

Batch: BCT_1 Roll No.: 1911020

Experiment No. 1

Title: Block chain demo and Block explorer – Bitcoin and Ethereum and Test Networks

Objective: To understand the important concepts used in blockchain and explore and analyse blocks, structure and statistics of existing blockchain implementations such as Bitcoin and Ethereum.

Expected Outcome of Experiment:

CO	Outcome
CO1	Build your own Blockchain businesses with acquired knowledge.

Books/ Journals/ Websites referred:

- 1) <https://www.sciencedirect.com/topics/engineering/blockchain>
- 2) <https://www.investopedia.com/terms/b/blockchain.asp>
- 3) <https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain>
- 4) <https://www.geeksforgeeks.org/features-of-blockchain/>
- 5) <https://www.geeksforgeeks.org/advantages-and-disadvantages-of-blockchain/>

Abstract:-

Blockchain is a technology that is developed using a combination of various techniques such as mathematics, algorithms, cryptography, economic models, and so on.

Blockchain is a public ledger of all cryptocurrency transactions that are digitized and decentralized. All the transactions of cryptocurrencies are stored in chronological order to help users in tracking the transactions without maintaining any central record of the transactions. Application prospects of blockchain are promising and have been delivering the result since its inception. Blockchain technology has evolved from initial cryptocurrency to new age smart contracts and has been implemented and applied in many fields. A blockchain consists of growing list of records, called blocks, that are securely linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

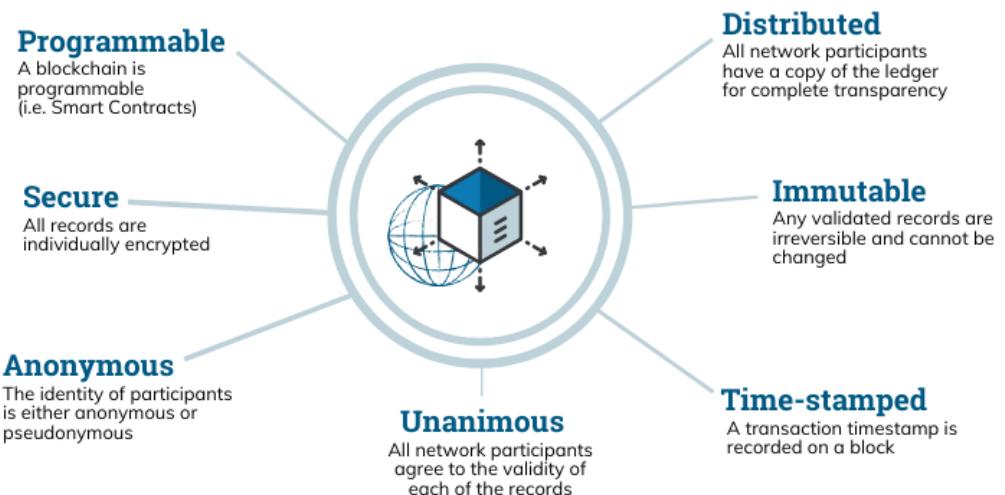
Related Theory: -

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT).

Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash.

The Properties of Distributed Ledger Technology (DLT)



© Euromoney Learning 2020

This means if one block in one chain was changed, it would be immediately apparent it had been tampered with. If hackers wanted to corrupt a blockchain system, they would have to change every block in the chain, across all of the distributed versions of the chain. Blockchains such as Bitcoin and Ethereum are constantly and continually growing as blocks are being added to the chain, which significantly adds to the security of the ledger.

There have been many attempts to create digital money in the past, but they have always failed. The prevailing issue is trust. If someone creates a new currency called the X dollar, how can we trust that they won't give themselves a million X dollars, or

Department of Computer Engineering

steal your X dollars for themselves? Bitcoin was designed to solve this problem by using a specific type of database called a blockchain. Most normal databases, such as an SQL database, have someone in charge who can change the entries (e.g. giving themselves a million X dollars). Blockchain is different because nobody is in charge; it's run by the people who use it. What's more, bitcoins can't be faked, hacked or double spent – so people that own this money can trust that it has some value.

Features of Blockchain:

1. Immutable

Immutability means that the blockchain is a permanent and unalterable network. Blockchain technology functions through a collection of nodes.

- Every node in the network has a copy of the digital ledger. To add a transaction every node checks the validity of the transaction and if the majority of the nodes think that it is a valid transaction then it is added to the network. This means that without the approval of a majority of nodes no one can add any transaction blocks to the ledger.
- Any validated records are irreversible and cannot be changed. This means that any user on the network won't be able to edit, change or delete it.

2. Distributed

All network participants have a copy of the ledger for complete transparency. A public ledger will provide complete information about all the participants on the network and transactions. The distributed computational power across the computers ensures a better outcome. Distributed ledger is one of the important features of blockchains due to many reasons like:

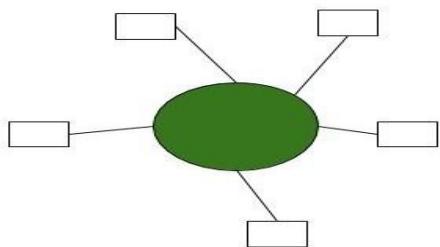
- In distributed ledger tracking what's happening in the ledger is easy as changes propagate really fast in a distributed ledger.
- Every node on the blockchain network must maintain the ledger and participate in the validation.
- Any change in the ledger will be updated in seconds or minutes and due to no involvement of intermediaries in the blockchain, the validation for the change will be done quickly.
- If a user wants to add a new block then other participating nodes have to verify the transaction. For a new block to be added to the blockchain network it must be approved by a majority of the nodes on the network.

- In a blockchain network, no node will get any sort of special treatment or favors from the network. Everyone will have to follow the standard procedure to add a new block to the network.

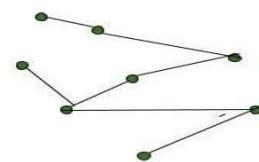
3. Decentralized

The blockchain network is decentralized which means that there is no central governing authority that will be responsible for all the decisions. Rather a group of nodes makes and maintains the network. Each and every node in the blockchain network has the same copy of the ledger. Decentralization property offers many advantages in the blockchain network:

- As a blockchain network does not depend on human calculations it is fully organized and fault-tolerant.
- The blockchain network is less prone to failure due to the decentralized nature of the network. Attacking the system is more expensive for the hackers hence it is less likely to fail.
- There is no third-party involved hence no added risk in the system.
- The decentralized nature of blockchain facilitates creating a transparent profile for every participant on the network. Thus, every change is traceable, and more concrete.
- Users now have control over their properties and they don't have to rely on third-party to maintain and manage their assets.



Centralised Network



Decentralised network

4. Secure

All the records in the blockchain are individually encrypted. Using encryption adds another layer of security to the entire process on the blockchain network. Since there is no central authority, it does not mean that one can simply add, update or delete data on the network.

Every information on the blockchain is hashed cryptographically which means that every piece of data has a unique identity on the network. All the blocks contain a unique hash of their own and the hash of the previous block. Due to this property, the

blocks are cryptographically linked with each other. Any attempt to modify the data means to change all the hash IDs which is quite impossible.

5. Consensus

Every blockchain has a consensus to help the network to make quick and unbiased decisions. Consensus is a decision-making algorithm for the group of nodes active on the network to reach an agreement quickly and faster and for the smooth functioning of the system. Nodes might not trust each other but they can trust the algorithm that runs at the core of the network to make decisions. There are many consensus algorithms available each with its pros and cons. Every blockchain must have a consensus algorithm otherwise it will lose its value.

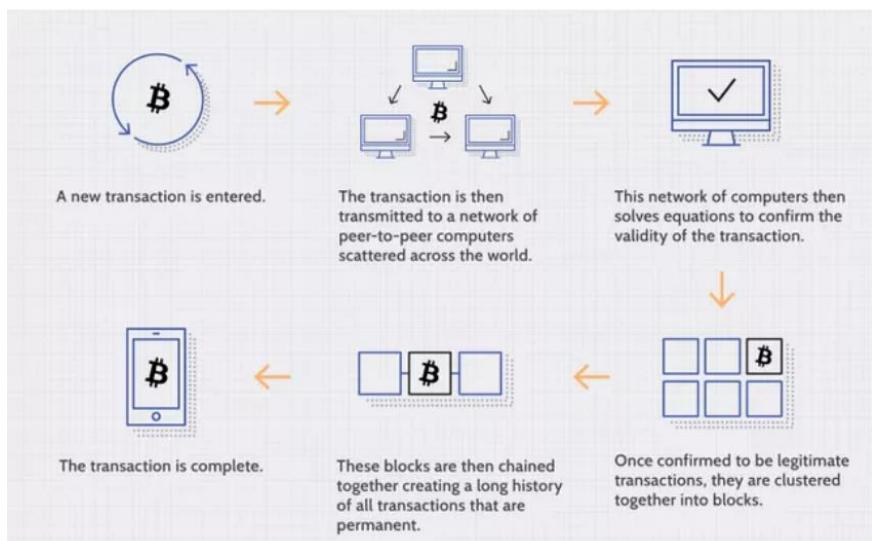
6. Unanimous

All the network participants agree to the validity of the records before they can be added to the network. When a node wants to add a block to the network then it must get majority voting otherwise the block cannot be added to the network. A node cannot simply add, update, or delete information from the network. Every record is updated simultaneously and the updates propagate quickly in the network. Thus it is not possible to make any change without consent from the majority of nodes in the network.

7. Faster Settlement

Traditional banking systems are prone to many reasons for fallout like taking days to process a transaction after finalizing all settlements, which can be corrupted easily. On the other hand, blockchain offers a faster settlement compared to traditional banking systems. This blockchain feature helps make life easier.

How Does Blockchain Technology Work?



Department of Computer Engineering

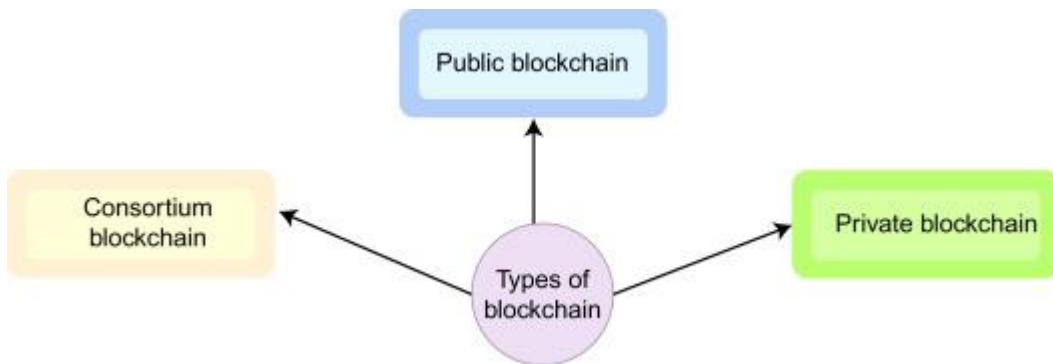
One of Blockchain technology's cardinal features is the way it confirms and authorizes transactions. For example, if two individuals wish to perform a transaction with a private and public key, respectively, the first person party would attach the transaction information to the public key of the second party. This total information is gathered together into a block.

The block contains a digital signature, a timestamp, and other important, relevant information. It should be noted that the block doesn't include the identities of the individuals involved in the transaction. This block is then transmitted across all of the network's nodes, and when the right individual uses his private key and matches it with the block, the transaction gets completed successfully.

The digital signature is merged with the peer-to-peer network; a large number of individuals who act as authorities use the digital signature in order to reach a consensus on transactions, among other issues. When they authorize a deal, it is certified by a mathematical verification, which results in a successful secured transaction between the two network-connected parties. So, to sum it up, Blockchain users employ cryptography keys to perform different types of digital interactions over the peer-to-peer network.

Types of Blockchain:

Blockchain is classified into three major categories :



- I. **Public blockchain:** All records in this blockchain system are broadcasted and all the members and everyone is involved in the process of confirming and validating the transactions.
- II. **Private blockchain:** This is also referred to as a centralized network, as the complete control is under one organization and only the members of the organization are involved in the process of concluding to consensus

Department of Computer Engineering

III. Consortium blockchain: This blockchain system is monitored and regulated by several bodies and is moderately decentralized as few pre-selected group of nodes would be selected to contribute to the decision-making process.

The comparison among different blockchain system:

- **Consensus determination:** Each node in public blockchain participates in the agreement process. Whereas, for validation of the block in consortium blockchain, only a few nodes are involved. Private blockchain system is under control by a single organization which also responsible for the validation.
- **Visibility:** In a public blockchain, transactions are transparent and available to the nodes, whereas the control is under one organization in the case of a private blockchain or a consortium blockchain.
- **Flexibility:** In public blockchains, the transactions are validated and checked by all the nodes in the public and it is not possible to tamper transactions. On the contrary, agreements in private or consortium blockchain can be meddled easily as it involves only a set of people.
- **Efficiency:** With limited number of nodes in consortium and private blockchain, the transactions are efficient as it is not propagated throughout the network. In public chain network, a large amount of time is required to deliver the transactions and blocks among the nodes. This results in limited transaction throughput and high latency.
- **Centralized:** Consortium blockchain involves partial centralization, public blockchain is decentralized, and private blockchain is completely centralized as the control is under a single unit.
- **Consensus Process:** Anyone can actively participate in the consensus process associated with public blockchain. Private and consortium blockchain nodes both being decentralized require permission from the regulatory organization.

Advantages of Blockchain Technology:

1. **Open:** One of the major advantages of blockchain technology is that it is accessible to all means anyone can become a participant in the contribution to blockchain technology, one does not require any permission from anybody to join the distributed network.
2. **Verifiable:** Blockchain technology is used to store information in a decentralized manner so everyone can verify the correctness of the information by using zero-knowledge proof through which one party proves the correctness of data to another party without revealing anything about data.

Department of Computer Engineering

3. Permanent: Records or information which is stored using blockchain technology is permanent means one needs not worry about losing the data because duplicate copies are stored at each local node as it is a decentralized network that has a number of trustworthy nodes.
4. Free from Censorship: Blockchain technology is considered free from censorship as it does not have control of any single party rather it has the concept of trustworthy nodes for validation and consensus protocols that approve transactions by using smart contracts.
5. Tighter Security: Blockchain uses hashing techniques to store each transaction on a block that is connected to each other so it has tighter security. It uses SHA 256 hashing technique for storing transactions.
6. Immutability: Data cannot be tampered with in blockchain technology due to its decentralized structure so any change will be reflected in all the nodes so one cannot do fraud here, hence it can be claimed that transactions are tamper-proof.
7. Transparency: It makes histories of transactions transparent everywhere all the nodes in the network have a copy of the transaction in the network. If any changes occur in the transaction it is visible to the other nodes.
8. Efficiency: Blockchain removes any third-party intervention between transactions and removes the mistake making the system efficient and faster. Settlement is made easier and smooth.
9. Cost Reduction: As blockchain needs no third man it reduces the cost for the businesses and gives trust to the other partner.

Disadvantages of Blockchain Technology:

1. Scalability: It is one of the biggest drawbacks of blockchain technology as it cannot be scaled due to the fixed size of the block for storing information. The block size is 1 MB due to which it can hold only a couple of transactions on a single block.
2. Immaturity: Blockchain is only a couple-year-old technology so people do not have much confidence in it, they are not ready to invest in it yet several applications of blockchain are doing great in different industries but still it needs to win the confidence of even more people to be recognized for its complete utilization.
3. Energy Consuming: For verifying any transaction a lot of energy is used so it becomes a problem according to the survey it is considered that 0.3 percent of the world's electricity had been used by 2018 in the verification of transactions done using blockchain technology.

Department of Computer Engineering

4. Time-Consuming: To add the next block in the chain miners need to compute nonce values many times so this is a time-consuming process and needs to be speed up to be used for industrial purposes.
5. Legal Formalities: In some countries, the use of blockchain technology applications is banned like cryptocurrency due to some environmental issues they are not promoting to use blockchain technology in the commercial sector.
6. Storage: Blockchain databases are stored on all the nodes of the network creates an issue with the storage, increasing number of transactions will require more storage.
7. Regulations: Blockchain faces challenges with some financial institution. Other aspects of technology will be required in order to adopt blockchain in wider aspect.

Applications:

- **Financial Services:** Bitcoin is the first and most prominent application of block chain technology as an e-payment system. Bitcoin was created in January 2009 by Satoshi Nakamoto as a digital currency independent of any central authority, transferable electronically, and with very low transaction costs. A stable and widely accepted crypto currency stands to revolutionize e-commerce, money transfers, and even letters of credit. Cryptocurrency poses a challenge to traditional banking.
- **Retail and Services:** It can be used in retail and services. Any merchant who accepts digital money as payment can exchange their goods and services. Persons and companies involved in a supply value chain can use private block chains to reduce transaction costs in their business relationships and make payments and transfers along the chain as well as pass information in a very transparent manner.
- **Digital Identity:** Identity theft is emerging as a bane of the digital age. Currently taking precautions against identify theft and attempting to restore identity after it has been compromised is an \$18.5 billion annual business and growing yearly according to Distil Networks. Using blockchain technologies would make the tracking and managing of digital identities both secure, efficient and low-cost.
- **Digital Voting:** Two of the biggest hurdles to electronic poll place machines and online voting is the fear that security can be breached and that votes can be manipulated. Using blockchain, a voter could verify if his or her vote was successfully transited and remain anonymous and because of the distributed ledger technology it would not be possible to alter a vote once casted.

Implementation Details:

1. Enlist all the Steps followed and various options explored

Blockchain demo 1 : <https://andersbrownworth.com/blockchain>

- Hashing is a fundamental concept used to build blockchains to provide immutability and integrity of blocks and the transactions they hold. A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length. Values returned by a hash function are called message digest or simply hash values. Common hash functions include SHA-256, SHA-512, SHA-1etc.

SHA256 Hash

Data:	1911020 Kritarth Jain BCT exp1
Hash:	bee178cda85a22bda5deae05c5dbedd70ef39d3ae7dfb134cf6b2128e00b39e2

- Hash of two strings is different and the length of input string may be arbitrary.
As we can see by comparing the two images.

SHA256 Hash

Data:	Example text1
Hash:	96381f47203ead02dd11162bf74b09f5d44b9136149d42001e6475757e9cbe64

SHA256 Hash

Data:	Example texts1
Hash:	e8c8bc18d33883e07370508a80da95168bacb37ad1ebaef188f79e9377130f49

Department of Computer Engineering

- Blocks must be mined before they are added to the blockchain. For this a complex mathematical puzzle is required to be solved. The puzzle in the demo is to find 4 leading zeros in the hash of the data and nonce by adjusting the nonce.

