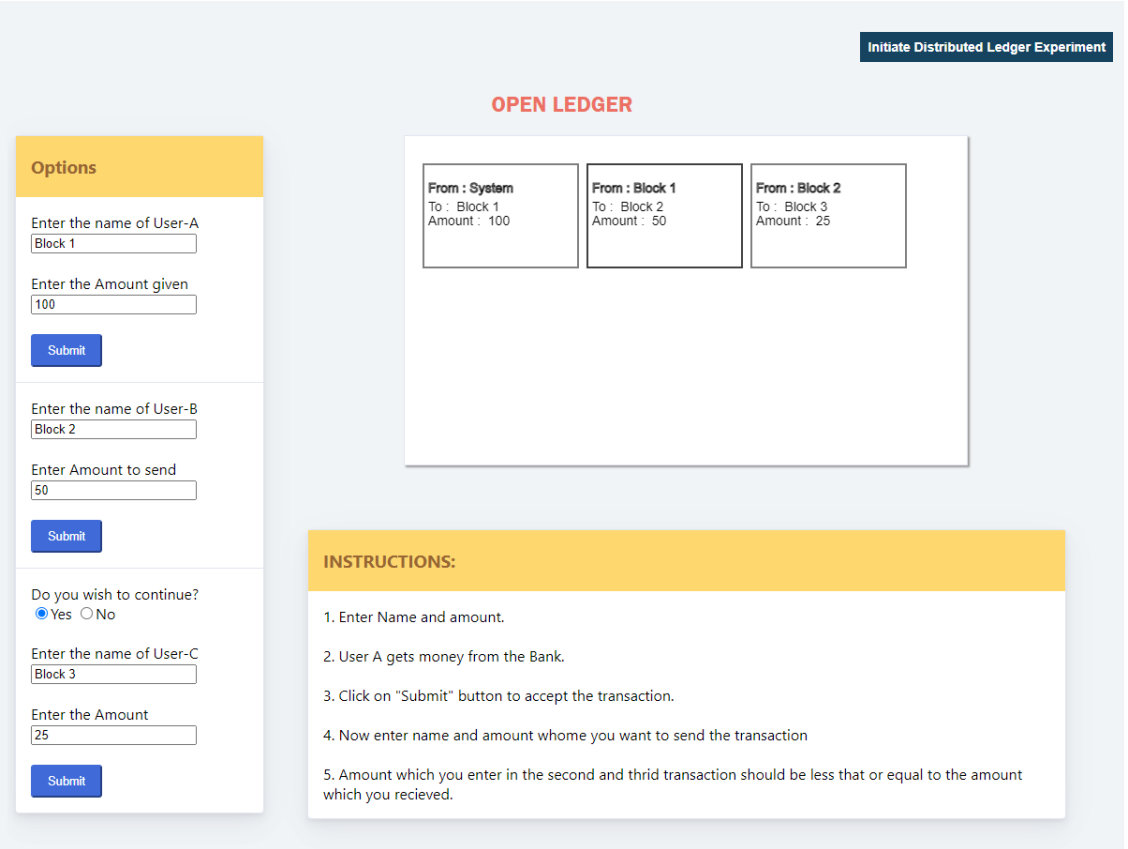
1. First complete the recall task as per the instructions given on the page.Then click on next button on the top of the page.
2. To Understand the concept of open ledger, Enter the Name and Amount of the sender as well as the recipient in the placeholder.
3. Click on the Submit button to complete the 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.