Block

Block:	#	1
Nonce:	72608	
Data:		
Hash:	0000f727854b50bb95c054b39c1fe5c92e5ebcf4bcb5dc279f56aa96a365e5a	
<input type="button" value="Mine"/>		

- If any fields are changed the hash changes which does not satisfy the proof of work puzzle.

Block

Block:	#	1
Nonce:	72608	
Data:	New data added but the block must be mined to get hash with 4 leading zeros	
Hash:	c5fd16499bbe39ae4d18d6eaa3b42602931c3406c73edeb8992455ae864e573e	
<input type="button" value="Mine"/>		

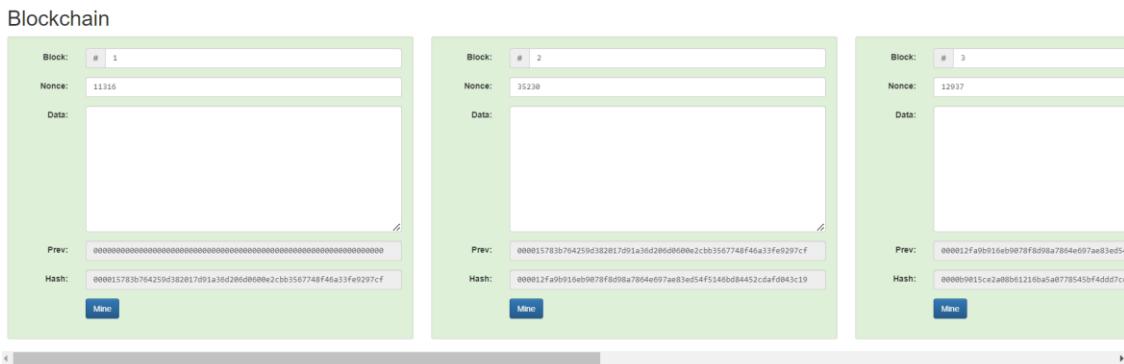
- The block needs to be mined to get corresponding nonce that solves the pow puzzle.

Department of Computer Engineering

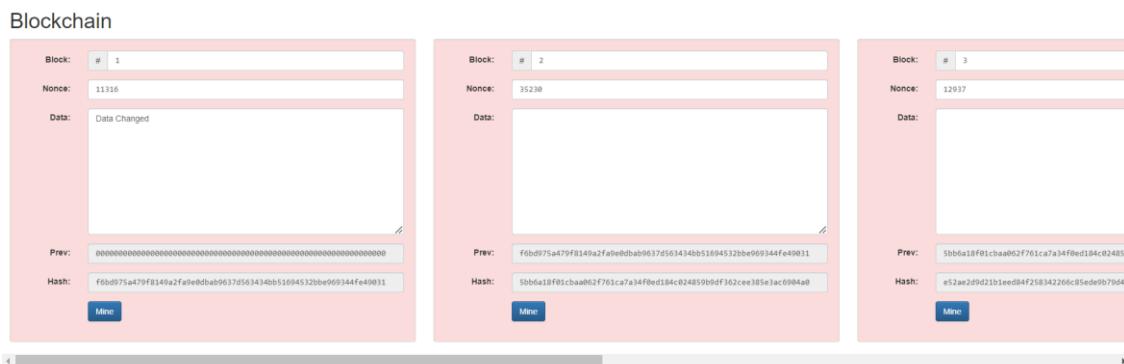
Block

Block:	# 1
Nonce:	82277
Data:	New data added but the block must be mined to get hash with 4 leading zeros
Hash:	00007cbe6c726312a3121b36f23869ff389c916f61ebe9574a66caaba39934fa
<input type="button" value="Mine"/>	

- Blockchain is the collection of blocks which are linked together like a linked list with the next block having the hash of the previous block thereby forming a chain.

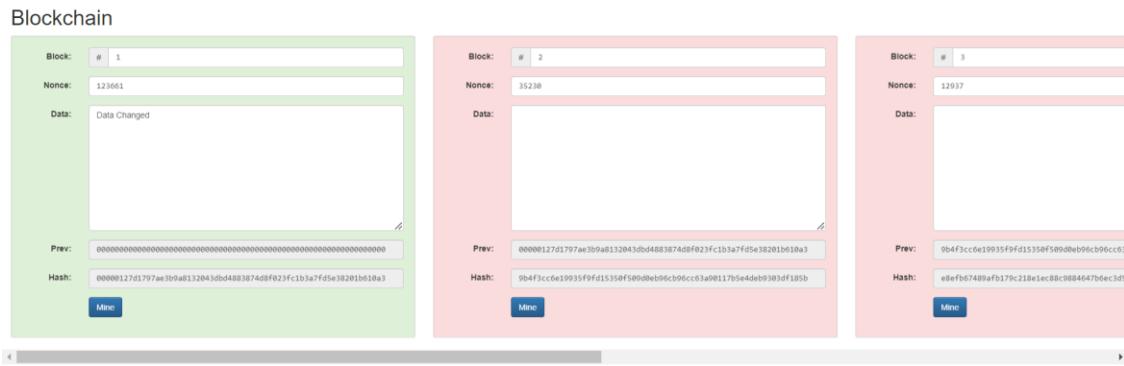


- If data is changed in any block then all blocks following it would be incorrect including itself and they would need to be mined to achieve correctness.

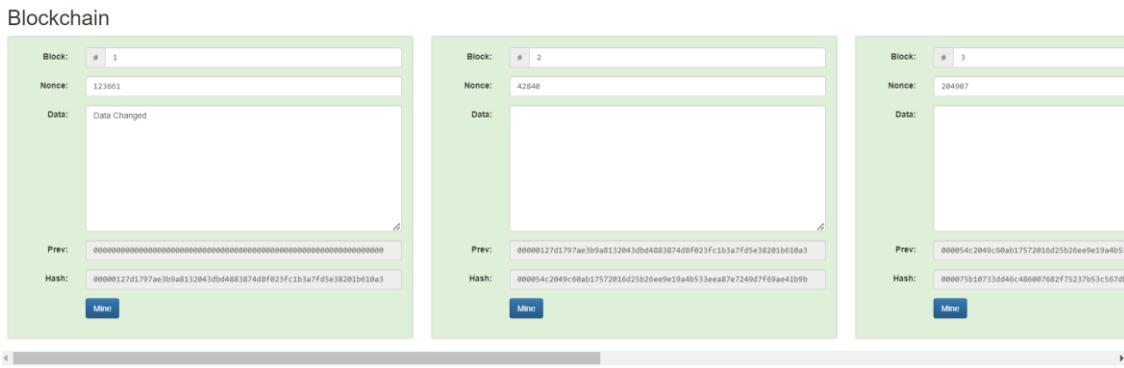


- After mining block 1:

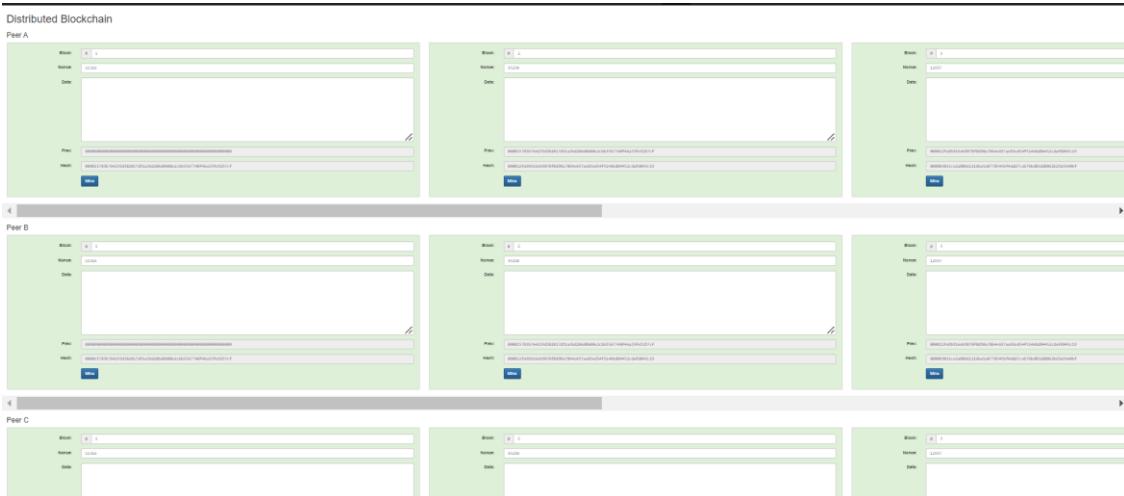
Department of Computer Engineering



- After mining all blocks following block 1



- Blockchain is a distributed ledger which means it is decentralized and distributed.



- All peers have the complete blockchain on their systems and the validity of their blockchain is made by consensus of more than 51% of the nodes present in the network. Changes in one peer don't affect the others.

Department of Computer Engineering

Peer A

Block:	#	1
Nonce:	11316	
Data:		
Prev:	00	
Hash:	000015783b764259d382017d91a36d206d0600e2ccb3567748	

Mine

Block: # 2

Nonce: 35230

Data: Block changed in peer 1

Prev: 000015783b764259d382017d91a36d206d0600e2ccb3567748

Hash: c6adc8151b2475b0848d8df018b4afdeedff38f8720a87870c

Mine

Block: # 3

Nonce: 12937

Data:

Prev: c6adc8151b2475b0848d8df018b4afdeedff38f8720a87870c

Hash: cb24f4ea0e2ca2befdd83bc2504d

Mine

Peer B

Block:	#	1
Nonce:	11316	
Data:		
Prev:	00	
Hash:	000015783b764259d382017d91a36d206d0600e2ccb3567748	

Mine

Block: # 2

Nonce: 35230

Data:

Prev: 000015783b764259d382017d91a36d206d0600e2ccb3567748

Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84

Mine

Block: # 3

Nonce: 12937

Data:

Prev: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84

Hash: 0000b9015ce2a08b61216ba5a077854

Mine

Peer C

Block:	#	1
Nonce:	11316	
Data:		
Prev:	00	
Hash:	000015783b764259d382017d91a36d206d0600e2ccb3567748	

Mine

Block: # 2

Nonce: 35230

Data:

Prev: 000015783b764259d382017d91a36d206d0600e2ccb3567748

Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84

Mine

Block: # 3

Nonce: 12937

Data:

Prev: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84

Hash: 0000b9015ce2a08b61216ba5a077854

Mine

- We make Peer A valid again by mining blocks in it.

Peer A	
Block:	# 1
Nonce:	11316
Data:	
Prev:	00
Hash:	000015783b764259d382017d91a36d206d0600e2ccb3567748
Mine	

Peer B	
Block:	# 2
Nonce:	30091
Data:	Block changed in peer1
Prev:	000015783b764259d382017d91a36d206d0600e2ccb3567748
Hash:	0000bef93eb90ddfe5a72348754dc46be268db49d9308f68ee
Mine	

Peer C	
Block:	# 3
Nonce:	58677
Data:	
Prev:	0000bef93eb90ddfe5a72348754dc46be268db49d9308f68ee
Hash:	00005bd7e0c79ce4fdcc0ccfd89ef
Mine	

Department of Computer Engineering

- Major application of blockchain is in cryptocurrencies for which transactions need to be stored on the chain.

Peer A

Block:	#	2
Nonce:		
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:	0000c52990e86de55ec4b9b32beef7d745d7167dc0eedfbc	
Hash:	00078be183417844c14a9251ca246fb15df1074019873f5d8	
Mine		

Block:	#	3
Nonce: 13804		
Tx:	\$ 10.00	From: Emily
	\$ 5.00	From: Madison
	\$ 20.00	From: Lucas
Prev:	00007@be183417844c14a9251ca246f	
Hash:	00002c95f54a49b4f2bee7056a7dc	
Mine		

Peer B

Block:	#	2
Nonce: 392807		
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:	00000c52990e86de55ec4b9b32beefd745d71675dc0eddfbc	
Hash:	00078be183417844c14a9251ca246fb15df1074019873f5d8	
Mine		

Block:	#	3
Nonce:	13804	
Tx:	\$ 10.00	From: Emily
	\$ 5.00	From: Madison
	\$ 20.00	From: Lucas
Prev:	00007bbe183417844c14a9251ca246f	
Hash:	0000c2c95f54a49bf2bee7056a7dc	
	Mine	

Peer C

Block:	#	2
Nonce:	39287	
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:	00000c52990ee86de55ec4b9b32beef7d745d71675dc0edd9fc	
Hash:	000078be183417844c14a9251ca246fb15df1074019873f5d8	
Mine		

Block:	#	3
Nonce:	13804	
Tx:	\$ 10.00	From: Emily
	\$ 5.00	From: Madison
	\$ 20.00	From: Lucas
Prev:	000078be183417844c14a9251ca246ft	
Hash:	0000c2c95f54a49b4f2be7056a7dc3t	
Mine		

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

Department of Computer Engineering

Peer A

Block:	#	2
Nonce:	39287	
Tx:		
	\$ 97.67	From: Ripley -> Lambert
	\$ 48.61	From: Kane -> Ash
	\$ 6.15	From: Parker -> Dallas
	\$ 10.445	From: Hicks -> Newt
	\$ 88.32	From: Bishop -> Burke
	\$ 45.00	From: Hudson -> Gorman
	\$ 92.00	From: Vasquez -> Apone
Prev:	0000c52990ee86de55ec4b9b32beefdf745d71675dc@eddfbe	
Hash:	0f3c237b7de92ee7344fd1d2acaze0ae1e557c73d3ffbd0	
	Mine	

Block:	#	3
Nonce:	13804	
Tx:	\$ 10.00	From: Emily
	\$ 5.00	From: Madison
	\$ 20.00	From: Lucas
Prev:	0f3c237b7de92ee7344fd1cd2aca2e	
Hash:	e53f7cb5ceefaf6b30295a0ef4a3d4	
	Mine	

Peer B

Block:	#	1
Nonce:	1399358	
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:	000	
Hash:	0000c52990ee86de55ec4b9b32beef745d71675dc0eddfbc	
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

Block:	#	3
Nonce:	13804	
Tx:	\$ 10.00	From: Emily
	\$ 5.00	From: Madison
	\$ 20.00	From: Lucas
Prev:	000078be183417844c14a9251ca240	
Hash:	0000c2c95f54a49b4f2bee7056a7d0	
	Mine	

Peer C

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:	00000c52990eee86de55ec4b0b32beefd745d71675dc0edd fbc	
Hash:	000078be183417844c14a9251ca246fb15df1074019873f5d8	

Block:	#	3
Nonce:	13804	
Tx:	\$ 10.00	From: Emily
	\$ 5.00	From: Madison
	\$ 20.00	From: Lucas
Prev:	000078be183417844c14a9251ca240	
Hash:	0000c2c95f54a49bf2bee7056a7d0	
Mine		

- To make peer A blockchain valid all the invalid blocks has to be mined again.

Peer A

Block:	#	2
Nonce:	66335	
Tx:		
\$ 97.67	From:	Ripley ➔ Lambert
\$ 48.61	From:	Kane ➔ Ash
\$ 6.15	From:	Parker ➔ Dallas
\$ 10.445	From:	Hicks ➔ Newt
\$ 88.32	From:	Bishop ➔ Burke
\$ 45.00	From:	Hudson ➔ Gorman
\$ 92.00	From:	Vasquez ➔ Apone
Prev:	0000c52990ee86de55ec4b9b32beef7d745d71675dc0eddffbc	
Hash:	0000c8ff06e77234d6584e0f5649eb05e5e94717defdc46a	

Block:	#	3
Nonce:	95378	
Tx:	\$ 10.00	From: Emily
	\$ 5.00	From: Madison
	\$ 20.00	From: Lucas
Prev:	000c8ff06e77234460584e0f5649e	
Hash:	0000c0a663989e1ec2e6e0930ac7c3d	

[Mine](#)

Department of Computer Engineering

- A coinbase transaction is the first transaction in a block. It is a unique type of bitcoin transaction that can be created by a miner. The miners use it to collect the block reward for their work and any other transaction fees collected by the miner are also sent in this transaction.

Peer A

Block:	# 1		
Nonce:	166651		
Coinbase:	\$ 100.00	>	Anders
Tx:			
Prev:	000		
Hash:	0000438d7625b86a6f366545b1929975a0d3ff1f8847e56c5		
<input type="button" value="Mine"/>			

Block:	#	2	
Nonce:	215458		
Coinbase:	\$ 100.00	>	Anders
Tx:	\$ 10.00	From:	Anders > Sophia
	\$ 20.00	From:	Anders > Lucas
	\$ 15.00	From:	Anders > Emily
	\$ 15.00	From:	Anders > Madison
Prev:	0000438d7e25b86a6f366545b1929975a0d3ff1f8847e56cc5		
Hash:	0000baeab68c2a609a6fa63553438d97c672a1549a7fce4a617		
	Mine		

Block:	#	3
Nonce: 146		
Coinbase:	\$ 100.00	→
Tx:	\$ 10.00	From: Emily
	\$ 5.00	From: Madison
	\$ 20.00	From: Lucas
Prev:	000baeb682ca60f9a6fa5635543bd:	
Hash:	000fd1d32b734f5a5fc126a0f0e885	
Mine		

Peer B

Block:	#	1
Nonce:	16651	
Coinbase:	\$ 100.00	→ Anders
Tx:		
Prev:	000	
Hash:	0000438d7625b86a6f366545b1929975a0dffff1ff8847e56cc5	
<input type="button" value="Mine"/>		

Block:	#	2
Nonce:	215458	
Coinbase:	\$ 100.00	⇒ Anders
Tx:	\$ 10.00	From: Anders ⇒ Sophia
	\$ 20.00	From: Anders ⇒ Lucas
	\$ 15.00	From: Anders ⇒ Emily
	\$ 15.00	From: Anders ⇒ Madison
Prev:	000043d87625b86a6f366545b1929975a0d3ff1f8847e56cc5	
Hash:	0000baeb68c2a609fa6fa6355438d97c672a15494fccea617	
	Mine	

Block:	#	3
Nonce:	146	
Coinbase:	\$ 100.00	→
Tx:	\$ 10.00	From: Emily
	\$ 5.00	From: Madison
	\$ 20.00	From: Lucas
Prev:	000baeb68c2a60f9a6fa6355438d5	
Hash:	000df1d632b734f5a5fc126a0f8e88f	
Mine		

Peer C

Block:	#	2
Nonce:	215458	
Coinbase:	\$ 100.00	→ Anders
Tx:	\$ 10.00	From: Anders → Sophia
	\$ 20.00	From: Anders → Lucas
	\$ 15.00	From: Anders → Emily
	\$ 15.00	From: Anders → Madison
Prev:	0000438d7e25b86af366545b1929975a0d3ff1f8847e56cc5	
Hash:	0000baebab6c2a60f9af6a5635438d97c672a15494fcea617	
	Mine	

Block:	#	3
Nonce:	146	
Coinbase:	\$ 100.00	→
Tx:	\$ 10.00	From: Emily
	\$ 5.00	From: Madison
	\$ 20.00	From: Lucas
Prev:	0000babeb8c2a60f9a6fa5635543bd	
Hash:	0000df1d632b734f5a5fc126a0f0e88	
	Mine	

Department of Computer Engineering

Peer B

The image shows three blockchain blocks from Peer B. Block 1 has a nonce of 16651 and a coinbase transaction of \$100.00 to Anders. Block 2 has a nonce of 215458 and a coinbase transaction of \$120.00 to Anders. It contains four txs: \$10.00 to Sophia, \$20.00 to Lucas, \$15.00 to Emily, and \$15.00 to Madison. Block 3 has a nonce of 146 and a coinbase transaction of \$100.00. It contains three txs: \$10.00 to Emily, \$5.00 to Madison, and \$20.00 to Lucas. All blocks have a previous hash and a unique hash.

- To make peer B blockchain valid all the invalid blocks has to be mined again

Peer B

The image shows three blockchain blocks from Peer B. Block 1 has a nonce of 16651 and a coinbase transaction of \$100.00 to Anders. Block 2 has a nonce of 97462 and a coinbase transaction of \$120.00 to Anders. It contains four txs: \$10.00 to Sophia, \$20.00 to Lucas, \$15.00 to Emily, and \$15.00 to Madison. Block 3 has a nonce of 54603 and a coinbase transaction of \$100.00. It contains three txs: \$10.00 to Emily, \$5.00 to Madison, and \$20.00 to Lucas. All blocks have a previous hash and a unique hash.

Blockchain demo2: <https://blockchaindemo.io/>

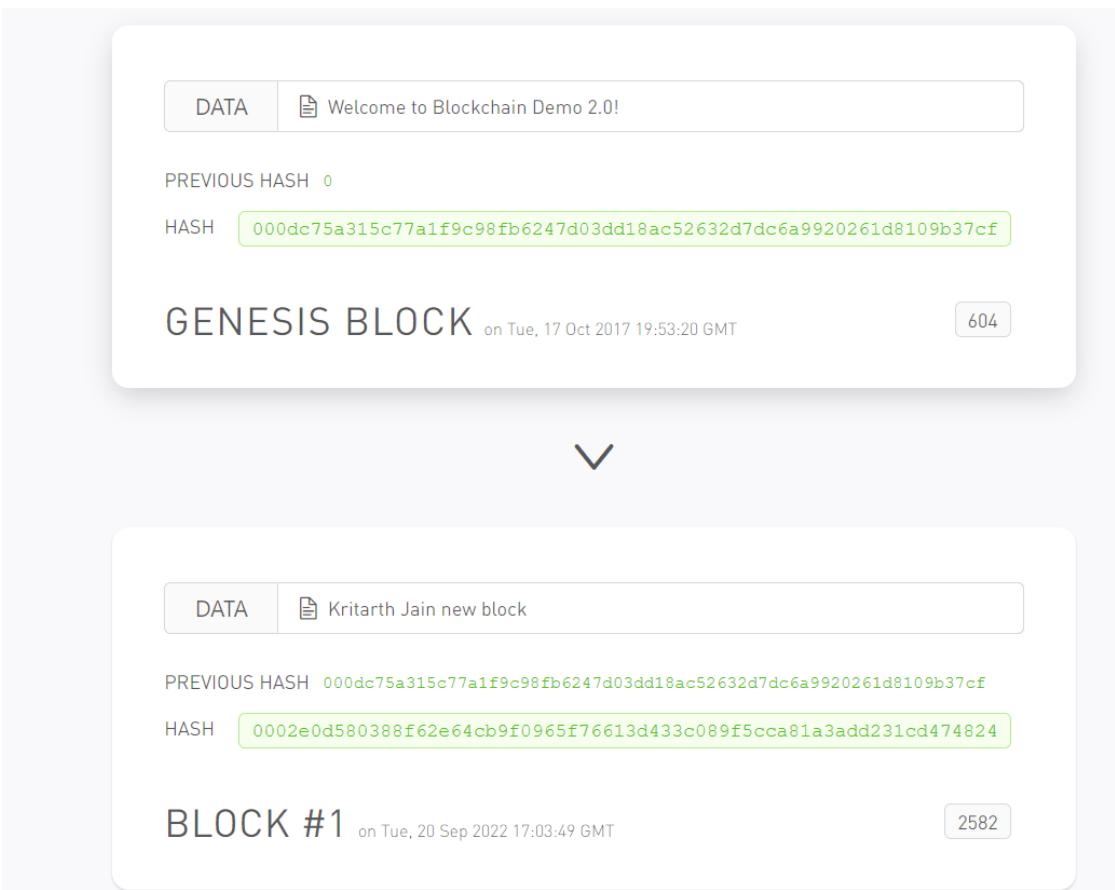
- In the previous demo the peer-to-peer functionality of blockchain was not demonstrated which is an important feature of blockchains. The first block in the blockchain is called the genesis block.

PEERS

The screenshot shows the Blockchain Demo 2.0 interface. At the top, there's a list of peers: Satoshi, with a blue user icon and an 'X' button. Below this is a large title "BLOCKCHAIN". A central box displays the "GENESIS BLOCK" with the timestamp "on Tue, 17 Oct 2017 19:53:20 GMT". Inside the box, there are tabs for "DATA" and "Welcome to Blockchain Demo 2.0!". Below these are fields for "PREVIOUS HASH" (empty) and "HASH" (containing the value "000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf"). A small "604" box is located in the bottom right corner of the central box.

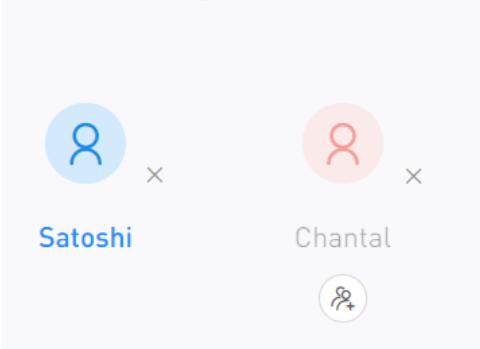
Department of Computer Engineering

- Currently only the genesis block is present with only one peer (Satoshi) . We can add a new block to the blockchain.

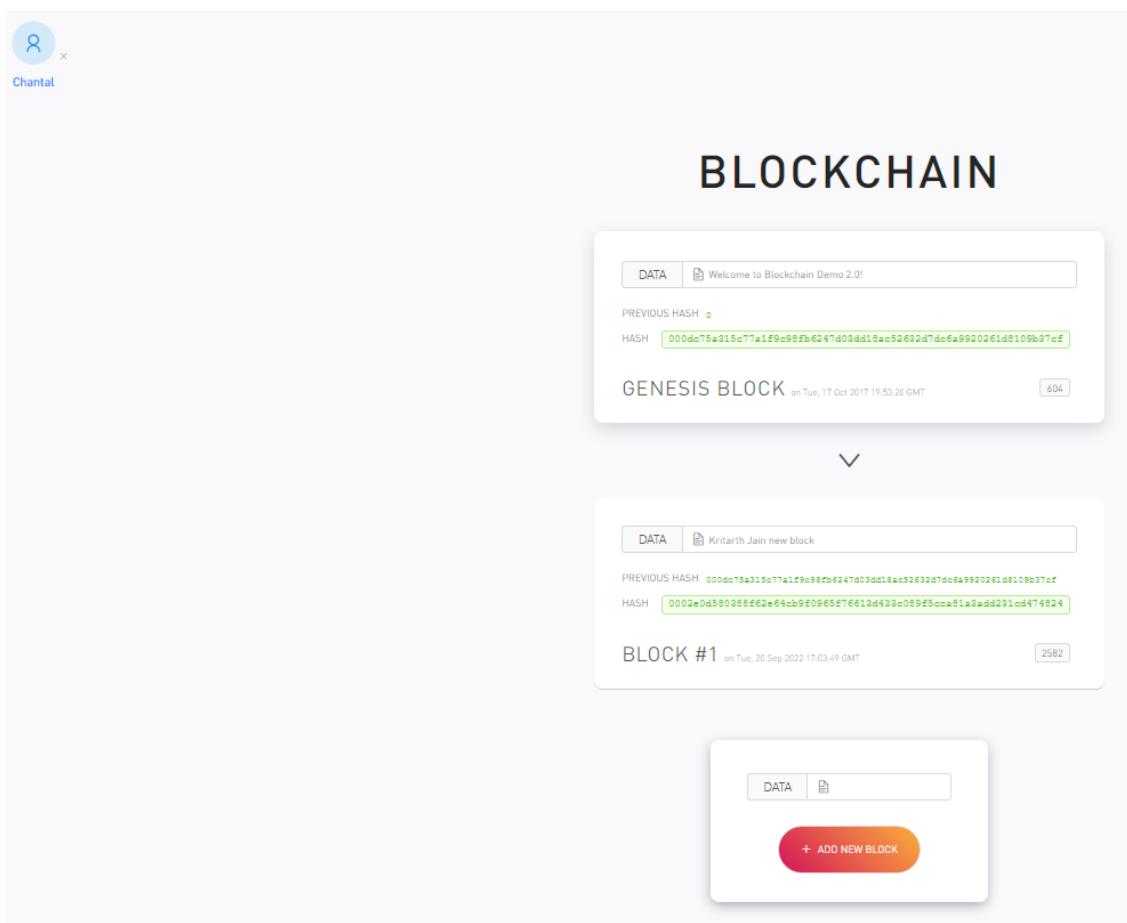


- We can also create another peer for the blockchain and connect it so that it receives the validated and accepted version of the blockchain.

PEERS



Department of Computer Engineering



- If a block is added in peer 2 (chantal) then the change is broadcasted to all peers and satoshi would also have the block added to his chain.

Department of Computer Engineering

PEERS

Satoshi Chantal

BLOCKCHAIN

DATA Welcome to Blockchain Demo 2.0!

PREVIOUS HASH: 000da75a315c77a1f9c98fb6247d03dd15ac52632d7dc6a9920261d8109b37cf

HASH: 0002e0d550388fe62e64cb9f0965f76613d433c08955ccaa81a3add231cd474824

GENESIS BLOCK on Tue, 17 Oct 2017 19:53:20 GMT [604]

▼

DATA Kritarth Jain new block

PREVIOUS HASH: 000da75a315c77a1f9c98fb6247d03dd15ac52632d7dc6a9920261d8109b37cf

HASH: 0002e0d550388fe62e64cb9f0965f76613d433c08955ccaa81a3add231cd474824

BLOCK #1 on Tue, 20 Sep 2022 17:03:49 GMT [2582]

▼

DATA new block

PREVIOUS HASH: 0002e0d550388fe62e64cb9f0965f76613d433c08955ccaa81a3add231cd474824

HASH: 0005e0ec8382608cd7ba7f40ce967e881466ddb9444d284357a11bbec271ae00

BLOCK #2 on Tue, 20 Sep 2022 17:07:32 GMT [689]

BLOCKCHAIN

DATA Welcome to Blockchain Demo 2.0!

PREVIOUS HASH: 000da75a315c77a1f9c98fb6247d03dd15ac52632d7dc6a9920261d8109b37cf

HASH: 0002e0d550388fe62e64cb9f0965f76613d433c08955ccaa81a3add231cd474824

GENESIS BLOCK on Tue, 17 Oct 2017 19:53:20 GMT [604]

▼

DATA Kritarth Jain new block

PREVIOUS HASH: 000da75a315c77a1f9c98fb6247d03dd15ac52632d7dc6a9920261d8109b37cf

HASH: 0002e0d550388fe62e64cb9f0965f76613d433c08955ccaa81a3add231cd474824

BLOCK #1 on Tue, 20 Sep 2022 17:03:49 GMT [2582]

▼

DATA new block

PREVIOUS HASH: 0002e0d550388fe62e64cb9f0965f76613d433c08955ccaa81a3add231cd474824

HASH: 0005e0ec8382608cd7ba7f40ce967e881466ddb9444d284357a11bbec271ae00

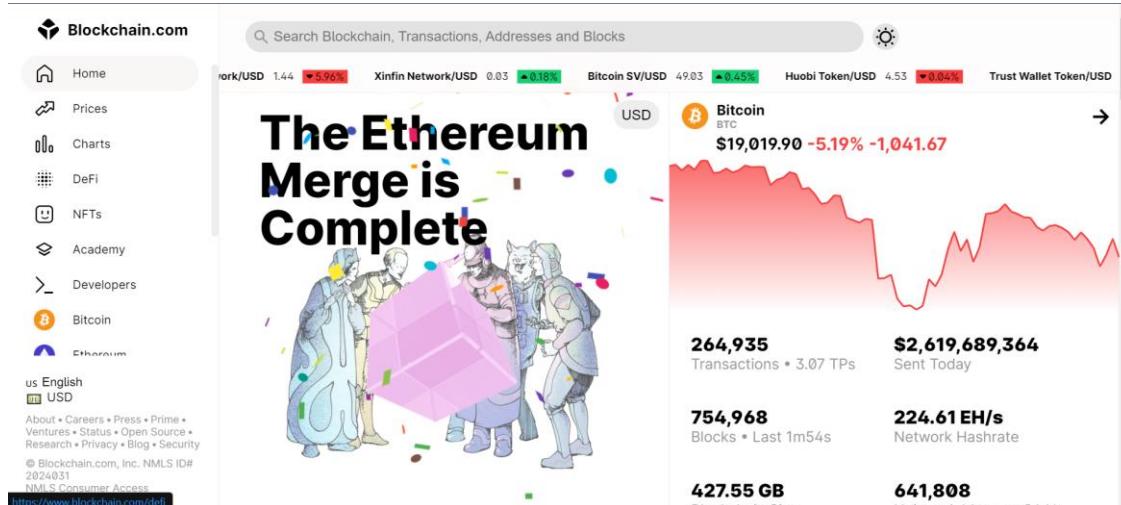
BLOCK #2 on Tue, 20 Sep 2022 17:07:32 GMT [689]

Department of Computer Engineering

Block explorer – Bitcoin: <https://www.blockchain.com/explorer>

Block explorers can be thought of as search engines for the blockchain. They allow users to search information such as balances, contracts, and transactions. More advanced block explorers even offer indexing capabilities, which enable them to provide a complete set of information, such as ERC-20 tokens in the network. They might even offer API services to access it via external services.

- Bitcoin blockchain has several blocks whose data can be easily viewed using the block explorers.



- We can search for blocks using their block numbers. The genesis block of bitcoin :

The block explorer shows the time the block was mined, number blocks ahead of this block in the blockchain. It also shows the reward earned by the miner and the number of transaction with their bitcoin consumptions.

Block 0 ⓘ

USD BTC

This block was mined on January 03, 2009 at 11:45 PM GMT+5:30 by [Unknown](#). It currently has 754,976 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 50.00000000 BTC (\$950,259.00). The reward consisted of a base reward of 50.00000000 BTC (\$950,259.00) with an additional 0.00000000 BTC (\$0.00) reward paid as fees of the 1 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this [address](#).

A total of 0.00000000 BTC (\$0.00) were sent in the block with the average transaction being 0.00000000 BTC (\$0.00).

A table will be displayed at the bottom containing more information related to the block that is searched. Hash shows the hash 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 transactions, nonce used to calculate block hash to satisfy proof of work, block reward, etc.

Department of Computer Engineering

Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f	copy
Confirmations	754,976	
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	
Fee Reward	0.00000000 BTC	

The explorer also shows the different transactions along with bitcoins transferred along with the addresses of the sender and the receivers. The green symbol shows that the amount is unspent and can be used in further transactions.

Block Transactions ⓘ

Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 204 bytes)	50.00000000 BTC
Hash	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b	2009-01-03 23:45

COINBASE (Newly Generated Coins) ➔ 1A1zP1eP5QGefi2DMPTTL5Lmv7DivfNa 50.00000000 BTC ⓘ

We can also click on the addresses to get information about that bitcoin address including the number of transactions involving the address and the balance held by the address.

Address ⓘ

This address has transacted 3,455 times on the Bitcoin blockchain. It has received a total of 68.55444405 BTC (\$1,295,862.03) and has sent a total of 0.00000000 BTC (\$0.00). The current value of this address is 68.55444405 BTC (\$1,295,862.03).

	Address	1A1zP1eP5QGefi2DMPTTL5Lmv7DivfNa	copy
	Format	BASE58 (P2PKH)	
	Transactions	3,455	
	Total Received	68.55444405 BTC	
	Total Sent	0.00000000 BTC	
	Final Balance	68.55444405 BTC	
Transactions ⓘ			
Fee	0.00000780 BTC (9.807 sat/B - 4,160 sat/WU - 590 bytes) (16,626 sat/vByte - 348 virtual bytes)	+0.00123604 BTC	
Hash	1a1zP1eP5QGefi2DMPTTL5Lmv7DivfNa 368e0MB8QJadNZ4S7Tx0DmNxRqfjRQD 394Kac0PiisCz0iAcjPjhpDjRaZw1mW777Q 34drMmHgSpjEUNKox7uvsyNaxX2ykw	2022-09-19 20:13	
		0.00868038 BTC ⚡ 0.00201961 BTC ⚡ 0.00180000 BTC ⚡	0.00123604 BTC ⓘ 0.00100609 BTC ⓘ

All the transactions involving the address can also be seen 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 transaction can also be visible.