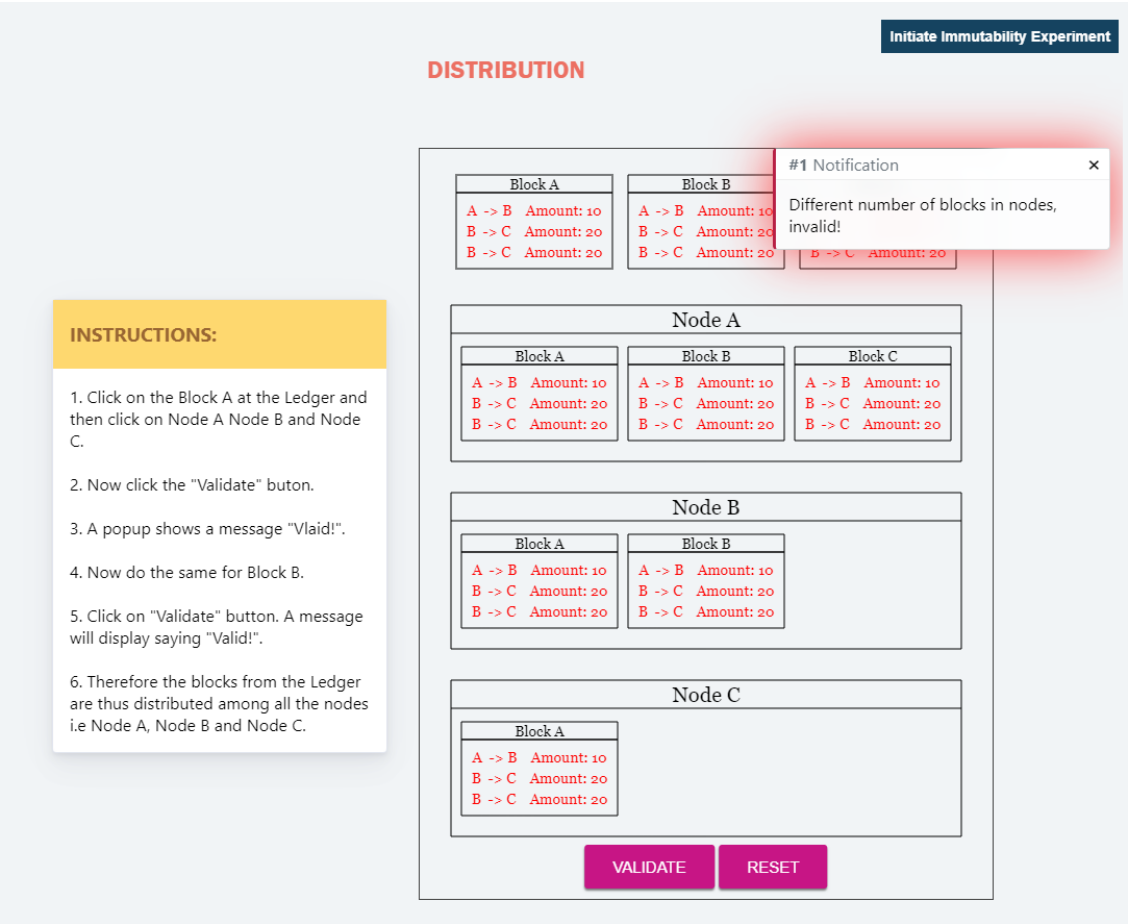
## 1) Blochchain validity

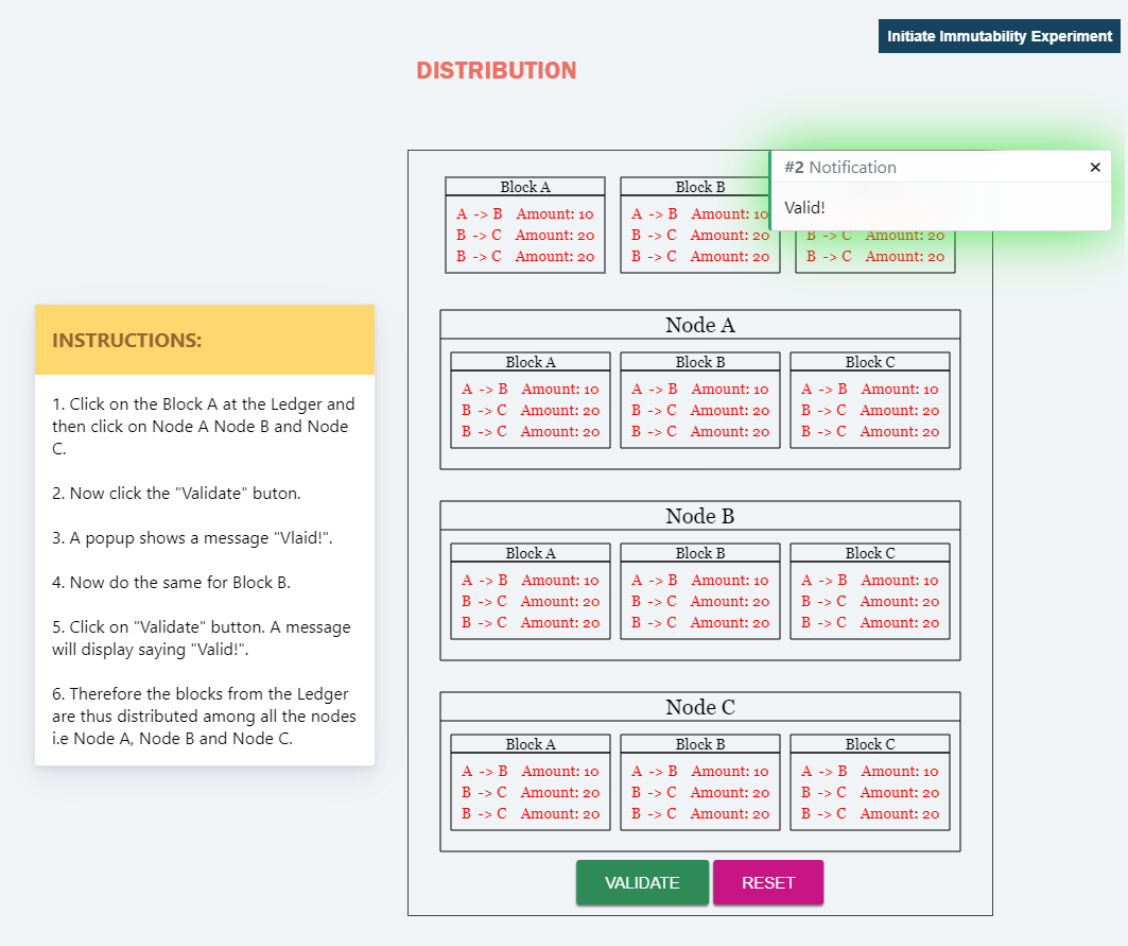



## 2) Open ledger

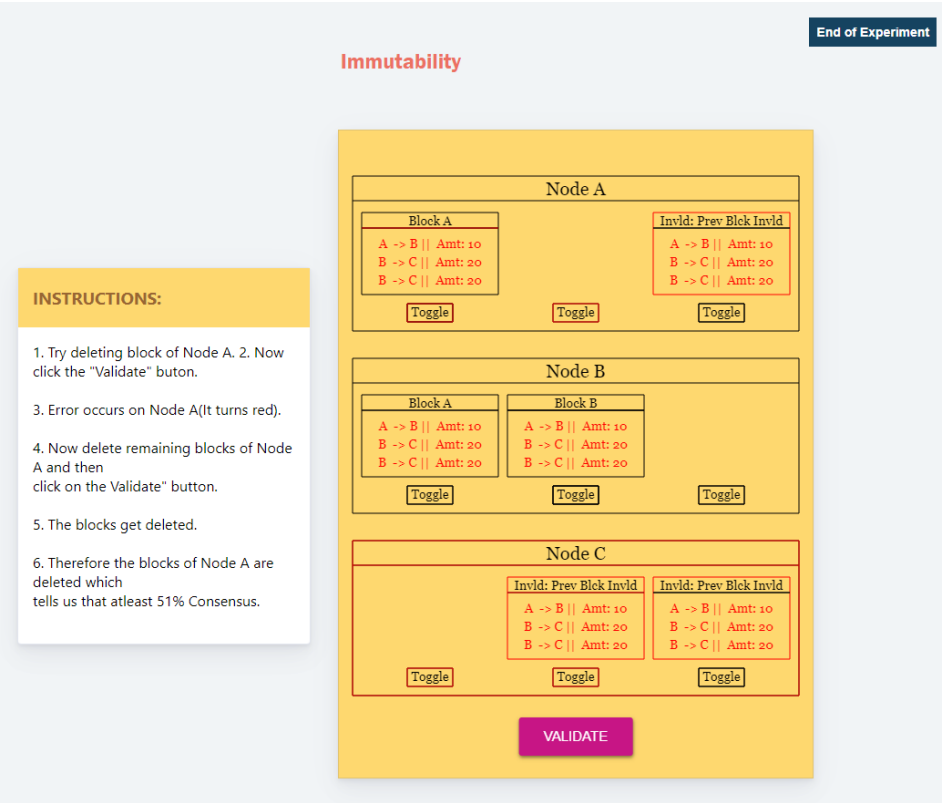


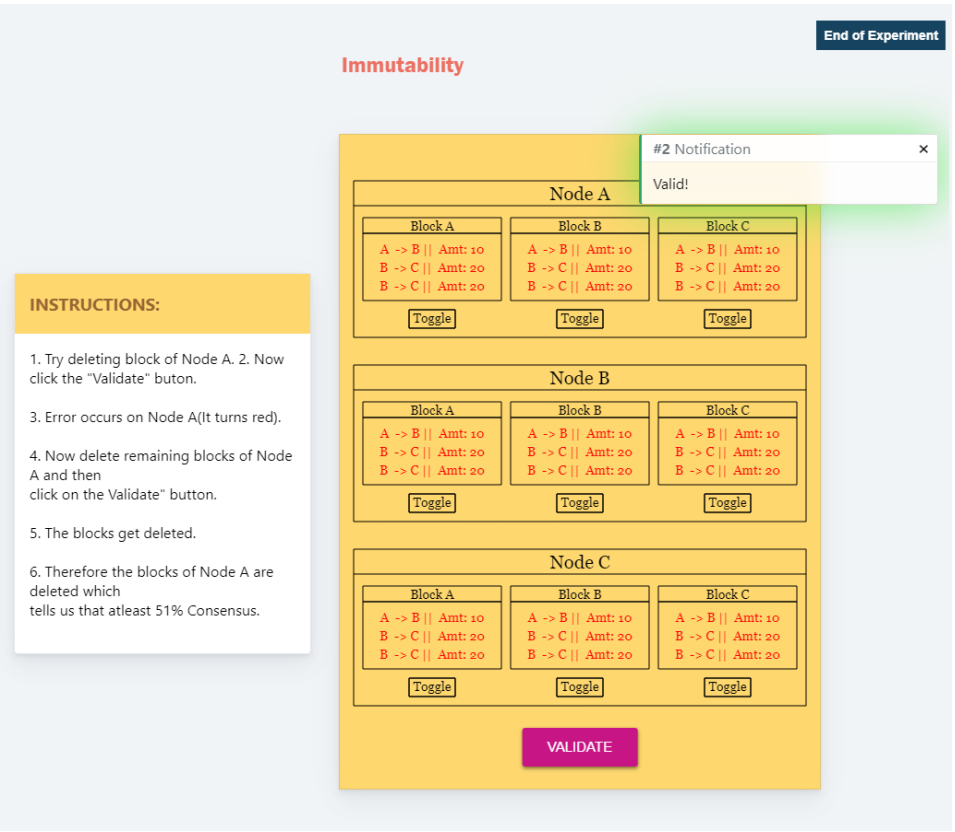
## 3) Distributed ledger




Initiate Immutability Experiment
DISTRIBUTION
#2 Notification
Valid!
Block A
A -> B Amount: 10
B -> C Amount: 20
B -> C Amount: 20
Block B
A -> B Amount: 10
B -> C Amount: 20
B -> C Amount: 20
B -> C Amount: 20
B -> C Amount: 20
INSTRUCTIONS:
1. Click on the Block A at the Ledger and then click on Node A Node B and Node C.
2. Now click the "Validate" buton.
3. A popup shows a message "Vlaid!".
4. Now do the same for Block B.
5. Click on "Validate" button. A message will display saying "Valid!".
6. Therefore the blocks from the Ledger are thus distributed among all the nodes i.e Node A, Node B and Node C.
Node A
Block A
Block B
Block C
Node B
Block A
Block B
Block C
Node C
Block A
Block B
Block C
VALIDATE
RESET

## 4) Immutability



# Post Test

**Which of these statements are true for open ledger?**

- a : Every one has copy of ledger.
- b : Ledger can be viewed by anyone. (selected)
- c : Ledger is mutable.
- d : None Of these

**Which of the following is true for distributed ledger?**

- a : Everyone has a copy of ledger (selected)
- b : There is one copy of the ledger
- c : Ledger is mutable.
- d : None of these

**A miner has completed the mining what will be the next step?**

- a : Wait for second miner to complete
- b : Wait for all members to complete
- c : Validate the transaction and add it to the ledger (selected)
- d : None of the above

**What is not a ledger type in blockchain?**

- a : Distributed Ledger
- b : Open Ledger
- c : Both a and b
- d : None of these (selected)

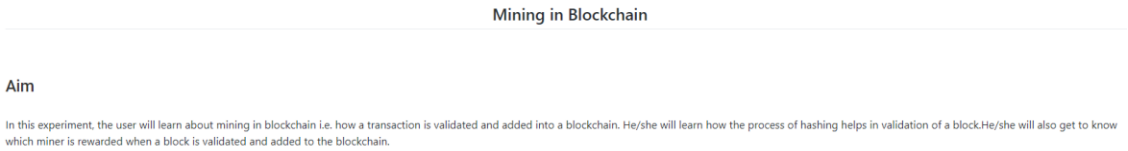
**How can a user successfully modify a blockchain?**

- a : It is immutable
- b : By simply deleting the block
- c : By use of consensus algorithm (selected)
- d : None of the above

Submit Quiz

5 out of 5

**Virtual lab 2 – Mining in Blockchain: Link**



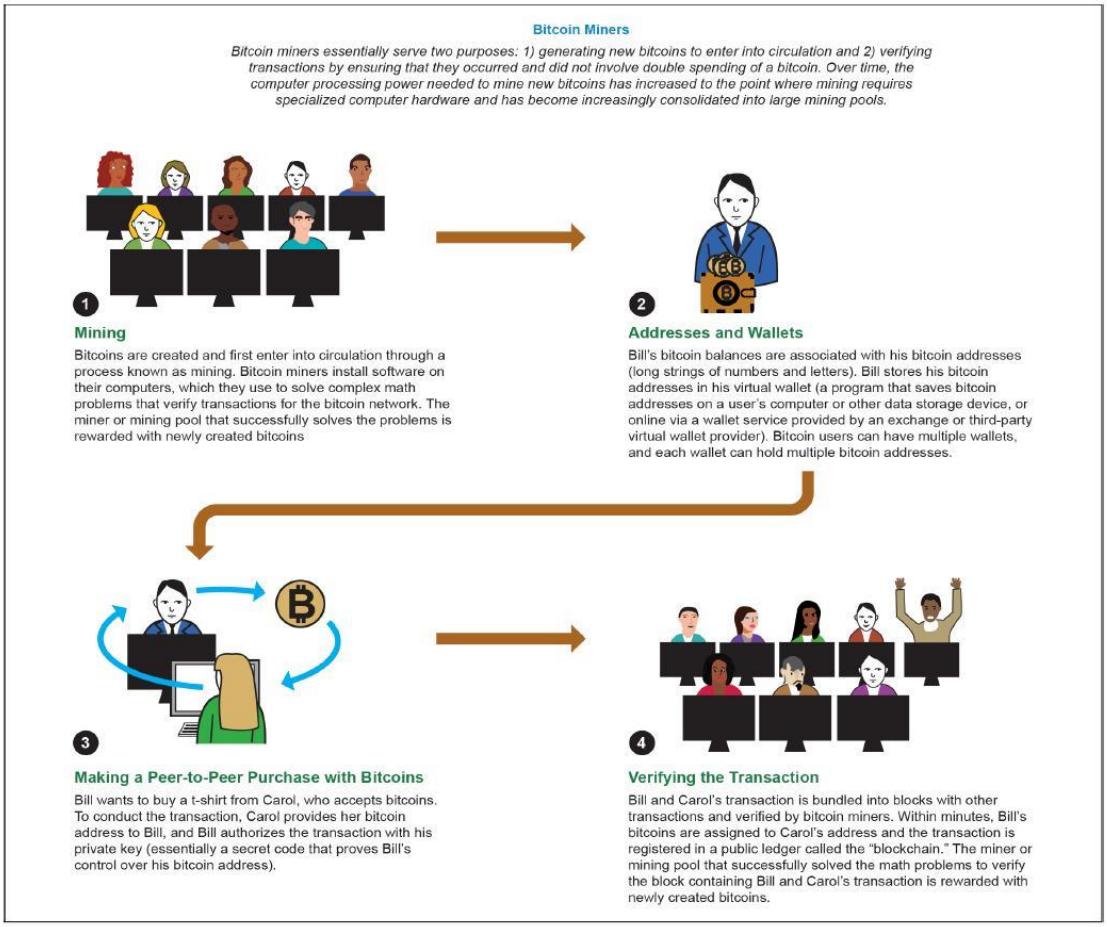

## Theory

### 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.

## Some Basic Algorithmic Rules Used

### SHA-256 and ECDSA

SHA-256 or Secure Hash Algorithm-256 bit is a type of hash function which is commonly used in Blockchain. SHA-256 changes an input from the user to a string which is a mixture of numbers and letter which is created through a cryptographically secure hashing function which is almost 0% similar to the input. SHA-256 is the strongest hash function available in the current scenario and it is a successor of SHA-1.
Eg:- SHA-256 hash of 'abc' will be 'ba7816bf8f01cfea414140de5dae2223b00361a3-96177a9cb410ff61f20015ad'
ECDSA stands for Elliptic Curve Digital Signature Algorithm. ECDSA consists of three parts.