Department of Computer Engineering

Transactions ⓘ

Fee	0.0000798 BTC (9.807 sat/B - 4160 sat/WU - 580 bytes) (16.928 sat/vByte - 348 virtual bytes)	+0.00123604 BTC
Hash	bb7620043cc1b054ade8a33bfa09b7b889553931e52fb69eb8785e243d94055	2022-09-19 20:13
	3GRmEBJLxDjN6NaGzG5ToTnQbCmRtRe6t9GD 394Kac-QfphoCzioMCg52hpDRAzWymHW77Q 34dYMrHg6j0pECUWkox7a5ySyNaxD2yhw	0.00688038 BTC ⓘ 0.00261961 BTC ⓘ 0.00180000 BTC ⓘ
Fee	0.00000144 BTC (0.640 sat/B - 0.251 sat/WU - 225 bytes) (1.000 sat/vByte - 144 virtual bytes)	+0.00008500 BTC
Hash	3f1abdc595d411fd17734dee6fd94438d1d05de21831cab2510c9171ed4f09	2022-09-18 19:19
	bc1q8gp6vxfax5e29gytr854ax3a3uw0x7wwxxmdx	0.00399934 BTC ⓘ bc1q8gp6vxfax5e29gytr854ax3a3uw0x7wwxxmdx 1A1zP1eP5QGeif20MPTTLL5Lmv7DlvfNa
Fee	0.00000146 BTC (0.649 sat/B - 0.255 sat/WU - 225 bytes) (1.014 sat/vByte - 144 virtual bytes)	+0.00000558 BTC
Hash	ffd9fb2bd57a3bd2717883c98b05f27bba619fd9c50eba766a75da119e7d0	2022-09-18 18:14
	bc1qex0aqq8mxqfh4cp162eg755836djjx20yzuuu8	0.00051407 BTC ⓘ bc1qex0aqq8mxqfh4cp162eg755836djjx20yzuuu8 1A1zP1eP5QGeif20MPTTLL5Lmv7DlvfNa 0.00000558 BTC ⓘ 0.00050703 BTC ⓘ

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

Details ⓘ

Hash	ffdd6fb2bd57a3bd2717883c98b05f27bba619fd9c50eba766a75da119e7d0
Status	Confirmed
Received Time	2022-09-16 18:14
Size	225 bytes
Weight	573
Included in Block	754352
Confirmations	25
Total Input	0.00051407 BTC
Total Output	0.00051261 BTC
Fees	0.00000146 BTC
Fee per byte	0.649 sat/B
Fee per vbyte	1.014 sat/vByte
Fee per weight unit	0.255 sat/WU
Value when transacted	\$10.15



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	bc1qex0aqq8mxqfh4cp162eg755836djjx20yzuuu8	Value	0.00051407 BTC
Pkscript	OP_0 c99fd000fb30137ae03fd2b28f52878e9b29194f		
Sigscript			
Witness	3044022017bd023c1c073d463ebea129e7e2a8bfffabb24c0695a344bdc4fba8e4304cbda02205f0175a05108757a0cc35a455645a1a6f1d047b13ec3aea348617a6bb2e5db a401 031f6fa906bb52f3e1bdc59156a5659ce1aa251eaf26f411413c76409360ef7205		

Output contains addresses, public key scripts and the amount of bitcoins spent/unspent.

Department of Computer Engineering

Outputs ①

Index	0	Details	Unspent
Address	1A1zP1eP5QGefi2DMPTfTL5Lmv7DivfNa	Value	0.00000558 BTC
Pkscript	OP_DUP OP_HASH160 62e907b15cbf27d5425399ebf6f0fb50ebb88f18 OP_EQUALVERIFY OP_CHECKSIG		
Index	1	Details	Unspent
Address	bc1qex0aqq8mxqfh4cpI62eg755836djx20yzuuu8	Value	0.00050703 BTC
Pkscript	OP_0 c99fd000fb30137ae03fd2b28f52878e9b29194f		

The block explorer also provides us with charts and statistics of the blockchain like currency statistics, block details, mining information, network activity, wallet activity etc.

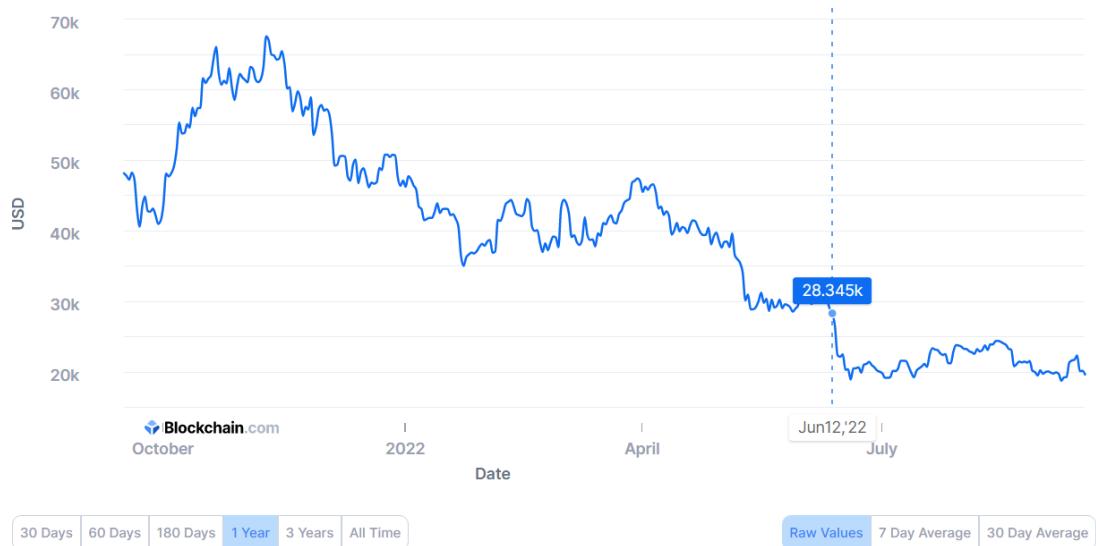
Blockchain Charts

The most trusted source for data on the bitcoin blockchain



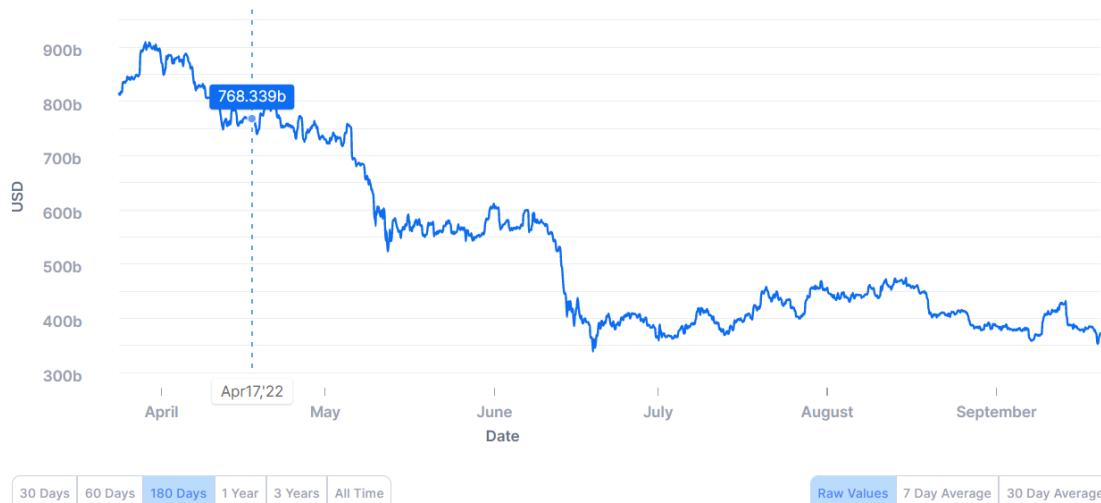
Market Price (USD)

The average USD market price across major bitcoin exchanges.

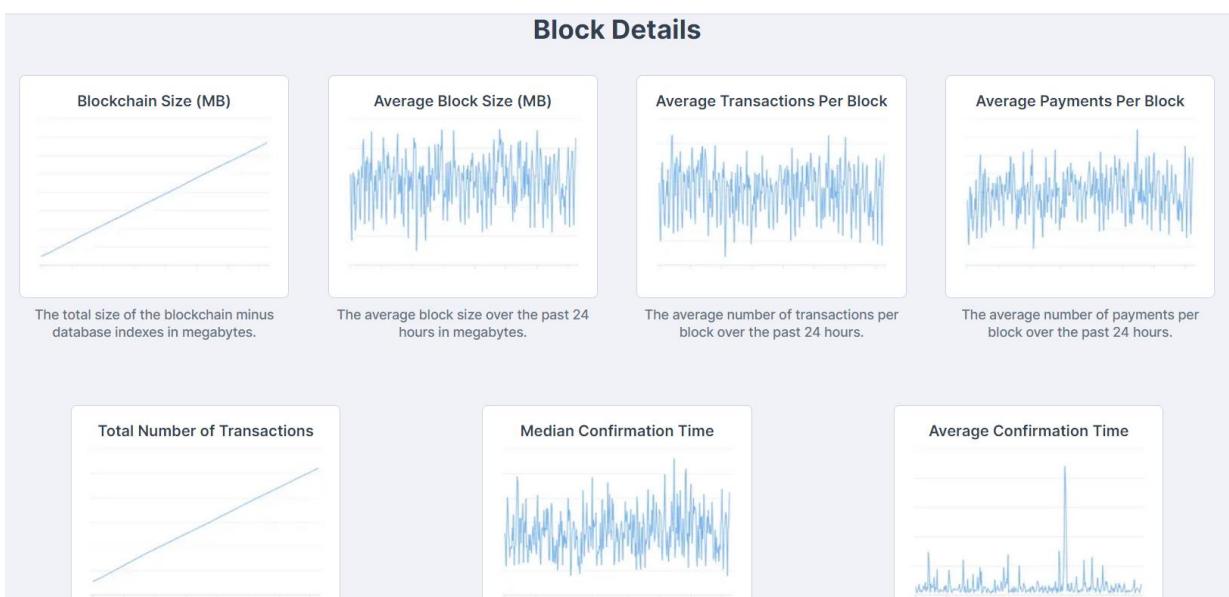


Market Capitalization (USD)

The total USD value of bitcoin in circulation.

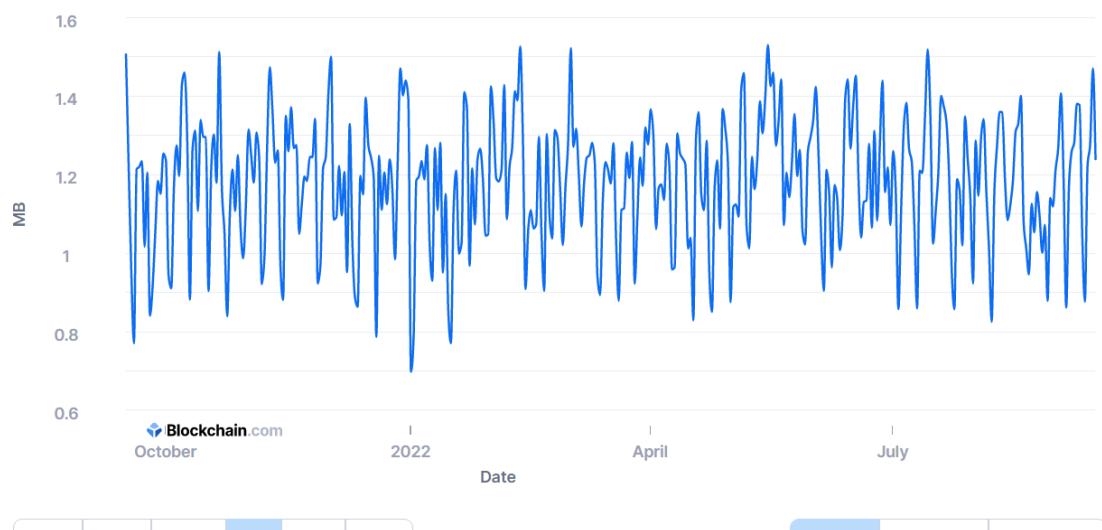


Department of Computer Engineering



Average Block Size (MB)

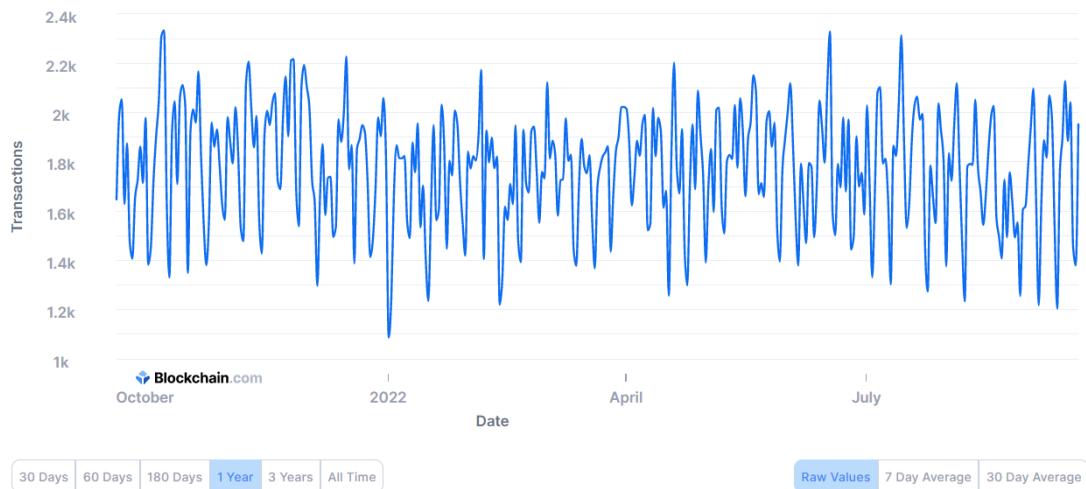
The average block size over the past 24 hours in megabytes.



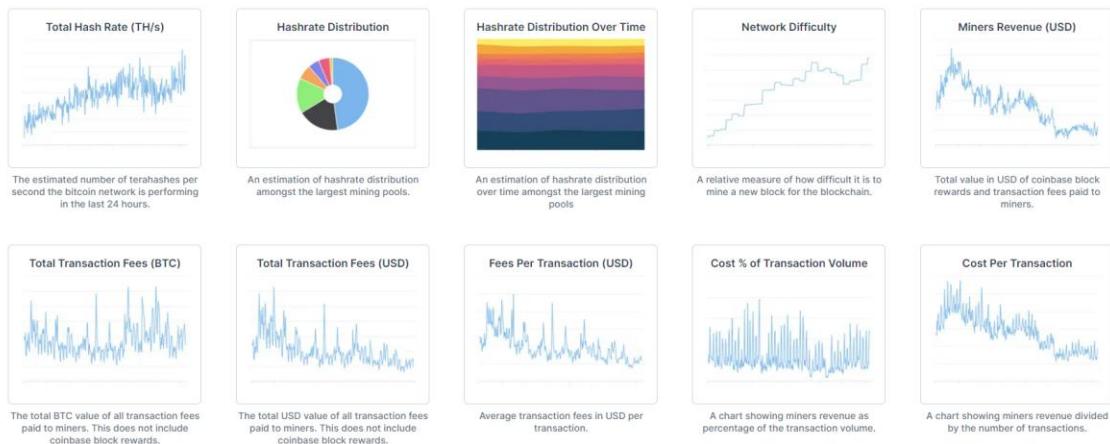
Department of Computer Engineering

Average Transactions Per Block

The average number of transactions per block over the past 24 hours.

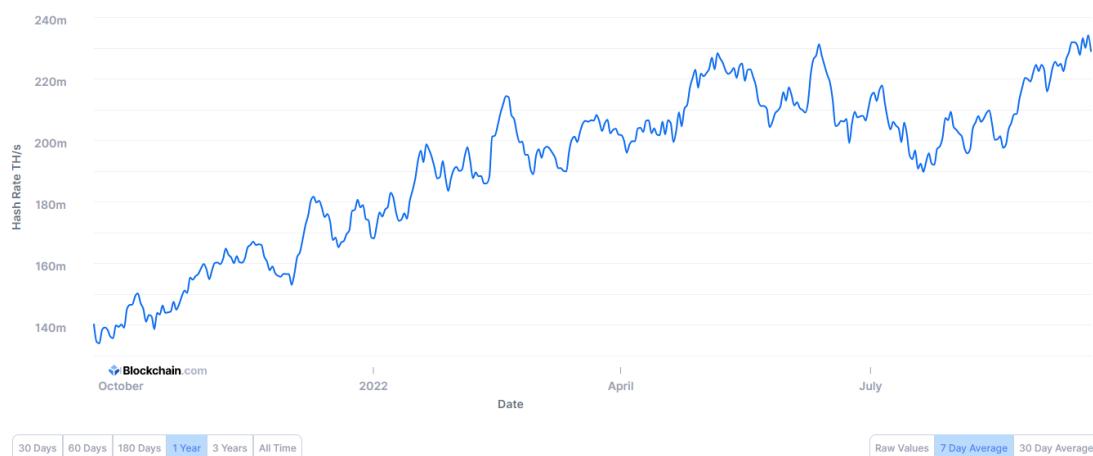


Mining Information



Total Hash Rate (TH/s)

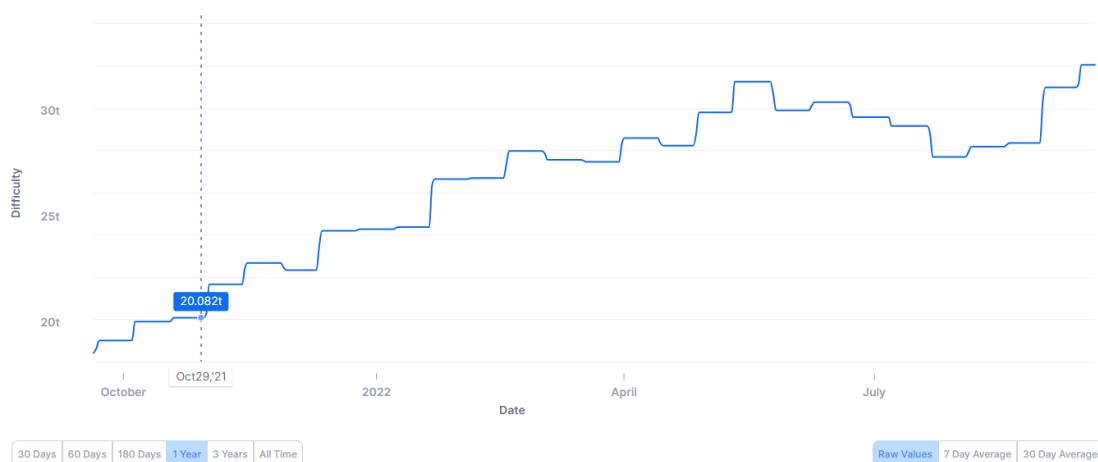
The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.



Department of Computer Engineering

Network Difficulty

A relative measure of how difficult it is to mine a new block for the blockchain.

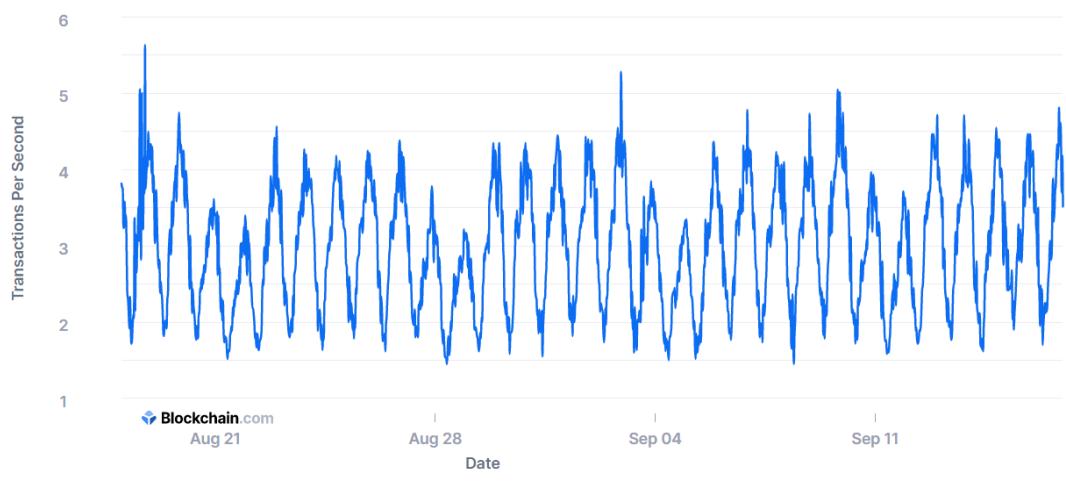


Network Activity



Transaction Rate Per Second

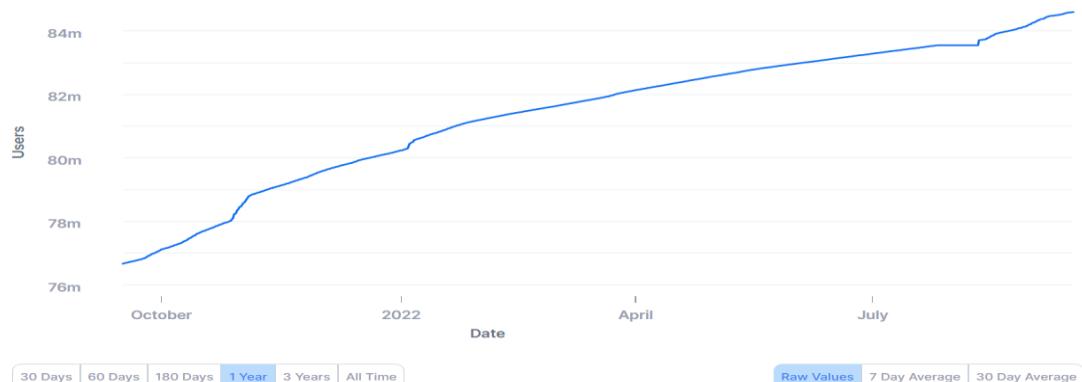
The number of transactions added to the mempool per second.



Department of Computer Engineering

Blockchain.com Wallets

The total number of unique Blockchain.com wallets created.



Market Signals

Market Value to Realised Value



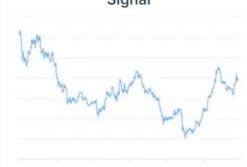
MVRV is calculated by dividing Market Value by Realised Value. In Realised Value, BTC prices are taken at the time they last moved, instead of the current price like in Market Value

Network Value to Transactions



NVT is computed by dividing the Network Value (= Market Value) by the total transactions volume in USD over the past 24hour.

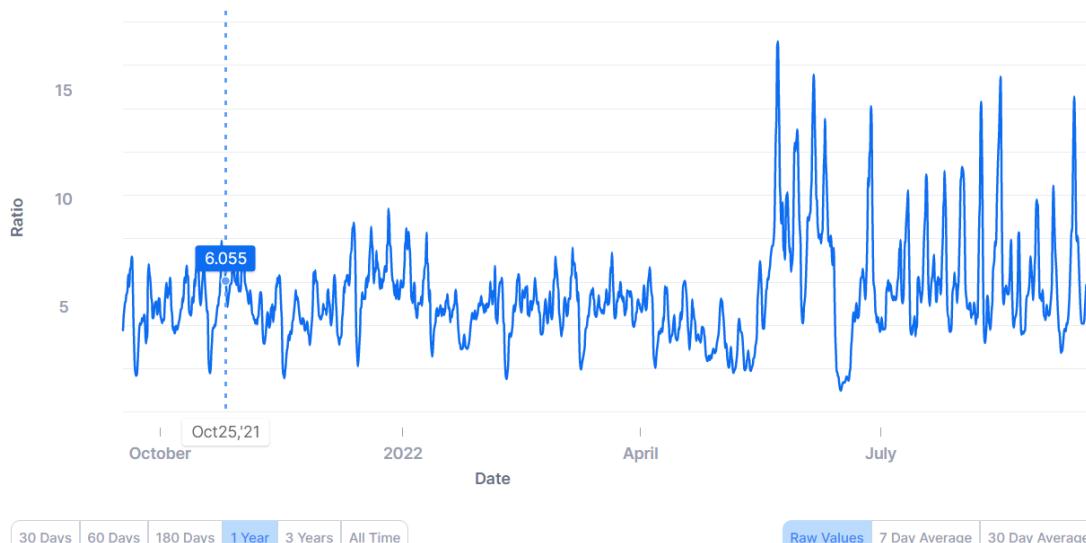
Network Value to Transactions Signal



NVTS is a more stable measure of NVT, with the denominator being the moving average over the last 90 days of NVT's denominator

Network Value to Transactions

NVT is computed by dividing the Network Value (= Market Value) by the total transactions volume in USD over the past 24hour.



Department of Computer Engineering

Block explorer – Ethereum: <https://etherscan.io/>
Ethereum blocks can be viewed by using etherscan.

The Ethereum Blockchain Explorer

All Filters ▼ Search by Address / Txn Hash / Block / Token / Ens 🔍

Sponsored:  - SX Bet | Bet on 100s of Sports | Bet in USDC or ETH

ETHER PRICE
\$1,339.82 @ 0.07103 BTC (+0.84%)

MARKET CAP
\$161,480,306,634.00

TRANSACTIONS
1,717.60 M (14.1 TPS)

LAST FINALIZED BLOCK
15576200

MED GAS PRICE
18 Gwei (\$0.51)

LAST SAFE BLOCK
15576232

AAX Savings Marathon
Up to 300,000 USDT Rewards in 42 Days.

AAX

ETHEREUM TRANSACTION HISTORY IN 14 DAYS



Latest Blocks

Bk	Fee Recipient	Fee
15576265	0x388c818ca8b9251b39...	0.03879 Eth 18 secs ago
156 txns	in 12 secs	

Latest Transactions

Tx	From	To	Value
0xb9b9ab42ec52...	0x31fc2cb761083a77cf2...	0xdac17f958d2ee523a2...	0 Eth

The genesis block in ethereum :

Block #0	
Overview	Comments
② Block Height:	0 (less) (more)
② Status:	Finalized
② Timestamp:	② 2609 days 2 hrs ago (Jul-30-2015 03:26:13 PM +UTC)
② Transactions:	8893 transactions and 0 contract internal transaction in this block
② Mined by:	0x00(Null Address: 0x000...000) in 15 secs
② Block Reward:	5 Ether
② Uncles Reward:	0
② Difficulty:	17,179,869,184
② Total Difficulty:	17,179,869,184
② Size:	540 bytes
② Gas Used:	0 (0.00%)
② Gas Limit:	5,000
② Extra Data:	0x000N4{N00 0p03000 0z8000000 (Hex 0x11bbe8db4e347b4e8c937c1c8370e4b5ed33adb3db69cdb7a38e1e50b1b82fa)
② Ether Price:	N/A
② Hash:	0xd4e56740f876aef8c010b86a40d5f56745a118d0906a34e69aec8c0db1cb8fa3
② Parent Hash:	0x00
② Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6cccd41ad312451b948a7413f0a142fd40d49347
② StateRoot:	0xd7f8974fb5ac78d9ac099b9ad5018bedc2ce0a72dad1827a1709da30580f0544
② Nonce:	0x00000000000000042

Department of Computer Engineering

The explorer also shows the different transactions along with ethers transferred along with the addresses of the sender and the receivers.

A total of 8,893 transactions found							
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	0xc951900c341abb3ba...	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	0xcf8882359c0fb233871...	6,000 Ether	0
GENESIS_457bcef37dd...	-	0	2605 days 21 hrs ago	GENESIS	0x457bcef37dd3d60b2d...	20 Ether	0

We can also click on the addresses to get information about that bitcoin address including the number of transactions involving the address and the balance held by the address.

Address 0x756f45e3fa69347a9a973a725e3c98bC4db0b5a0

Featured: Wallet-to-wallet instant messaging via [Blockscan Chat!](#)

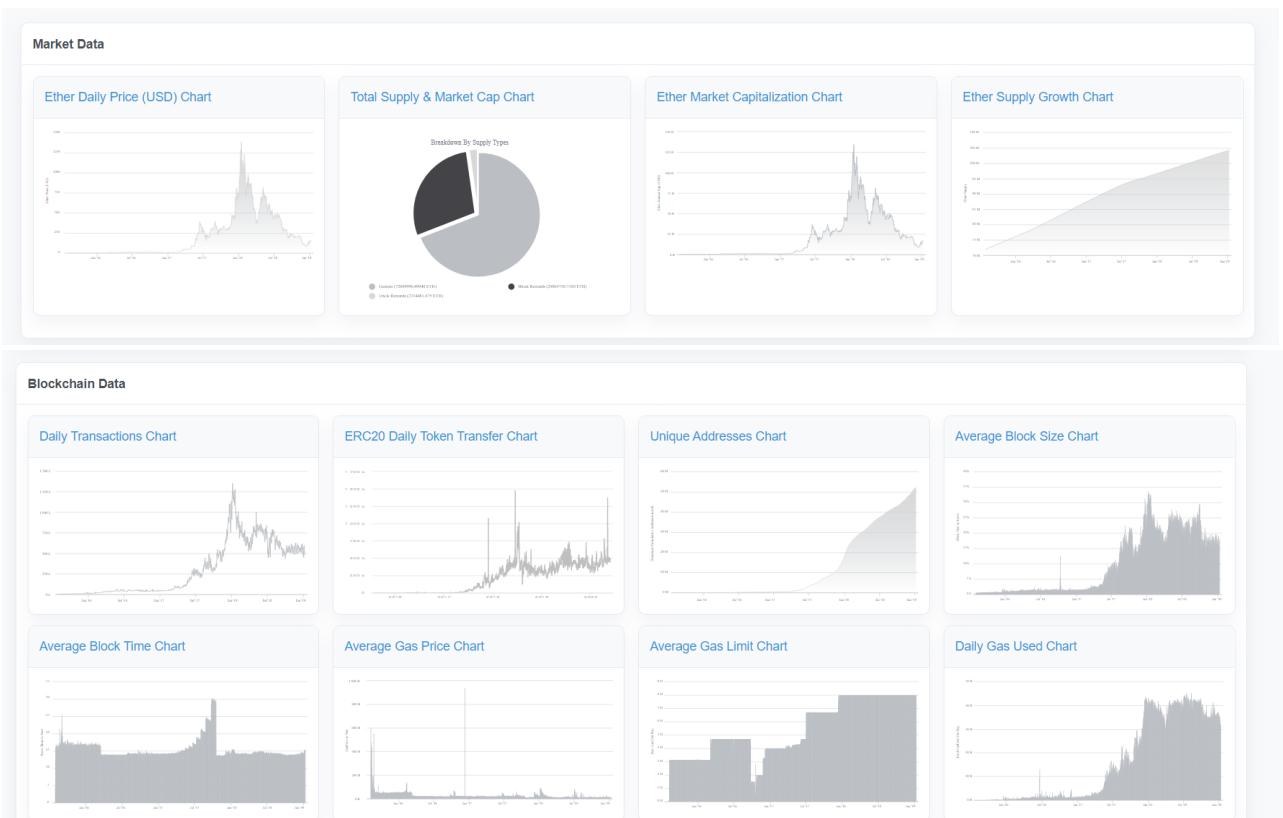
Overview	More Info
Balance: 0.026991556 Ether	My Name Tag: Not Available, login to update
Ether Value: \$38.41 (@ \$1,422.97/ETH)	
Token: \$0.00	View token holdings in more detail

All the transactions involving the address can also be seen at the bottom of the page. All the transactions with its transaction fees, amount of ethers transferred, from and to address of the transaction and the date of the transaction can also be visible.

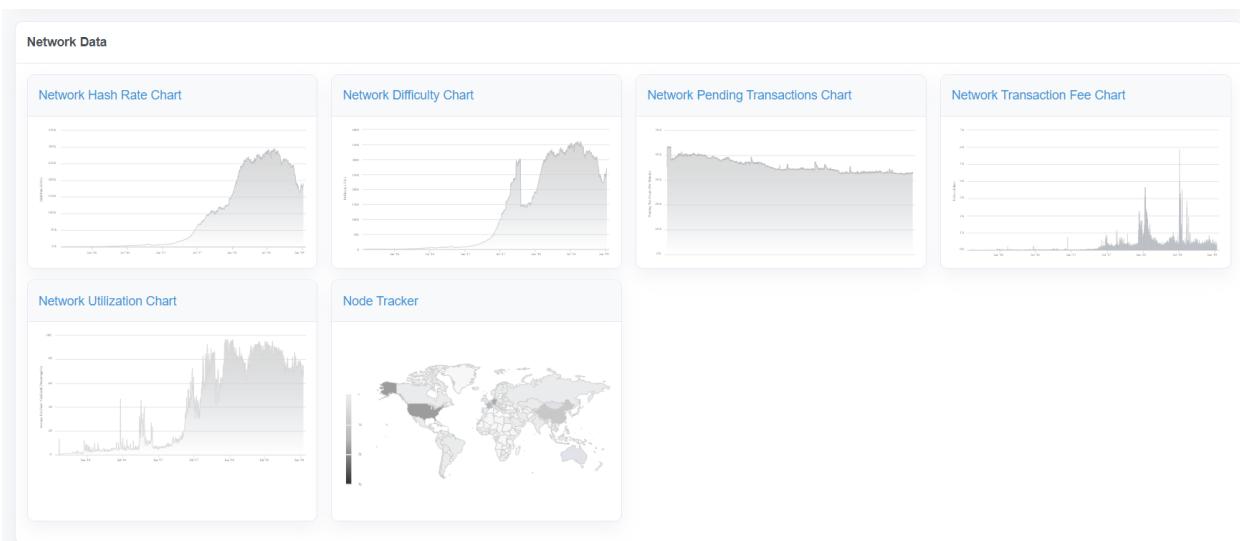
Department of Computer Engineering

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				
0xf31b0681935feaab3c...	Transfer	14633598	148 days 4 hrs ago	0x8f40bebfa753e6392d...	IN	0x756f45e3fa69347a9a9...	0.000001 Ether	0.000525			
0x8244c599c49f2de53b...	Transfer*	8986057	1029 days 1 hr ago	0x503a58e109472e0cc...	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			
0x7cae935a73739b3ac...	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			

Like bitcoin, ethereum block explorer also provides the historical data of the ethereum in terms of charts which can be seen in the charts section. Market data, Blockchain data, network data, etc are available in the charts section.



Department of Computer Engineering



Ethereum includes smart contracts which are computer programs or transaction protocols that are intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement. Etherscan shows 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](#).

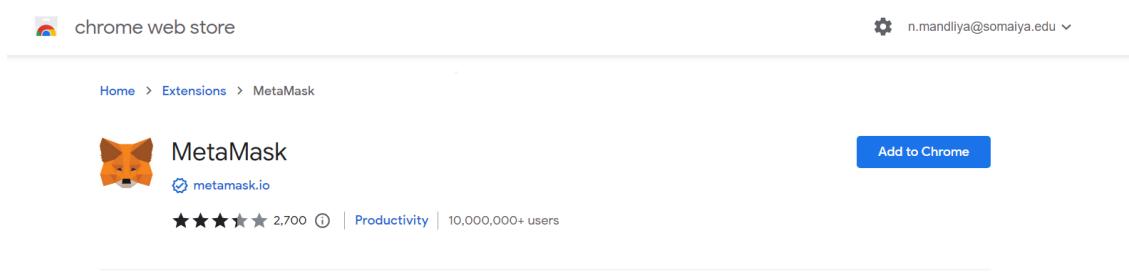
Showing the last 500 verified contracts source code									
Address	Contract Name	Compiler	Version	Balance	Txns	Setting	Verified	Audited	License
0x7ff923eb49c0cd16f0b6...	SQUID	Solidity	0.8.4	0 Ether	10	⌚	9/17/2022	-	Unlicense
0xbd0d8c8a1521076297...	ElevateSplit	Solidity	0.8.4	0 Ether	2	⌚	9/17/2022	-	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	-	-
0x4beaefaa2a6682f454...	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...	CyriLand	Solidity(Json)	0.8.9	0 Ether	2	⌚	9/17/2022	-	-
0xb6e34b42c0be1c618b9...	VoterUpgradeable	Solidity(Json)	0.8.2	0 Ether	1	⌚	9/17/2022	-	-

Testnets:

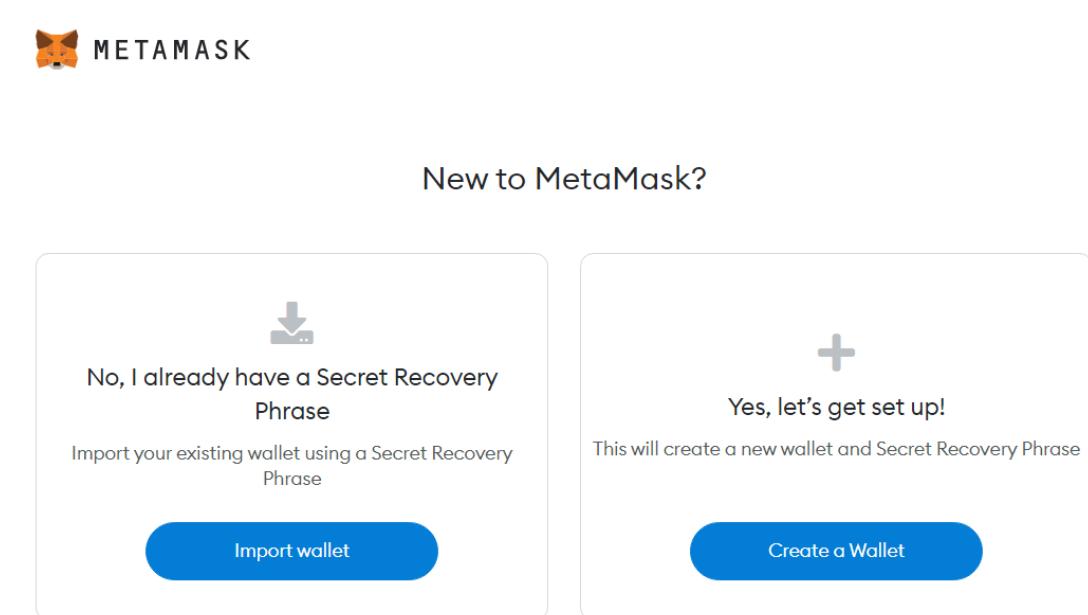
In blockchain technology, a testnet is an instance of a blockchain powered by the same or a newer version of the underlying software, to be used for testing and experimentation without risk to real funds or the main chain. Testnet coins are separate and distinct from the official (*mainnet*) coins, don't have value, and can be obtained freely from *faucets*. Testnets can be reset at any time.