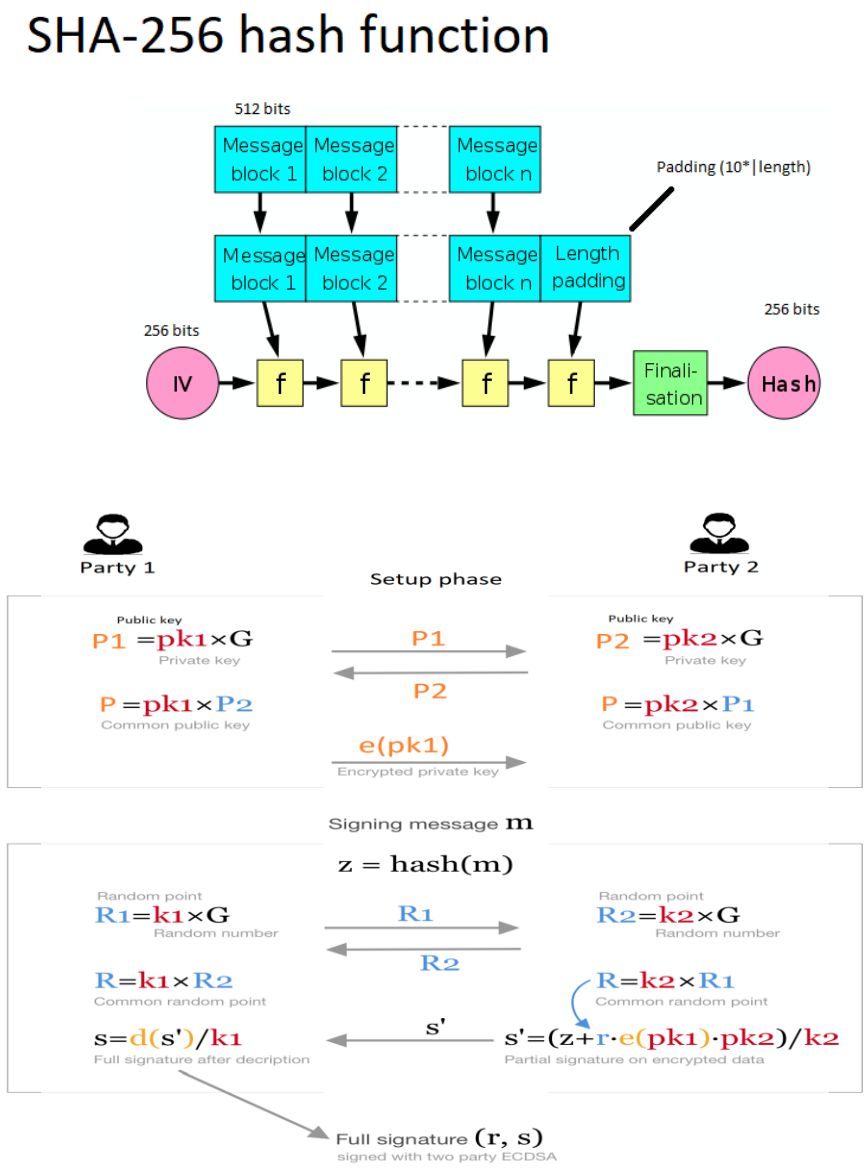
- Private Key
- Public Key
- Signature

**Private Key :-** It is a number in form of secret key which is known only to the person

who owns it and does transactions. Private Key is a randomly generated number which is a single unsigned 256 bit integer.

**Public Key :-** It is a number generated from Private Key but is not kept secret. A public Key can be determined from Private Key but Private Key cannot be determined from Public Key. A Public Key can be used to determine whether a Signature is genuine or not without requiring Private Key.

**Signature :-** It is a number that confirms about a signing operation taking place. A Signature is a mathematically generated hash of the signed number and Priavte Key. A Public Key is used to determine whether the signature entered is genuine or not which provides security to the transactions.



## Pre Test

**Which key is used for Asymmetric Cryptography?**

- a : Public Key
- b : Private Key
- c : Both public and private keys
- d : None of the above

**The full form of SHA is?**

- a : Social Hash Algorithm
- b : Secure Hash Algorithm
- c : System Hash Algorithm
- d : None of the above

**Which of the following is a full form of P2P?**

- a : Peer to Peer
- b : Public key to Public key
- c : Private key to Public key
- d : None of the above

**Where can you reserve your cryptocurrrency?**

- a : Rerserve Bank of India
- b : Wallet
- c : Compact Disk (CD)
- d : Both (a) and (b)

**Identify the correct statement?**

- a : Blockchain is centralized
- b : Blockchain is mutable
- c : Both a and b
- d : None of these

**What is a miner?**

- a : A type of blockchain
- b : An algorithm that predicts the next part of the chain
- c : A person doing calculations to verify a transaction
- d : Computers that validate and process blockchain transactions

**What is the process of creating new bitcoins popularly known as?**

- a : Finding
- b : Panning
- c : Sourcing
- d : Mining

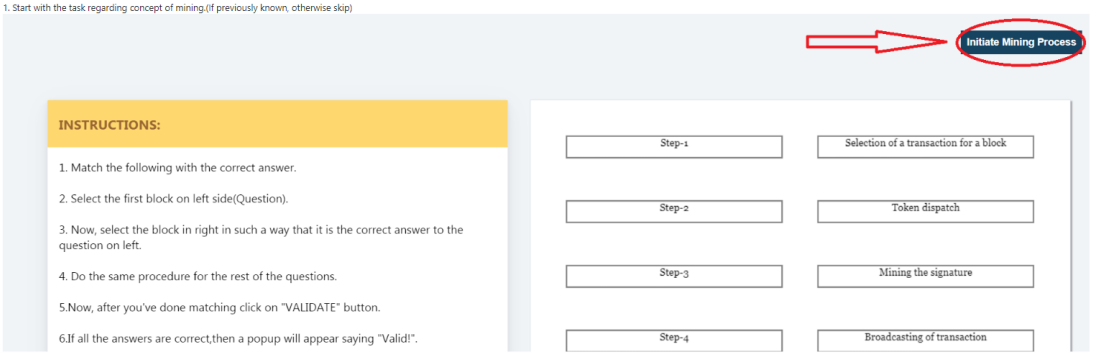
Submit Quiz

7 out of 7

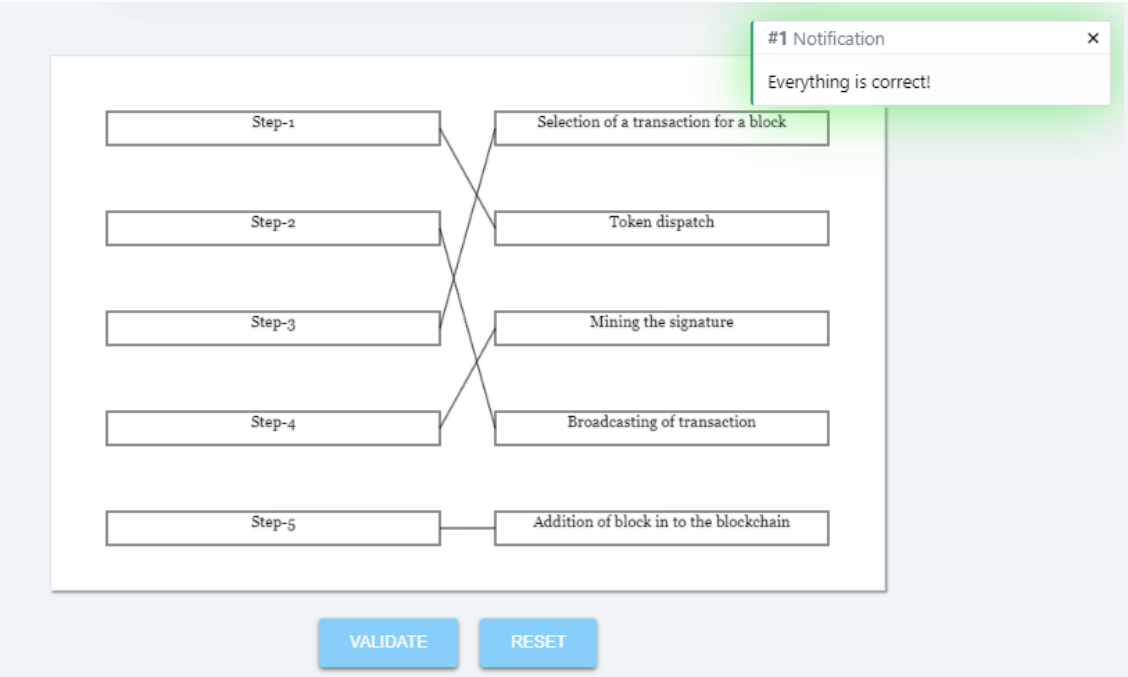
Procedure

Steps of simulator

1. Start with the task regarding concept of mining.(If previously known, otherwise skip)




2. Match the following with the correct answer.
3. Select the first block on left side(Step number).
4. Now, select the block in right in such a way that it is the correct position on left.
5. Do the same procedure for the rest of the steps.
6. Now, after you've done matching click on "VALIDATE" button.
7. If all the answers are correct,then a popup will appear saying "Valid!".
8. If popup shows "Not Valid!" then reset the test by cicking on "RESET" button to restart the test.
9. Now click on initiate mining process to go to the next part.
10. 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. The illustration will take place according to the inputs given by the user.
13. Complete the same process for the next user.
14. Click on the start mining process button, to start the mining process.
15. Click on the reset button to reset all the details that were entered by the user.
16. The instruction pane will also be there to make the user understand about the basic process that is happening in the simulator.