Metamask: <https://metamask.io/>

Install Metamask extension from chrome.



Open the chrome extension and click on create wallet.





Create Password

New password (8 characters min)

.....

Confirm password

.....



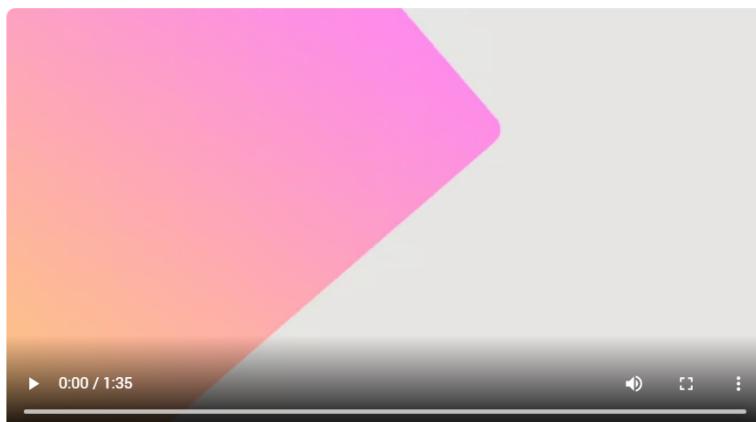
I have read and agree to the [Terms of Use](#)

Create



Secure your wallet

Before getting started, watch this short video to learn about your Secret Recovery Phrase and how to keep your wallet safe.



What is a Secret Recovery Phrase?

Your Secret Recovery Phrase is a 12-word phrase that is the “master key” to your wallet and your funds

How do I save my Secret Recovery Phrase?

- Save in a password manager
- Store in a bank vault
- Store in a safe deposit box
- Write down and store in multiple secret places

Should I share my Secret Recovery Phrase?

Never, ever share your Secret Recovery Phrase, not even with MetaMask!

If someone asks for your recovery phrase they are likely trying to scam you and steal your wallet funds.

A secret recovery phrase is given during the account creation and which is unique for every account, store the recovery phase securely.

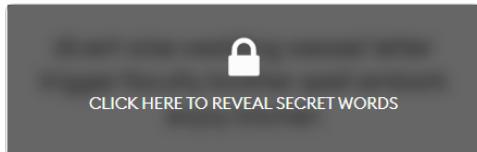


< Back

Secret Recovery Phrase

Your Secret Recovery Phrase makes it easy to back up and restore your account.

WARNING: Never disclose your Secret Recovery Phrase. Anyone with this phrase can take your Ether forever.



Remind me later

Next

Tips:

Store this phrase in a password manager like 1Password.

Write this phrase on a piece of paper and store in a secure location. If you want even more security, write it down on multiple pieces of paper and store each in 2 - 3 different locations.

Memorize this phrase.

Download this Secret Recovery Phrase and keep it stored safely on an external encrypted hard drive or storage medium.



Congratulations

You passed the test - keep your Secret Recovery Phrase safe, it's your responsibility!

Tips on storing it safely

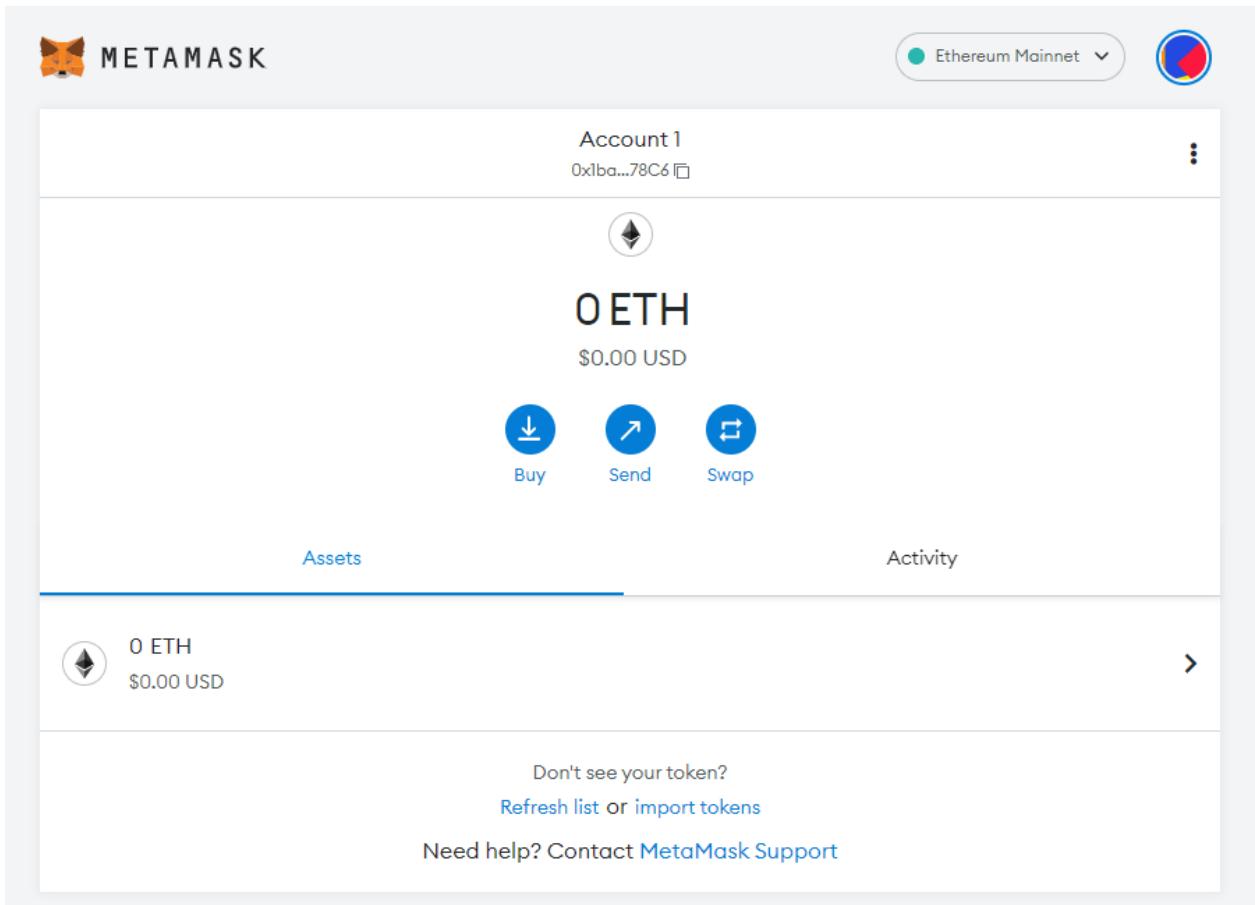
- Save a backup in multiple places.
- Never share the phrase with anyone.
- Be careful of phishing! MetaMask will never spontaneously ask for your Secret Recovery Phrase.
- If you need to back up your Secret Recovery Phrase again, you can find it in Settings -> Security.
- If you ever have questions or see something fishy, contact our support [here](#).

*MetaMask cannot recover your Secret Recovery Phrase. [Learn more](#).

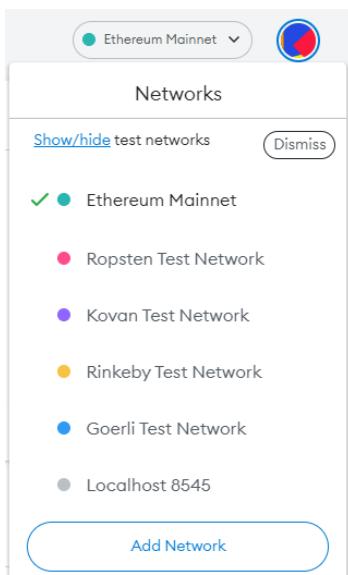
All Done

Department of Computer Engineering

After the wallet is created home page will show the amount of cryptocurrency available in the wallet, account address, activity and assets associated with the account.

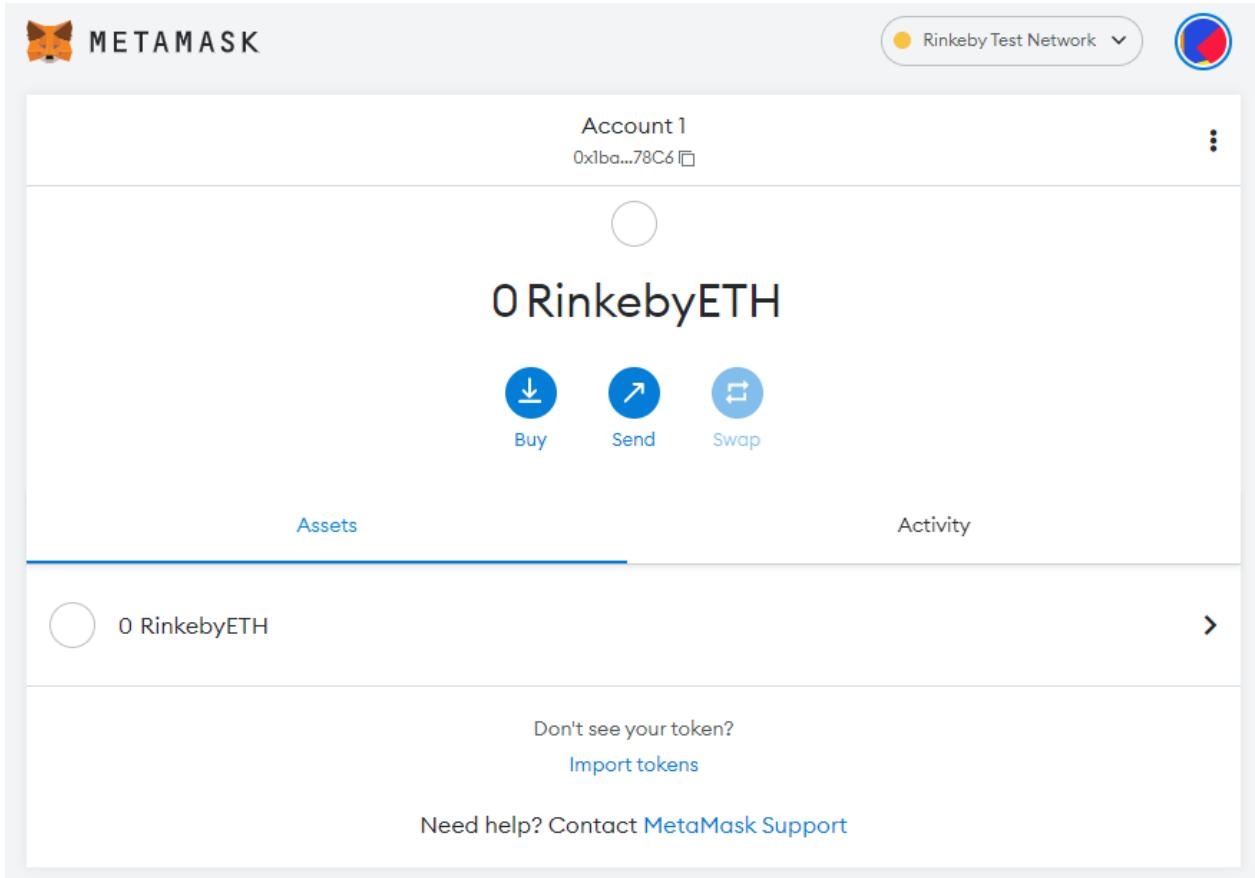


Metamask allows us to own currencies and make transactions on different testnets seen in the drop down menu.

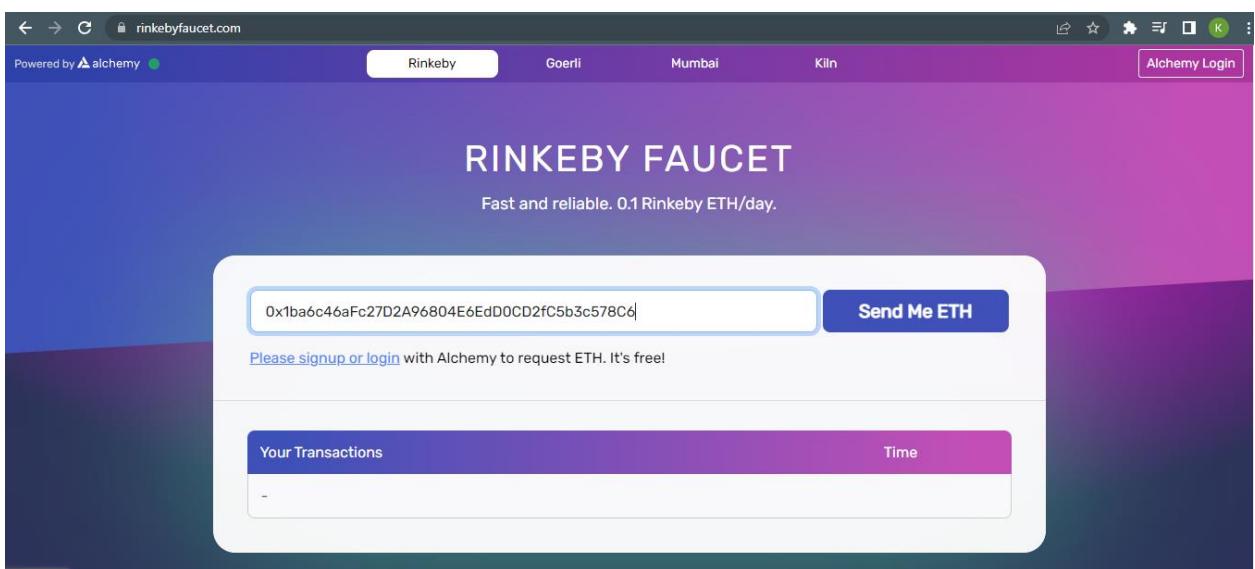


Department of Computer Engineering

Currencies for the test networks can be obtained using faucets. I have currently 0 ethers in rinkeby but I can obtain the ethers using rinkebyfaucet.



Rinkeby Faucet: We just need to copy our address and paste it to get the test ethers.



Department of Computer Engineering

Wallet address

0x1ba6c46afc27d2a96804e6edd0cd2fc5b3c578c6

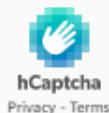
Request type

20 test LINK

0.1 test ETH

Verify request

 I am human



Send request

RINKEBY FAUCET

Fast and reliable. 0.5 Rinkeby ETH/day.

Due to ETH Merge, the Rinkeby Testnet will be deprecated soon. Please develop using our [Goerli Testnet faucet](#). 

0x1ba6c46aFc27D2A96804E6EdD0CD2fC5b3c578C6

Send Me ETH

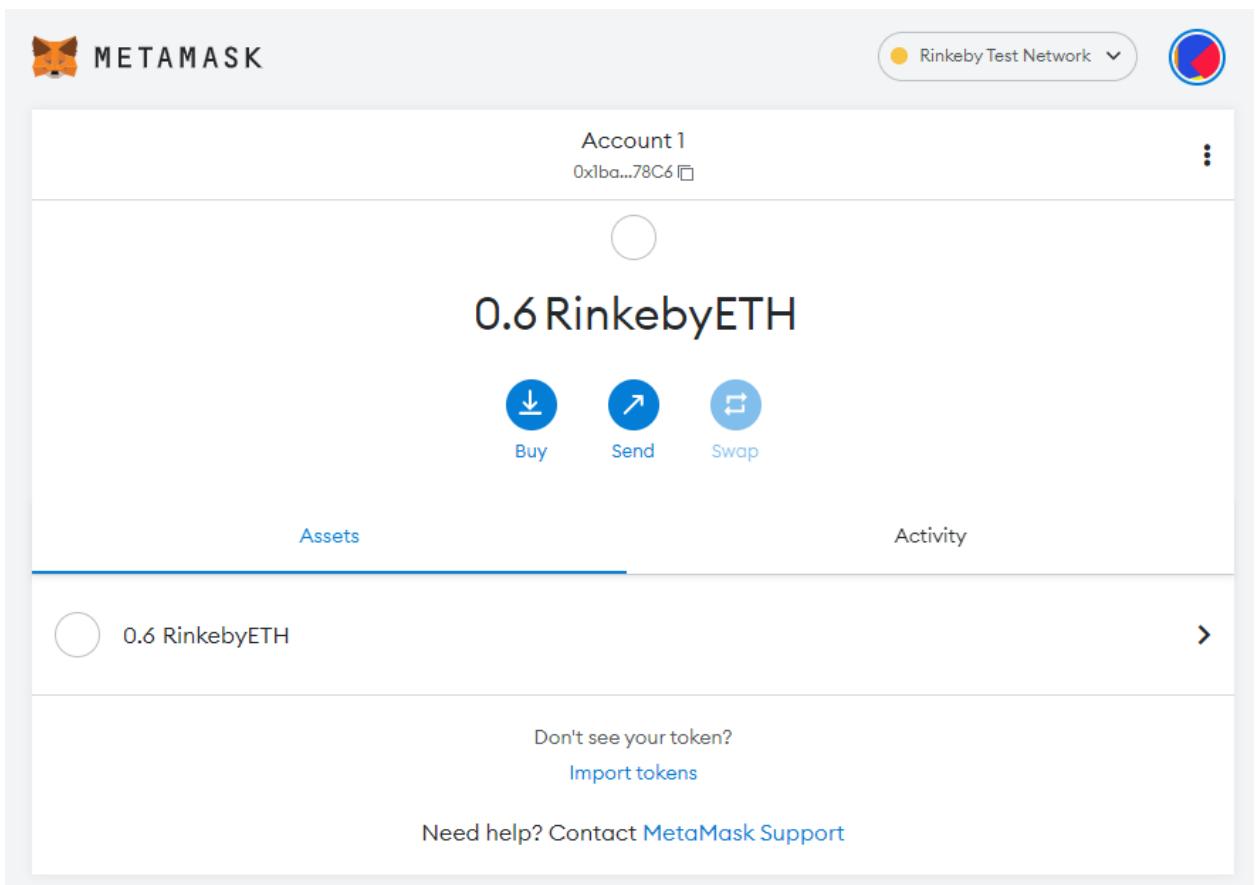
✓ Alchemy account connected, receive 0.5 Rinkeby ETH! Get 2x ETH by [sending requests](#) through Alchemy!

Your Transactions

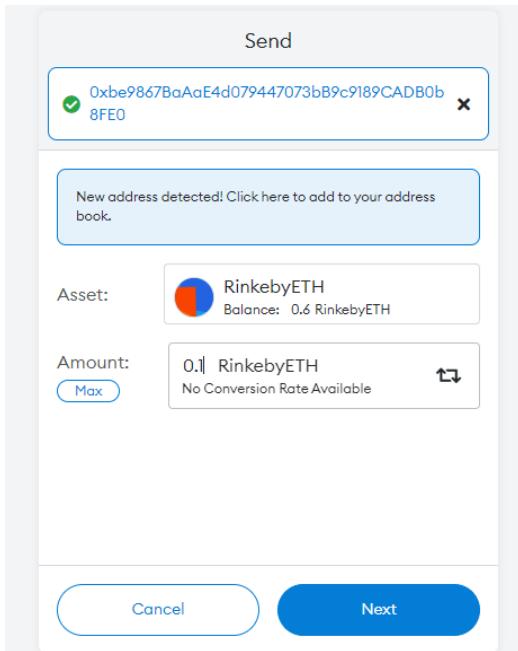
Time

◆ 0x6ce12405c804df4e12423dffff70d936e39450fc9ebe47f0c481aeb3e5ff515

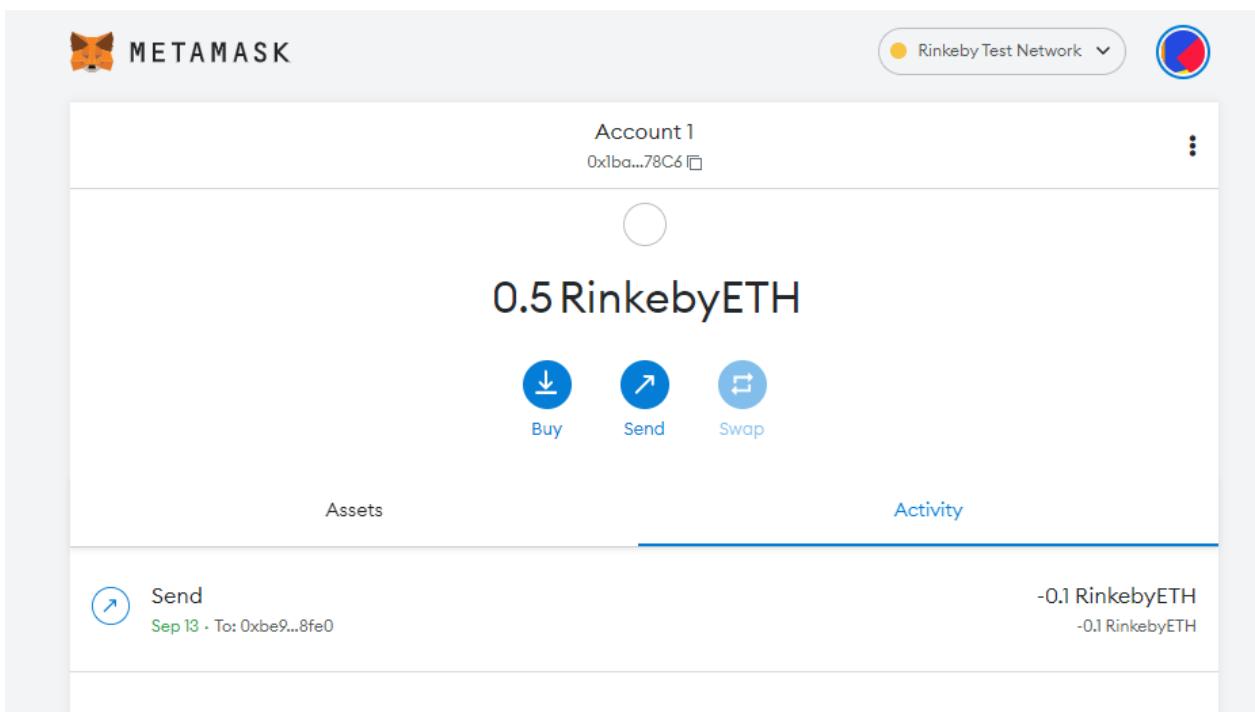
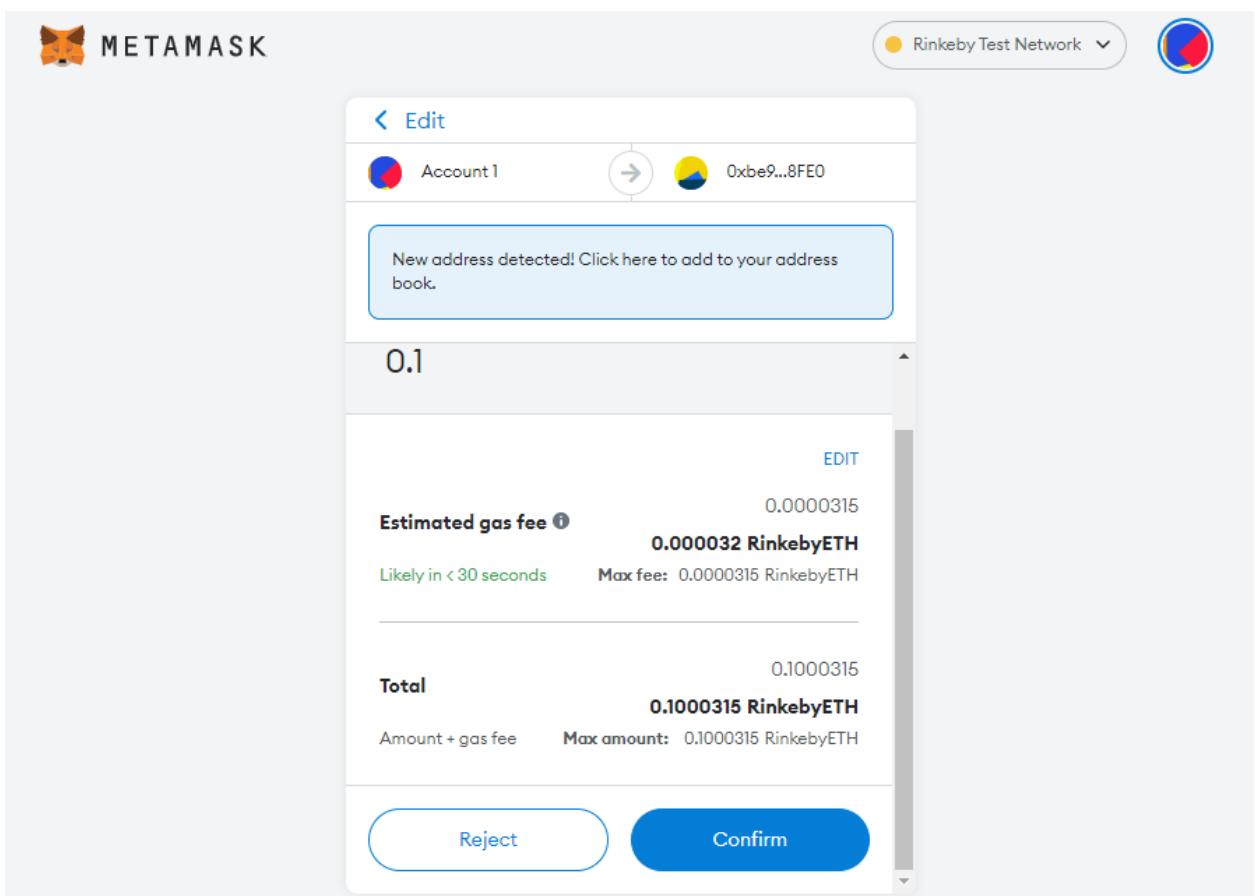
43 seconds ago



Thus 0.6 rinkeby eth were added to my account by using faucets. This can be used to make transactions to other addresses as well.



Department of Computer Engineering



Department of Computer Engineering

From	To
0x1ba...78C6	0xbe9...8FEO

Transaction	
Nonce	0
Amount	-0.1 RinkebyETH
Gas Limit (Units)	21000
Gas Used (Units)	21000
Base Fee (GWEI)	0.000000008
Priority Fee (GWEI)	1.5
Total Gas Fee	0.0000031 RinkebyETH
Max Fee Per Gas	0.000000002 RinkebyETH
Total	0.1000315 RinkebyETH

+ Activity log

Thus 0.1 RinkebyETH has been sent from my account to another address.

Conclusion:-

Understood the important concepts used in blockchain by performing demonstrations and explored and analysed blocks, structure and statistics of existing blockchain implementations such as Bitcoin and Ethereum using their respective block explorers. Also understood use of testnets and performed transactions on it using metamask wallets.

Virtual labs:

Virtual lab 1

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.

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

Department of Computer Engineering

1) Blockchain valid chain:

Simulation

Pop Up Procedure

Blockchain valid chain exercise

INSTRUCTIONS:

Connect the blocks(circles) in the order specified below to make a valid chain!

1. B -> D
2. D -> C
3. A -> B

#1 Notification
It is valid

2) Open ledger:

OPEN LEDGER

INSTRUCTIONS:

1. Enter Name and amount.
2. User A gets money from the Bank.
3. Click on "Submit" button to accept the transaction.
4. Now enter name and amount whom you want to send the transaction
5. Amount which you enter in the second and third transaction should be less than or equal to the amount which you received.

Department of Computer Engineering

3) Distributed ledger:

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" button.
3. A popup shows a message "Valid!".
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.

DISTRIBUTION

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Block A</td> <td style="width: 50%; padding: 5px;">Block B</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	Initiate Immutability Experiment			
Block A	Block B								
A -> B Amount: 10	A -> B Amount: 10								
B -> C Amount: 20	B -> C Amount: 20								
B -> C Amount: 20	B -> C Amount: 20								

#2 Notification
 Different number of blocks in nodes, invalid!

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Block A</td> <td style="width: 50%; padding: 5px;">Block B</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Block A</td> <td style="width: 50%; padding: 5px;">Block B</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Block A</td> <td style="width: 50%; padding: 5px;">Block B</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20									
Block A	Block B																									
A -> B Amount: 10	A -> B Amount: 10																									
B -> C Amount: 20	B -> C Amount: 20																									
B -> C Amount: 20	B -> C Amount: 20																									
Block A	Block B																									
A -> B Amount: 10	A -> B Amount: 10																									
B -> C Amount: 20	B -> C Amount: 20																									
B -> C Amount: 20	B -> C Amount: 20																									
Block A	Block B																									
A -> B Amount: 10	A -> B Amount: 10																									
B -> C Amount: 20	B -> C Amount: 20																									
B -> C Amount: 20	B -> C Amount: 20																									

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Block A</td> <td style="width: 50%; padding: 5px;">Block B</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Block A</td> <td style="width: 50%; padding: 5px;">Block B</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Block A</td> <td style="width: 50%; padding: 5px;">Block B</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20									
Block A	Block B																									
A -> B Amount: 10	A -> B Amount: 10																									
B -> C Amount: 20	B -> C Amount: 20																									
B -> C Amount: 20	B -> C Amount: 20																									
Block A	Block B																									
A -> B Amount: 10	A -> B Amount: 10																									
B -> C Amount: 20	B -> C Amount: 20																									
B -> C Amount: 20	B -> C Amount: 20																									
Block A	Block B																									
A -> B Amount: 10	A -> B Amount: 10																									
B -> C Amount: 20	B -> C Amount: 20																									
B -> C Amount: 20	B -> C Amount: 20																									

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Block A</td> <td style="width: 50%; padding: 5px;">Block B</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Block A</td> <td style="width: 50%; padding: 5px;">Block B</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Block A</td> <td style="width: 50%; padding: 5px;">Block B</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20									
Block A	Block B																									
A -> B Amount: 10	A -> B Amount: 10																									
B -> C Amount: 20	B -> C Amount: 20																									
B -> C Amount: 20	B -> C Amount: 20																									
Block A	Block B																									
A -> B Amount: 10	A -> B Amount: 10																									
B -> C Amount: 20	B -> C Amount: 20																									
B -> C Amount: 20	B -> C Amount: 20																									
Block A	Block B																									
A -> B Amount: 10	A -> B Amount: 10																									
B -> C Amount: 20	B -> C Amount: 20																									
B -> C Amount: 20	B -> C Amount: 20																									

VALIDATE
RESET

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" button.
3. A popup shows a message "Valid!".
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.

DISTRIBUTION

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Block A</td> <td style="width: 50%; padding: 5px;">Block B</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	Initiate Immutability Experiment			
Block A	Block B								
A -> B Amount: 10	A -> B Amount: 10								
B -> C Amount: 20	B -> C Amount: 20								
B -> C Amount: 20	B -> C Amount: 20								

#3 Notification
 Valid!

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; padding: 5px;">Block A</td> <td style="width: 33%; padding: 5px;">Block B</td> <td style="width: 33%; padding: 5px;">Block C</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	Block C	A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; padding: 5px;">Block A</td> <td style="width: 33%; padding: 5px;">Block B</td> <td style="width: 33%; padding: 5px;">Block C</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	Block C	A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; padding: 5px;">Block A</td> <td style="width: 33%; padding: 5px;">Block B</td> <td style="width: 33%; padding: 5px;">Block C</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	Block C	A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20															
Block A	Block B	Block C																																				
A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				
Block A	Block B	Block C																																				
A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				
Block A	Block B	Block C																																				
A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; padding: 5px;">Block A</td> <td style="width: 33%; padding: 5px;">Block B</td> <td style="width: 33%; padding: 5px;">Block C</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	Block C	A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; padding: 5px;">Block A</td> <td style="width: 33%; padding: 5px;">Block B</td> <td style="width: 33%; padding: 5px;">Block C</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	Block C	A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; padding: 5px;">Block A</td> <td style="width: 33%; padding: 5px;">Block B</td> <td style="width: 33%; padding: 5px;">Block C</td> </tr> <tr> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> <td>A -> B Amount: 10</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> <tr> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> <td>B -> C Amount: 20</td> </tr> </table>	Block A	Block B	Block C	A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10	B -> C Amount: 20															
Block A	Block B	Block C																																				
A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				
Block A	Block B	Block C																																				
A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				
Block A	Block B	Block C																																				
A -> B Amount: 10	A -> B Amount: 10	A -> B Amount: 10																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				
B -> C Amount: 20	B -> C Amount: 20	B -> C Amount: 20																																				

VALIDATE
RESET

Department of Computer Engineering

BCT Sem-VII – July-Nov 2022

Page - 46

Department of Computer Engineering

4) Immutability:

End of Experiment

Immutability

INSTRUCTIONS:

1. Try deleting block of Node A. 2. Now click the "Validate" button.
3. Error occurs on Node A(it turns red).
4. Now delete remaining blocks of Node A and then click on the "Validate" button.
5. The blocks get deleted.
6. Therefore the blocks of Node A are deleted which tells us that atleast 51% Consensus.

Node A		
Incomplete chain A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	Invld: Prev Blck Invld A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	
<input type="button" value="Toggle"/>	<input type="button" value="Toggle"/>	<input type="button" value="Toggle"/>

Node B		
Block A A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	Block B A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	Block C A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20
<input type="button" value="Toggle"/>	<input type="button" value="Toggle"/>	<input type="button" value="Toggle"/>

Node C		
Block A A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	Block B A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	Block C A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20
<input type="button" value="Toggle"/>	<input type="button" value="Toggle"/>	<input type="button" value="Toggle"/>

VALIDATE

End of Experiment

Immutability

INSTRUCTIONS:

1. Try deleting block of Node A. 2. Now click the "Validate" button.
3. Error occurs on Node A(it turns red).
4. Now delete remaining blocks of Node A and then click on the "Validate" button.
5. The blocks get deleted.
6. Therefore the blocks of Node A are deleted which tells us that atleast 51% Consensus.

Node A		
Block A A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	Block B A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	Block C A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20
<input type="button" value="Toggle"/>	<input type="button" value="Toggle"/>	<input type="button" value="Toggle"/>

Node B	
Invld: Prev Blck Invld A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	Invld: Prev Blck Invld A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20
<input type="button" value="Toggle"/>	<input type="button" value="Toggle"/>

Node C		
Block A A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	Block B A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	Block C A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20
<input type="button" value="Toggle"/>	<input type="button" value="Toggle"/>	<input type="button" value="Toggle"/>

VALIDATE

Department of Computer Engineering

Immutability
End of Experiment

INSTRUCTIONS:

1. Try deleting block of Node A. 2. Now click the "Validate" button.
3. Error occurs on Node A (it turns red).
4. Now delete remaining blocks of Node A and then click on the "Validate" button.
5. The blocks get deleted.
6. Therefore the blocks of Node A are deleted which tells us that atleast 51% Consensus.

#2 Notification

Node A

Block A	Block B	Block C
A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20
<button style="border: 1px solid #ccc; padding: 2px 5px;">Toggle</button>	<button style="border: 1px solid #ccc; padding: 2px 5px;">Toggle</button>	<button style="border: 1px solid #ccc; padding: 2px 5px;">Toggle</button>

Valid!