**1) Initiate mining**

**Instructions:**

1. Enter the name of User-A(Sender) and User-B(Reciever) to send transaction.

2. Now click on the button "ADD TO BLOCK".

3. The details you entered will appear on the block.

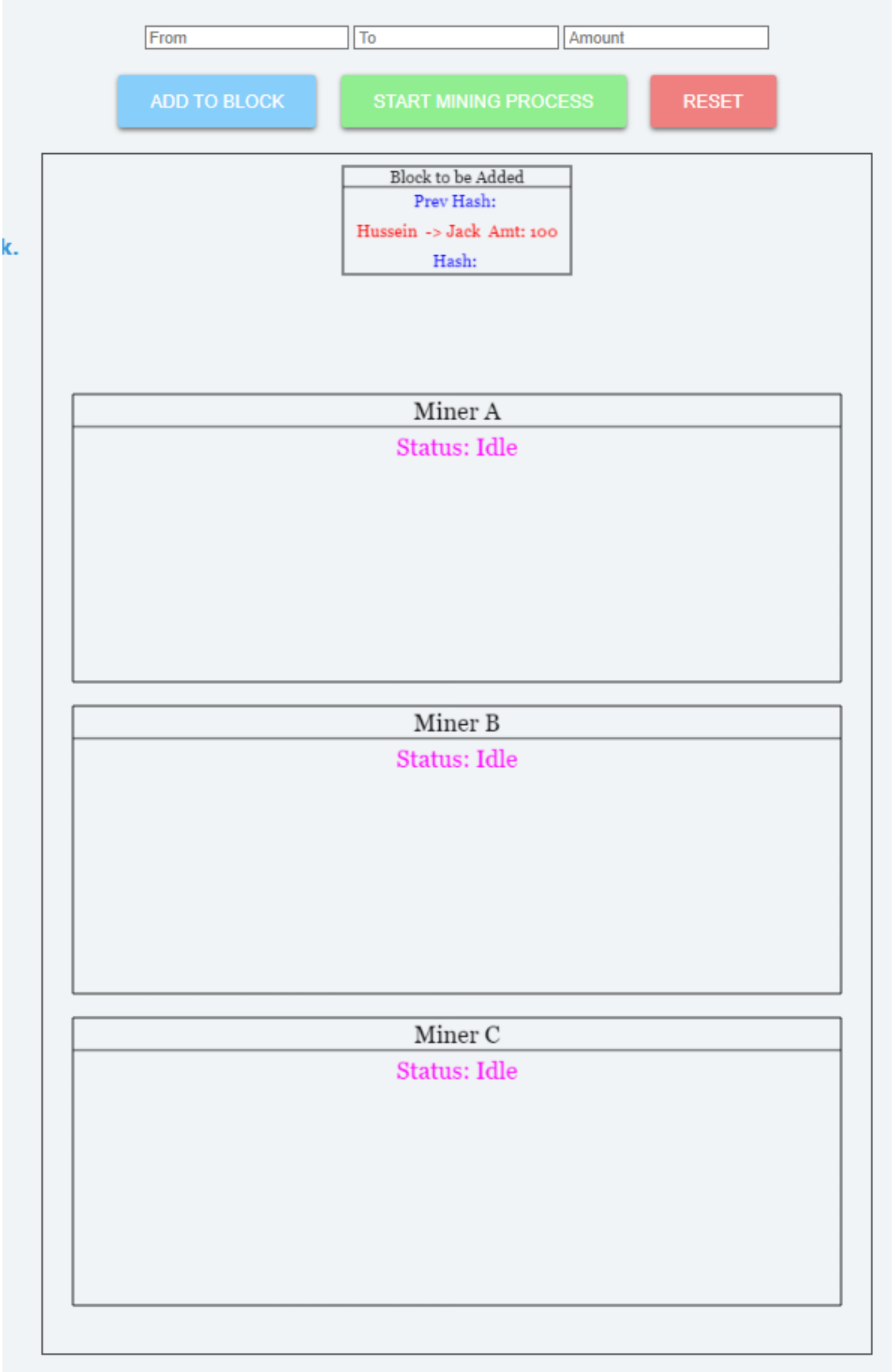
4. Now click on the button "START MINING PROCESS".

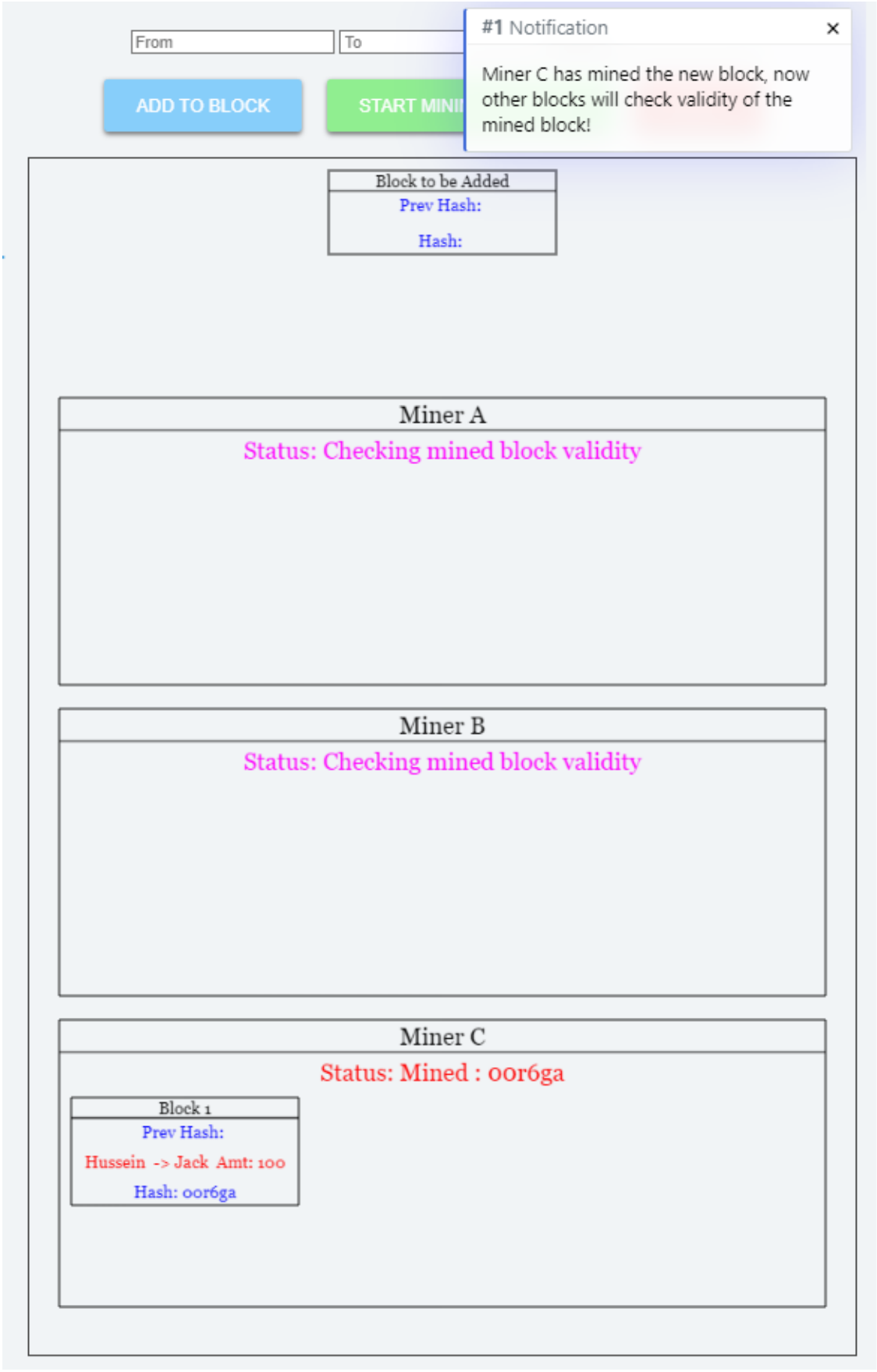
5.Mining process will start. Miner A,Miner B and Miner C will start calculating the proper Hash .

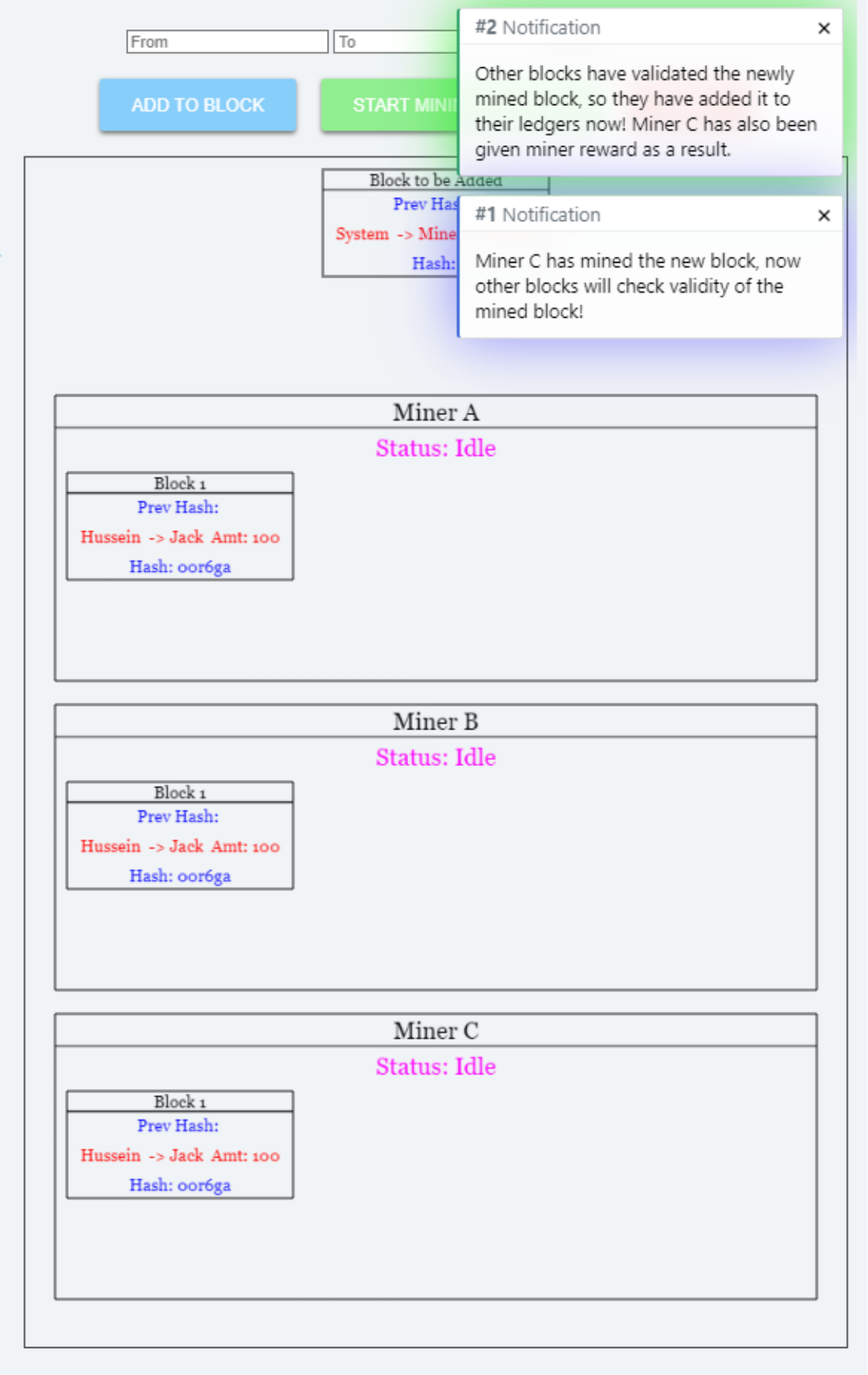
6.One of the miner completes the mining process and other miners confirm the hash calculated.

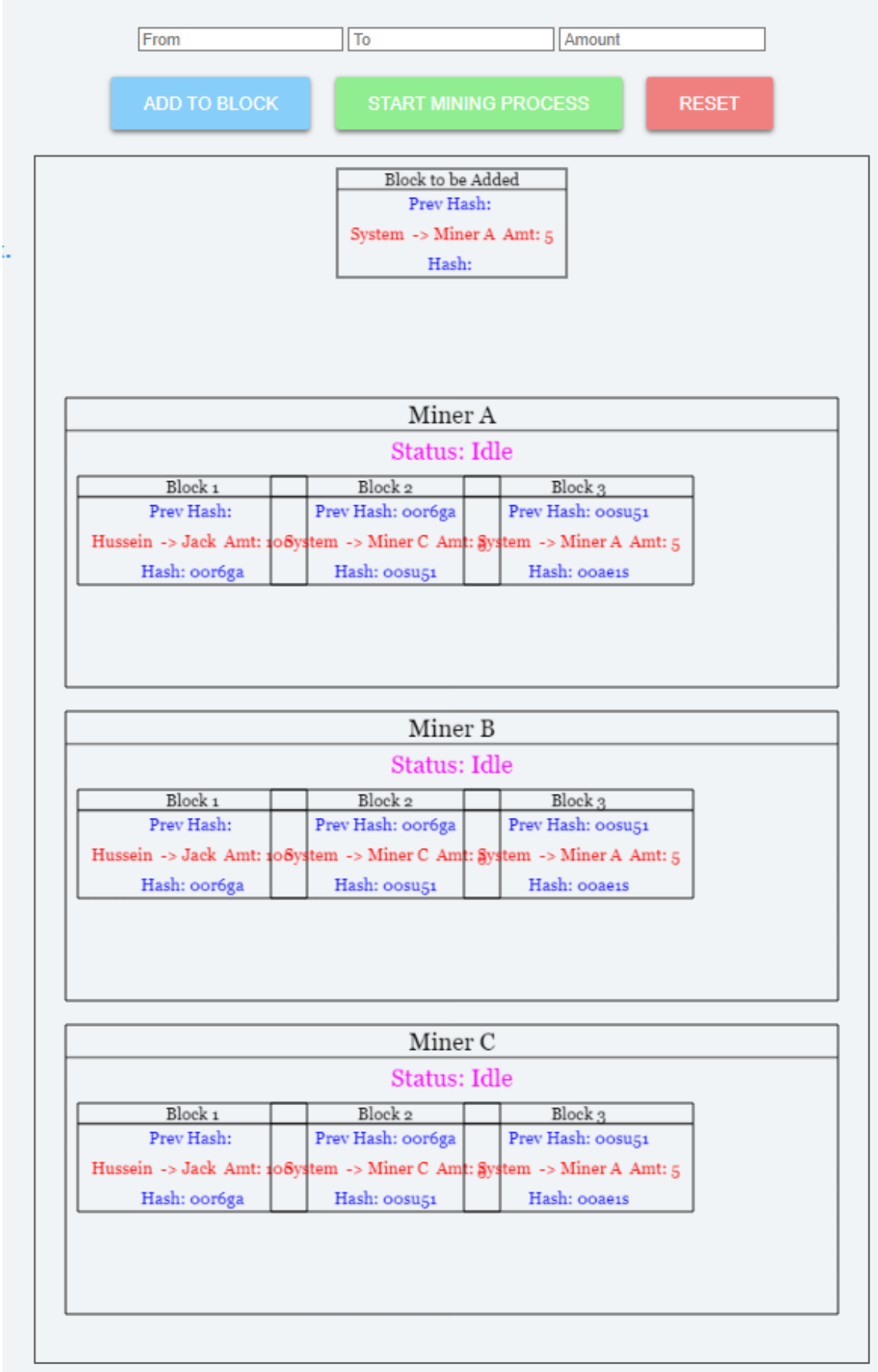
7. Click on "RESET" button to do the experiment again.

Algorithm used


From
To
Amount
ADD TO BLOCK
START MINING PROCESS
RESET
Block to be Added
Prev Hash:
Hussein -> Jack Amt: 100
Hash:
Miner A
Status: Idle
Miner B
Status: Idle
Miner C
Status: Idle


From
To
ADD TO BLOCK
START MINI
#1 Notification
Miner C has mined the new block, now other blocks will check validity of the mined block!
Block to be Added
Prev Hash:
Hash:
Miner A
Status: Checking mined block validity
Miner B
Status: Checking mined block validity
Miner C
Status: Mined : 00r6ga
Block 1
Prev Hash:
Hussein -> Jack Amt: 100
Hash: 00r6ga


From
To
ADD TO BLOCK
START MINI
#2 Notification
Other blocks have validated the newly mined block, so they have added it to their ledgers now! Miner C has also been given miner reward as a result.
Block to be Added
Prev Has
System -> Mine
Hash:
#1 Notification
Miner C has mined the new block, now other blocks will check validity of the mined block!
Miner A
Status: Idle
Block 1
Prev Hash:
Hussein -> Jack Amt: 100
Hash: oor6ga
Miner B
Status: Idle
Block 1
Prev Hash:
Hussein -> Jack Amt: 100
Hash: oor6ga
Miner C
Status: Idle
Block 1
Prev Hash:
Hussein -> Jack Amt: 100
Hash: oor6ga


From
To
Amount
ADD TO BLOCK
START MINING PROCESS
RESET
Block to be Added
Prev Hash:
System -> Miner A Amt: 5
Hash:
Miner A
Status: Idle
Block 1
Prev Hash:
Hussein -> Jack Amt: 10
Hash: oor6ga
Block 2
Prev Hash: oor6ga
System -> Miner C Amt: 8
Hash: oosu51
Block 3
Prev Hash: oosu51
System -> Miner A Amt: 5
Hash: ooae1s
Miner B
Status: Idle
Block 1
Prev Hash:
Hussein -> Jack Amt: 10
Hash: oor6ga
Block 2
Prev Hash: oor6ga
System -> Miner C Amt: 8
Hash: oosu51
Block 3
Prev Hash: oosu51
System -> Miner A Amt: 5
Hash: ooae1s
Miner C
Status: Idle
Block 1
Prev Hash:
Hussein -> Jack Amt: 10
Hash: oor6ga
Block 2
Prev Hash: oor6ga
System -> Miner C Amt: 8
Hash: oosu51
Block 3
Prev Hash: oosu51
System -> Miner A Amt: 5
Hash: ooae1s

## Post Test

**Which statement is correct?**

- a : Mining is a process of adding transactions in a ledger
- b : SHA-256 is the only cryptographic algorithm used in blockchain
- c : Both a and b
- d : None Of the above

**Which is not an advantage of blockchain technology?**

- a : Anonymity & Privacy
- b : Mutability
- c : Low transaction cost
- d : Digital freedom and decntralization

**Initial miner has completed the mining process, what will be the next step?**

- a : Wait for the next miner to complete
- b : Terminate the process
- c : Validate the transaction and add it to the ledger
- d : None of the above

**Which of the following listed is not involved in mining?**

- a : Hash Value
- b : Hash function
- c : Sender and Reciever
- d : None of the above

**Which statement is not correct?**

- a : Mining is not done in blockchain
- b : Ledger is related to the process of mining
- c : Both a and b
- d : None of the above

**The block in the blockchain consist of?**

- a : A hash pointer to the previous block
- b : Timestamp
- c : List of transactions
- d : All of the above

**The main advantage of immutability is_____.**

- a : Scalability
- b : Improved Security
- c : Tamper Proof
- d : Increased Efficiency

Submit Quiz

7 out of 7

**Virtual lab 3 – Proof of Work (PoW) & Proof of Stake (PoS): Link**

Proof of Work (PoW) & Proof of Stake (PoS)

Aim

In this experiment, the user will learn about Proof of Stake and Proof of Work. The simulator will demonstrate the working of both these algorithms by one short example of each concept. Apart from that, he/she will also be able to recall concepts with the help of a Fill in the Blanks exercise.

## Theory

### Blockchain Technology

A block chain 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 Block chain, 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.

### 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.

## Pre Test

**Which statement is not correct?**

- a : Mining is related to PoW
- b : Mining is related to PoS
- c : PoS is an alternative to PoW
- d : None of the above

**Which statement are correct?**

- a : Ledger is a component of Mining
- b : Ledger is not a concept of Mining
- c : Hashing is related to ledger
- d : PoW is Proof of work

**How mining is done?**

- a : Through Hashing
- b : Through Adding to blocks, Hashing
- c : Through Adding of blocks, Hash of current block, Hash of Previous block
- d : None of the above

**Full form of PoS is?**

- a : Privacy of Stake
- b : Proof of Stack
- c : Proof of Stake
- d : None of the above

**Pillars of blockchain are?**

- a : Centralization, Mutability, Transparency
- b : Decentralization, Immutability, Transparency
- c : Confidentiality, Integrity, availability
- d : None of these

**What is a hash?**

- a : A type of blockchain
- b : An algorithm that predicts the next part of the chain
- c : Function that convert input string into encrypted output
- d : None of the above

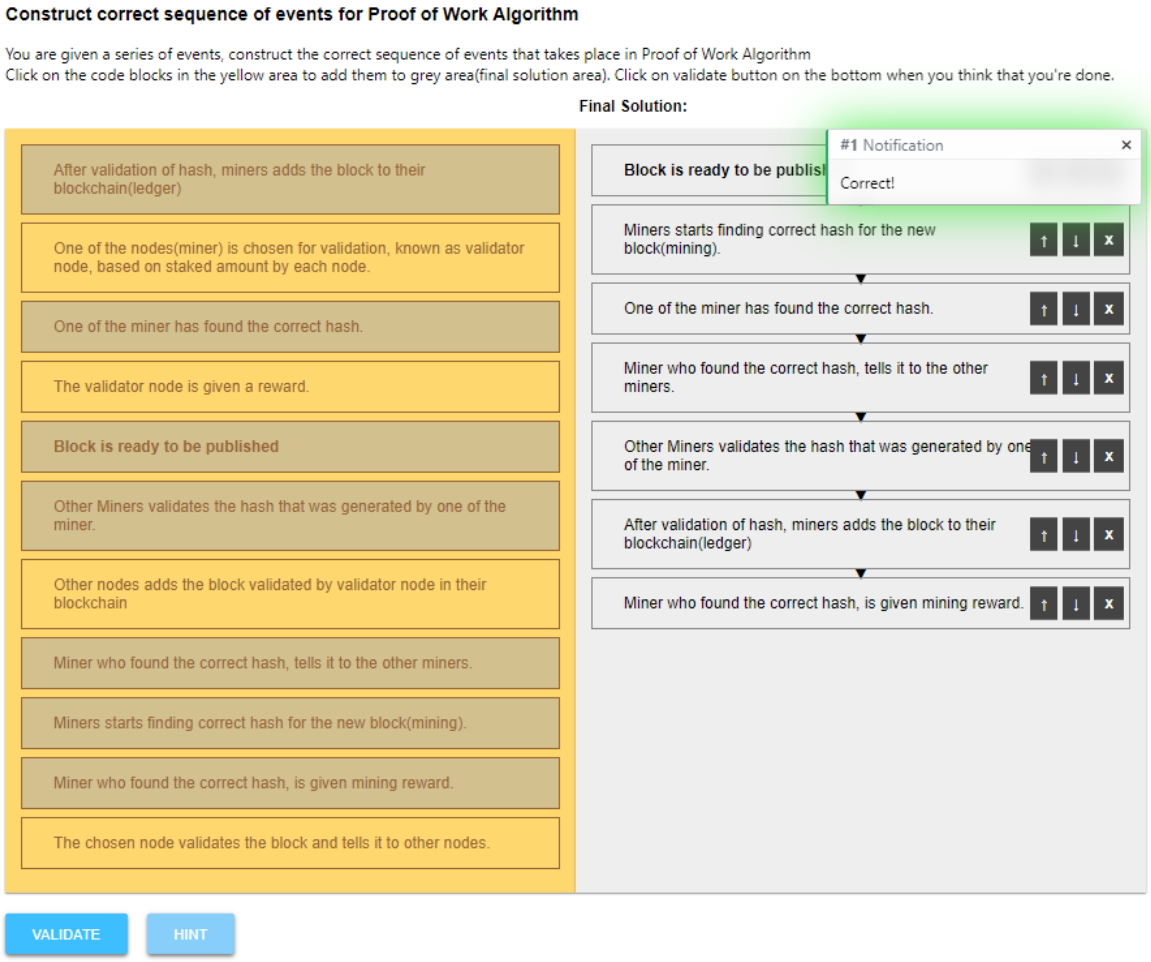
**What is the process of creating new bitcoins popularly known as?**

- a : Finding
- b : Panning
- c : Mining
- d : None of the above

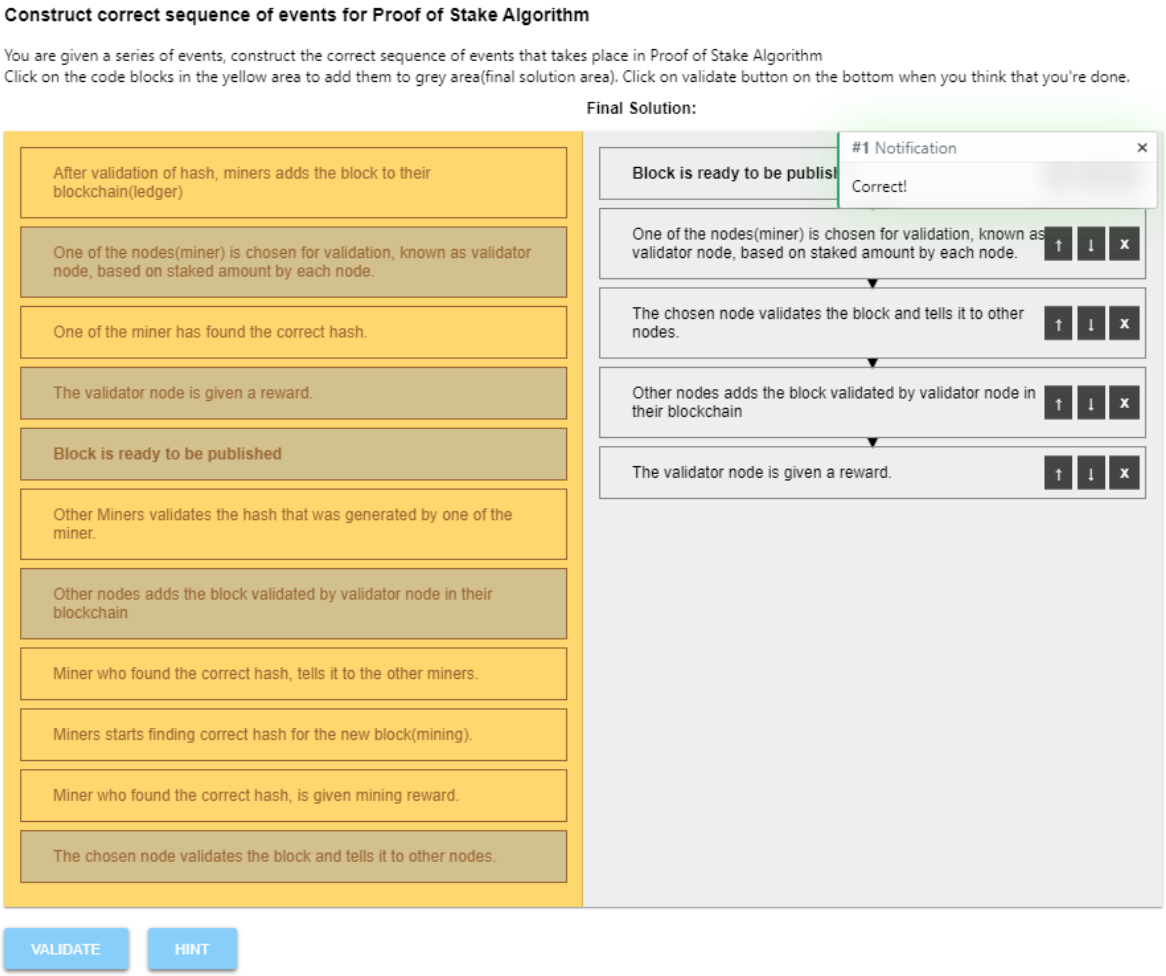
Submit Quiz

7 out of 7

# Proof of work puzzle



# Proof of stake puzzle




## Proof of work activity:

## 1) Instructions

**Instructions:**

**1. Enter the name of User-A(Sender) and User-B(Reciever) to send transaction.**

**2. Now click on the button "ADD TO BLOCK".**

**3. The details you entered will appear on the block.**

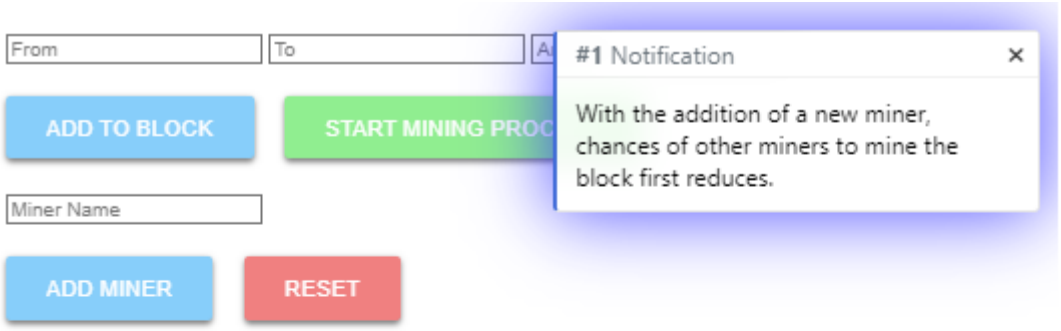
**4. Now click on the button "START MINING PROCESS".**

**5.Mining process will start. Miner A,Miner B and Miner C will start calculating the proper Hash .**

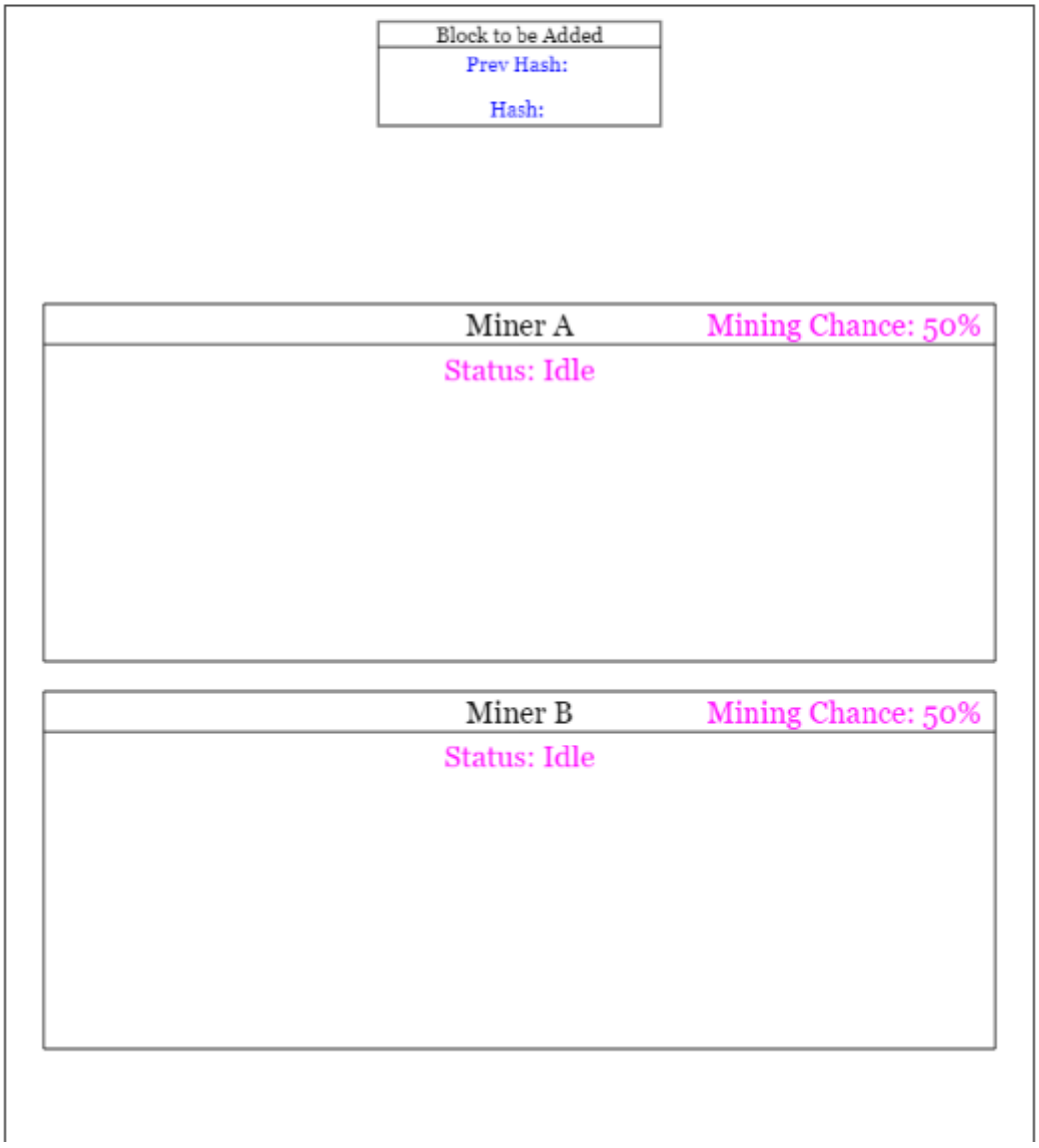
**6.One of the miner completes the mining process**
**and other miners confirm the hash calculated.**

**7. Click on "RESET" button to do the experiment again.**

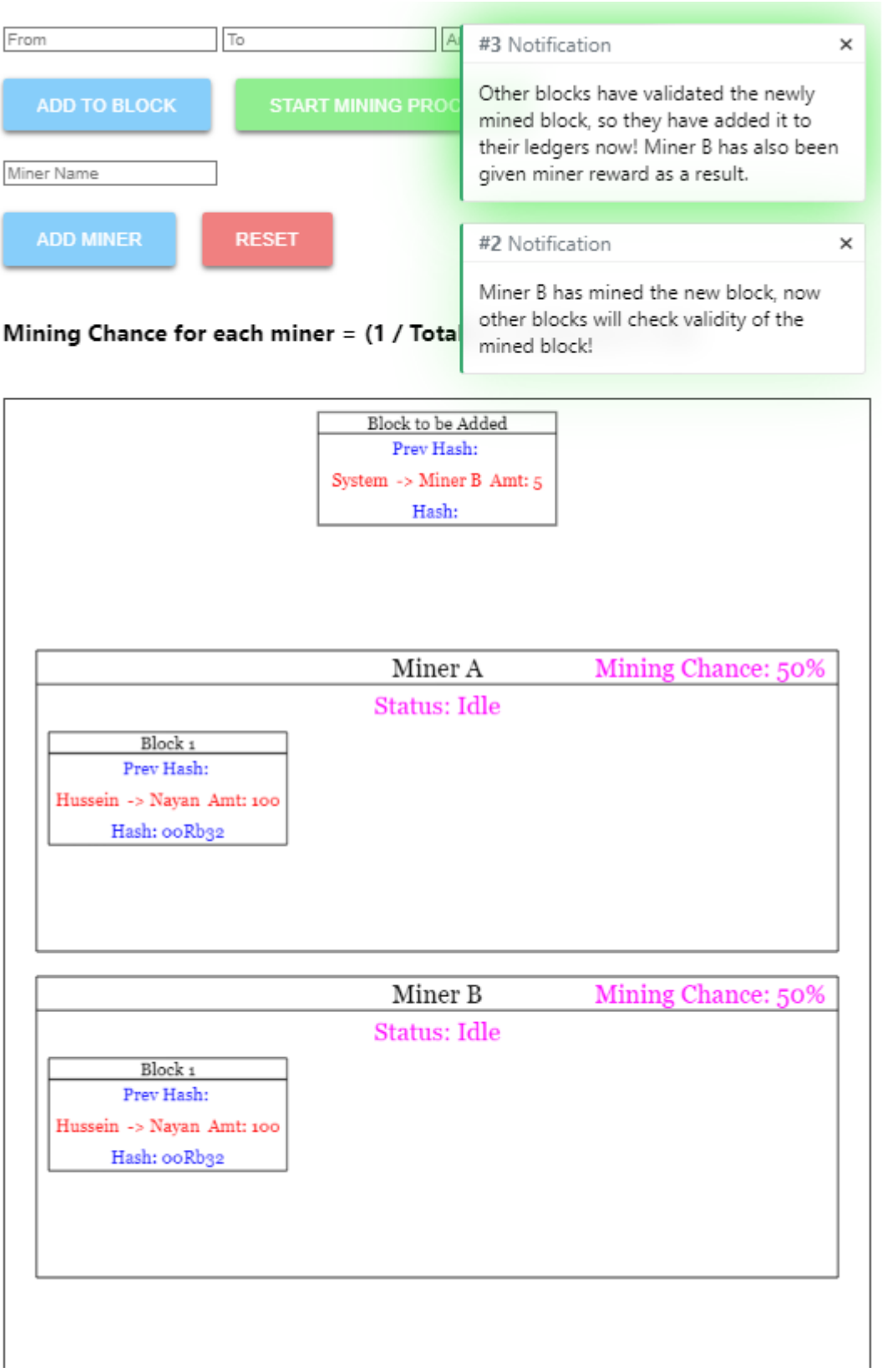
**2) Miner B added**



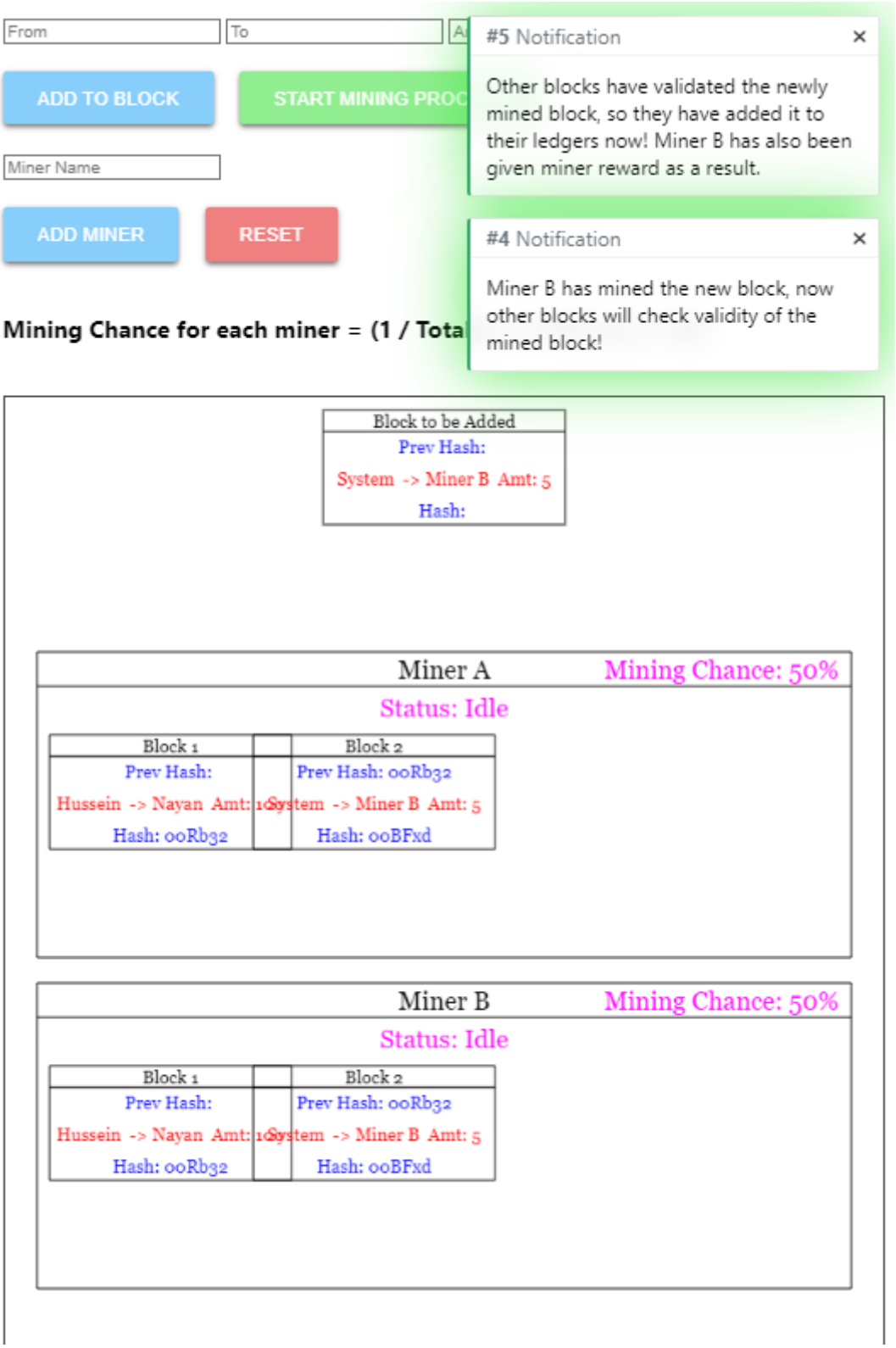

**Mining Chance for each miner = (1 / Total no. of Miners) X 100**



**3) New block added that will be mined by one of the miners**

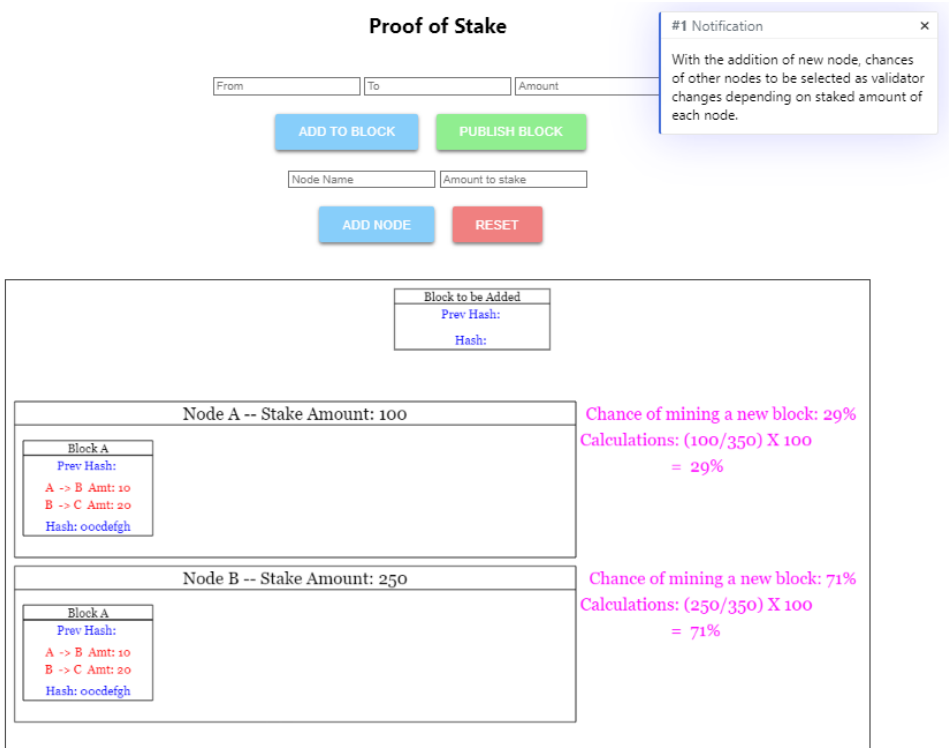


**4) Second block added**

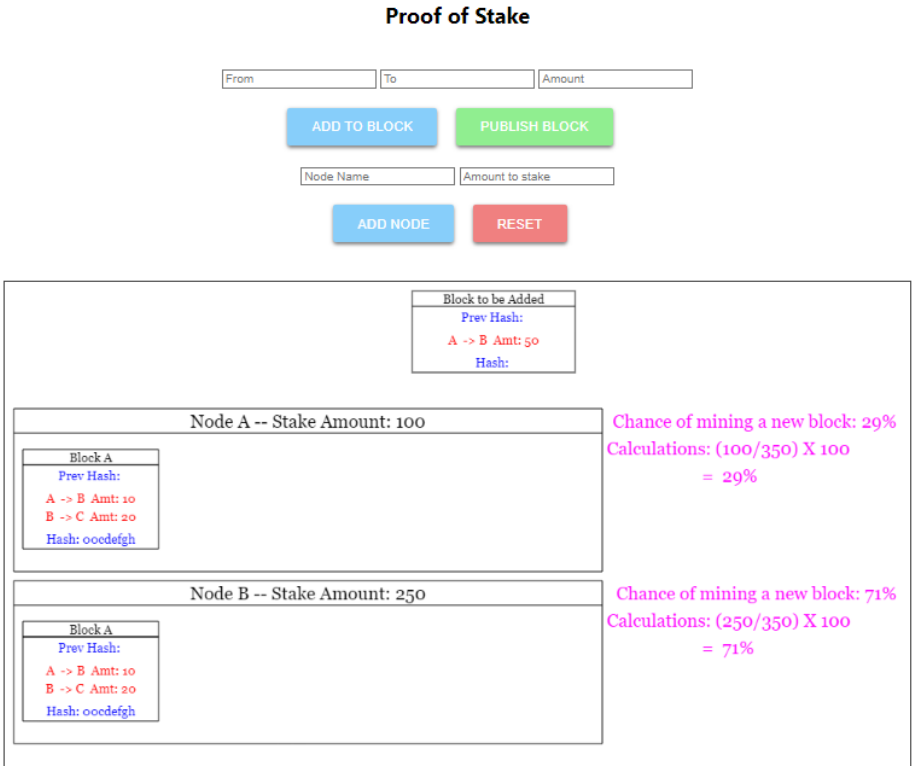


## Proof of stake activity

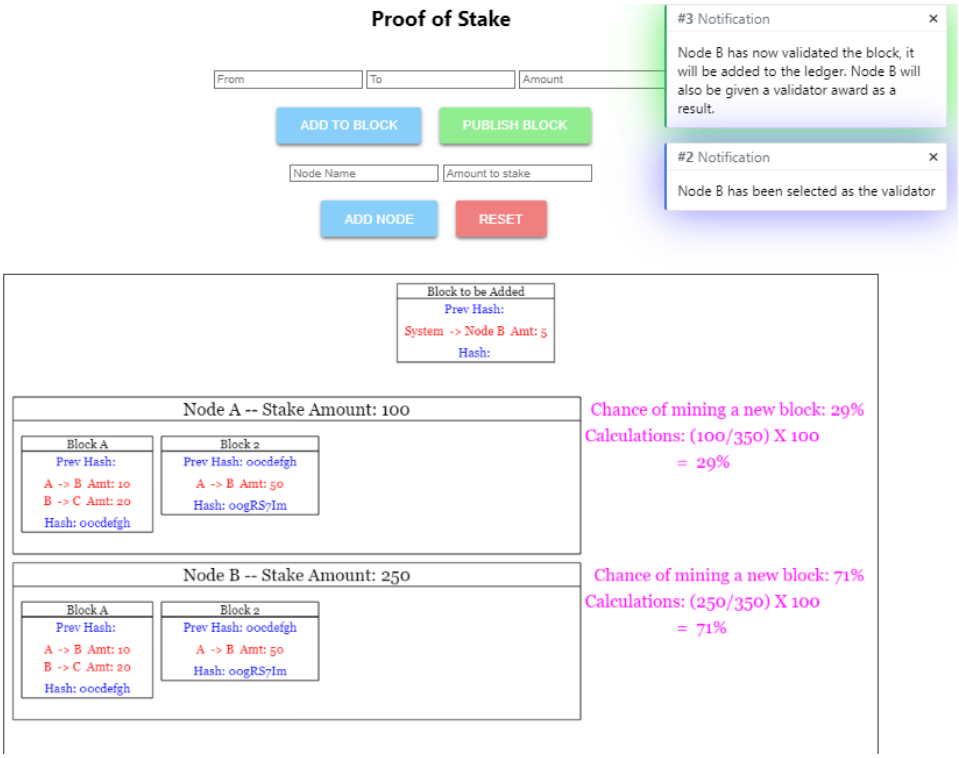
### 1) Node B added to the chain



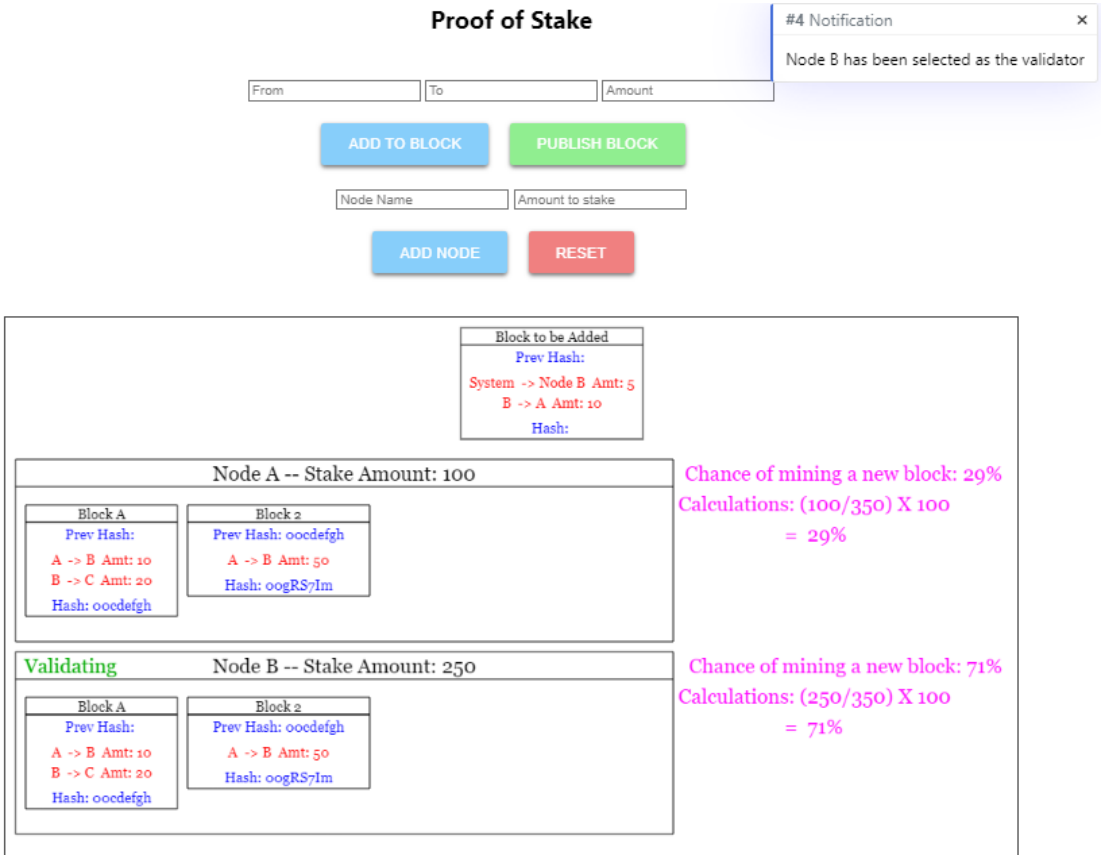

### 2) New block added to the blockchain (A → B = amount (50))



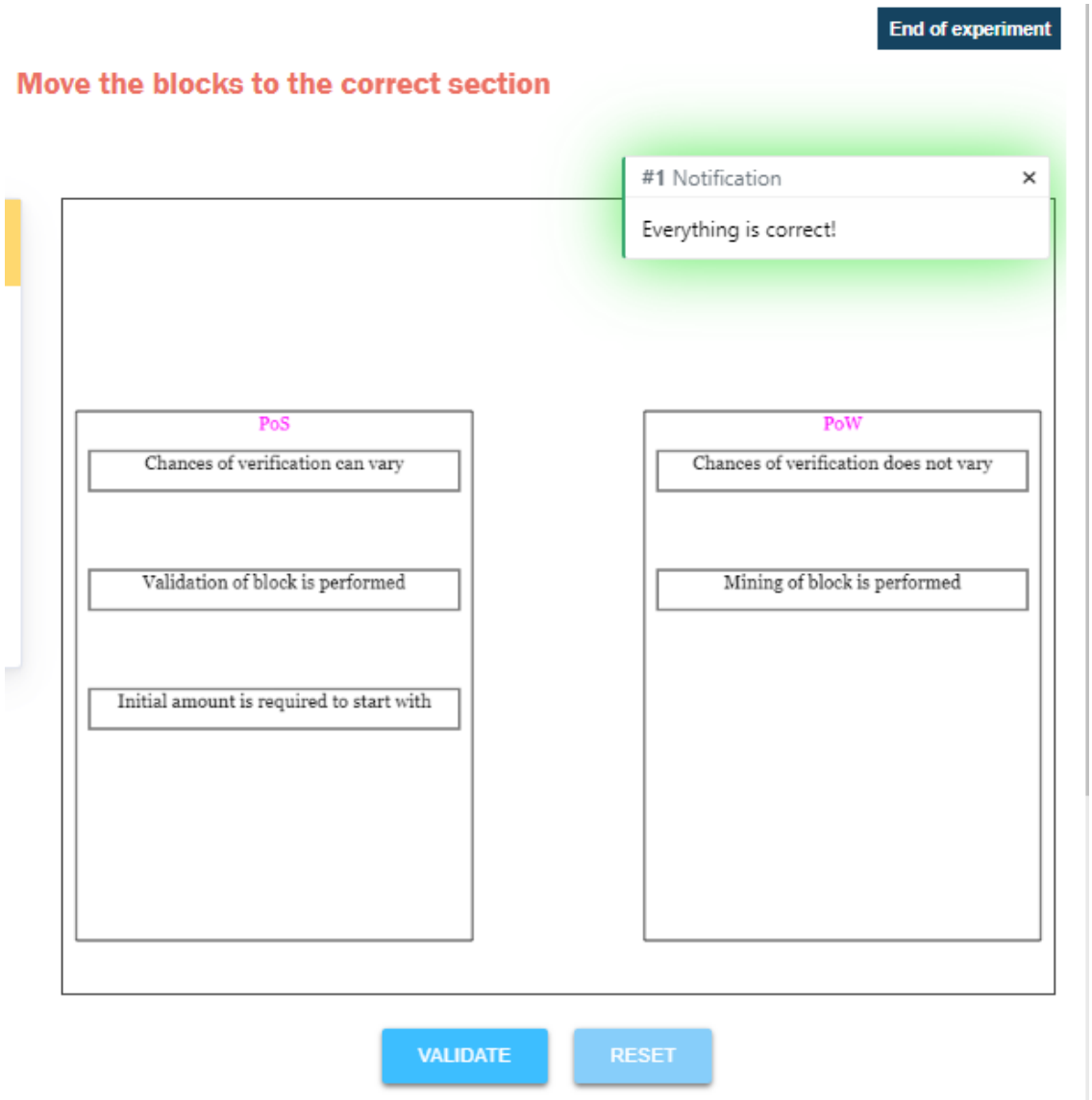
### 3) The added block is mined by one of the miners in the blockchain




### 4) Another block added



**5) Difference**



## Post Test

**What is Proof of Stake?**

- ○ a : A timestamp
- ◉ b : A Consensus protocol
- ○ c : A Cryptographic dimension
- ○ d : None Of the above

**What is Proof Of work?**

- ○ a : A timestamp
- ◉ b : A Consensus protocol
- ○ c : A Cryptographic dimension
- ○ d : None of these

**What role does consensus algorithm play in mining?**

- ○ a : Validation
- ○ b : Adding of blocks
- ◉ c : Both a and b
- ○ d : None of the above

**Is there, a better algorithm for PoW than SHA-256?**

- ◉ a : Yes
- ○ b : No
- ○ c : Can't say

**Pos is an alternative measure of?**

- ◉ a : PoW
- ○ b : PoA
- ○ c : PoB
- ○ d : PoC

**Which statement is correct?**

- ○ a : Mining is a mutable option in blockchain
- ○ b : SHA-256 is the only cryptographic algorithm used in blockchain
- ○ c : Both A and B
- ◉ d : None of the above

**Which is not an advantage of blockchain technology?**

- ◉ a : Anonymity & Privacy
- ○ b : Mutability
- ○ c : Both A and B
- ○ d : None of the above

Submit Quiz

6 out of 7

**Conclusion:- Understood the working and concept of blockchain. Also explored what are the constituents of a block that gets added to a blockchain. Used metamask to get some free testnet ethereum. Also performed some virtual labs to understand the concepts better.**