X

Node B

Block A	Block B	Block C
A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20
<button style="border: 1px solid #ccc; padding: 2px 5px;">Toggle</button>	<button style="border: 1px solid #ccc; padding: 2px 5px;">Toggle</button>	<button style="border: 1px solid #ccc; padding: 2px 5px;">Toggle</button>

X

X

Node C

Block A	Block B	Block C
A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20	A -> B Amt: 10 B -> C Amt: 20 B -> C Amt: 20
<button style="border: 1px solid #ccc; padding: 2px 5px;">Toggle</button>	<button style="border: 1px solid #ccc; padding: 2px 5px;">Toggle</button>	<button style="border: 1px solid #ccc; padding: 2px 5px;">Toggle</button>

X

X

VALIDATE

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.
- c : Ledger is mutable.
- d : None Of these

Which of the following is true for distributed ledger?

- a : Everyone has a copy of ledger
- 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
- 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

How can a user successfully modify a blockchain?

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

Submit Quiz

5 out of 5

Department of Computer Engineering

BCT Sem-VII – July-Nov 2022

Page - 48

Virtual lab 2

Mining in Blockchain

Aim

In this experiment, the user will learn about mining in blockchain i.e. how a transaction is validated and added into a blockchain. He/she will learn how the process of hashing helps in validation of a block. He/she will also get to know which miner is rewarded when a block is validated and added to the blockchain.

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 cryptocurrency?

- a : Reserve 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

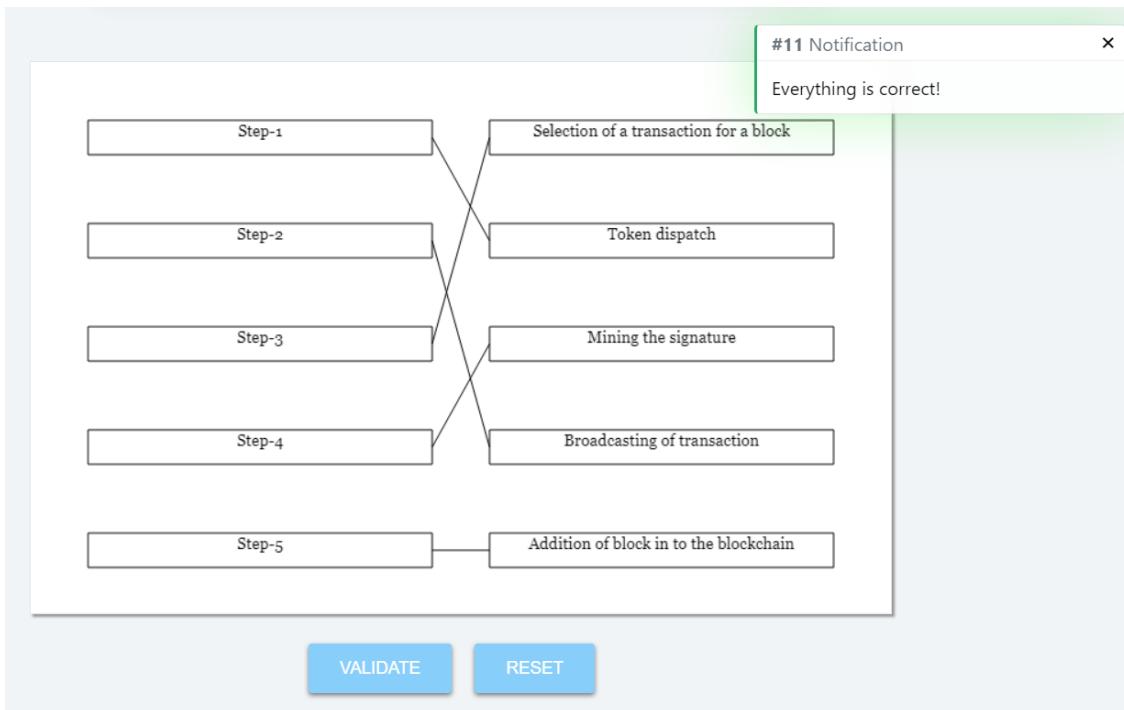
What is the process of creating new bitcoins popularly known as?

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

Submit Quiz

7 out of 7

Department of Computer Engineering



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.

Before mining:

Mining Process

From To Amount

ADD TO BLOCK **START MINING PROCESS** **RESET**

k.

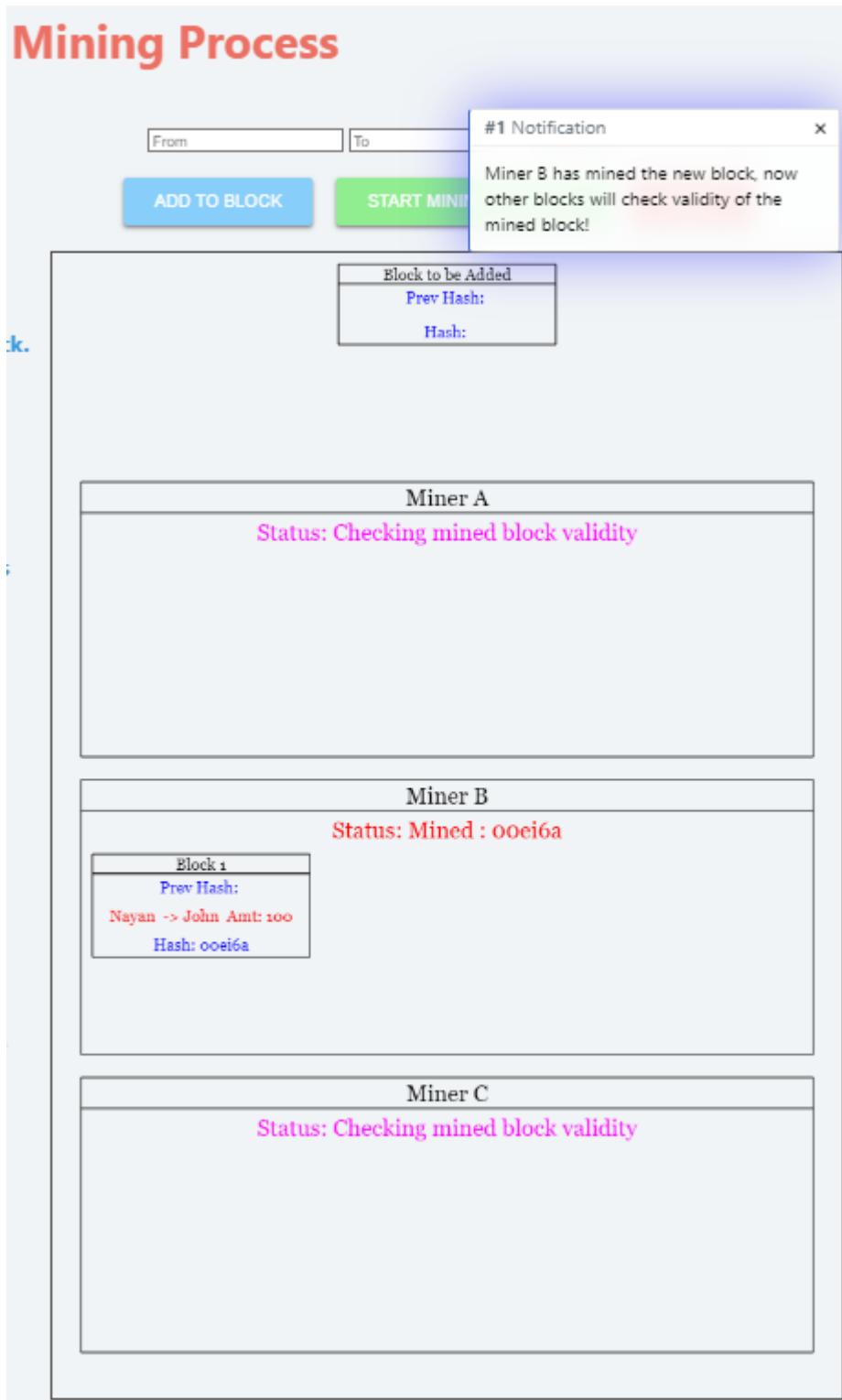
Block to be Added
Prev Hash:
Nayan -> John Amt: 100
Hash:

Miner A
Status: Idle

Miner B
Status: Idle

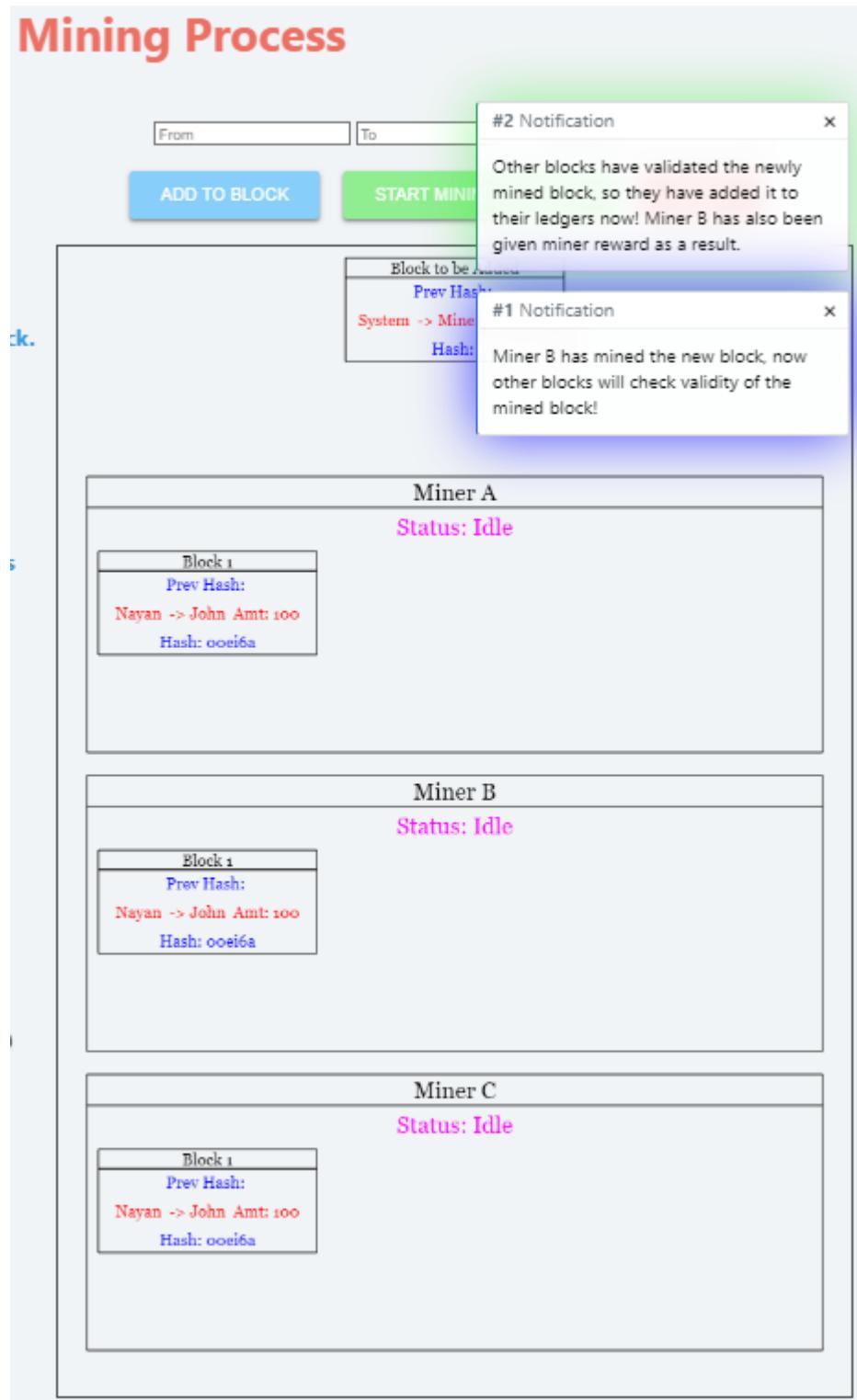
Miner C
Status: Idle

After mining (hash calculated by one of the miners):



Department of Computer Engineering

After mining (block published to all):



Another transaction:

Mining Process

From To

ADD TO BLOCK **START MINING**

Block to be mined
Prev Hash:
System -> Miner C
Hash: ooSPJF

#6 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.

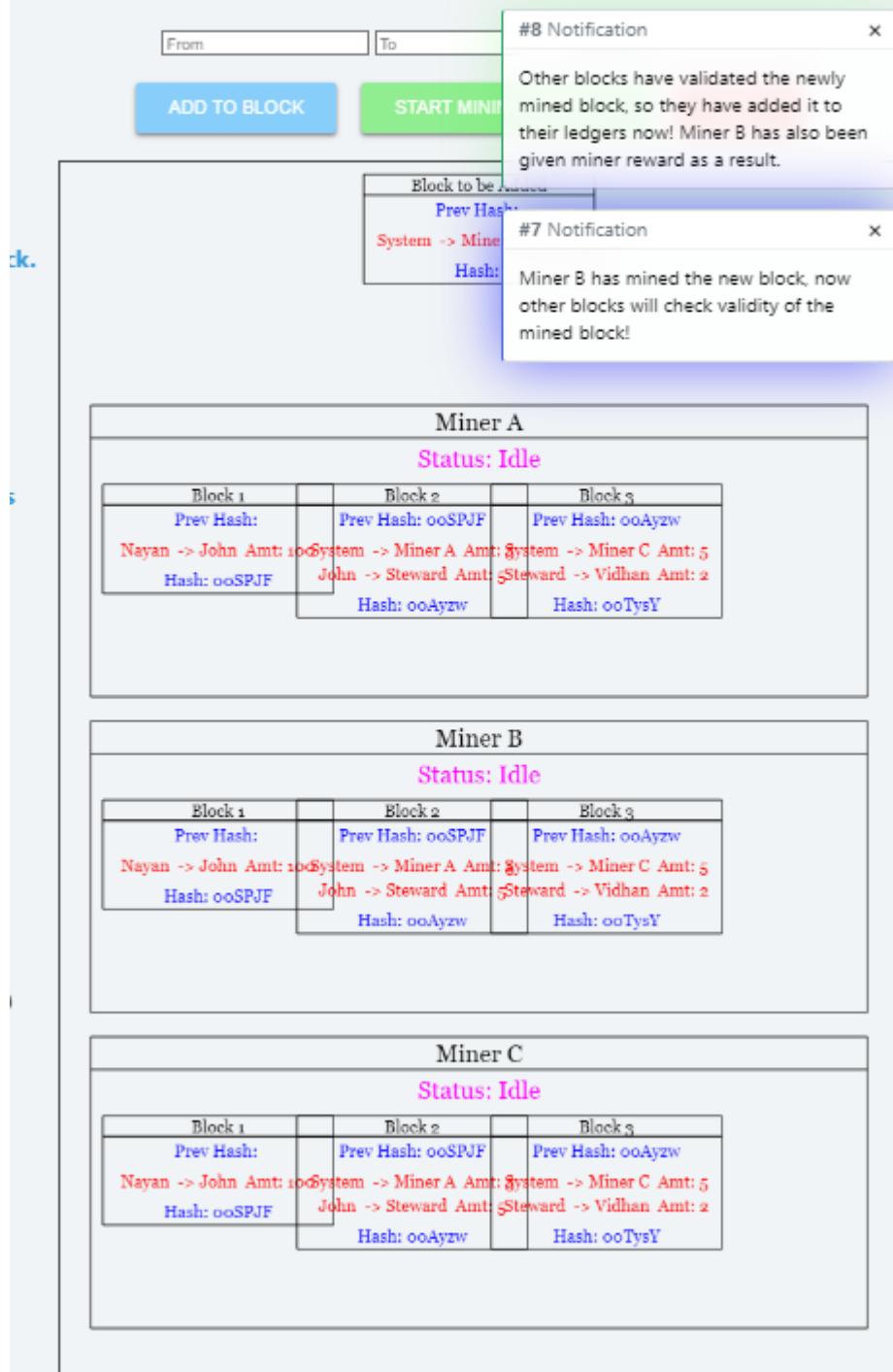
#5 Notification
Miner C has mined the new block, now other blocks will check validity of the mined block!

Miner A	
Status: Idle	
Block 1	Block 2
Prev Hash: ooSPJF Nayan -> John Amt: 10 Hash: ooSPJF	Prev Hash: ooSPJF System -> Miner A Amt: 5 John -> Steward Amt: 5 Hash: ooAyzw

Miner B	
Status: Idle	
Block 1	Block 2
Prev Hash: ooSPJF Nayan -> John Amt: 10 Hash: ooSPJF	Prev Hash: ooSPJF System -> Miner A Amt: 5 John -> Steward Amt: 5 Hash: ooAyzw

Miner C	
Status: Idle	
Block 1	Block 2
Prev Hash: ooSPJF Nayan -> John Amt: 10 Hash: ooSPJF	Prev Hash: ooSPJF System -> Miner A Amt: 5 John -> Steward Amt: 5 Hash: ooAyzw

Mining Process



Department of Computer Engineering

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 decentralization

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)

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.

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

Department of Computer Engineering

Proof of work puzzle:

Construct correct sequence of events for Proof of Work Algorithm

You are given a series of events, construct the correct sequence of events that takes place in Proof of Work Algorithm. Click on the code blocks in the yellow area to add them to grey area(final solution area). Click on validate button on the bottom when you think that you're done.

Final Solution:

A vertical stack of 12 yellow rectangular boxes containing the following text from top to bottom:

- After validation of hash, miners adds the block to their blockchain(ledger)
- One of the nodes(miner) is chosen for validation, known as validator node, based on staked amount by each node.
- One of the miner has found the correct hash.
- The validator node is given a reward.
- Block is ready to be published
- Other Miners validates the hash that was generated by one of the miner.
- Other nodes adds the block validated by validator node in their blockchain
- Miner who found the correct hash, tells it to the other miners.
- Miners starts finding correct hash for the new block(mining).
- Miner who found the correct hash, is given mining reward.
- The chosen node validates the block and tells it to other nodes.

A vertical stack of 8 grey rectangular boxes containing the following text from top to bottom:

- #8 Notification
Block is ready to be published
Correct!
- Miners starts finding correct hash for the new block(mining).
- One of the miner has found the correct hash.
- Miner who found the correct hash, tells it to the other miners.
- Other Miners validates the hash that was generated by one of the miner.
- After validation of hash, miners adds the block to their blockchain(ledger)
- Miner who found the correct hash, is given mining reward.

VALIDATE
HINT

Proof of stake puzzle:

Construct correct sequence of events for Proof of Stake Algorithm

You are given a series of events, construct the correct sequence of events that takes place in Proof of Stake Algorithm. Click on the code blocks in the yellow area to add them to grey area(final solution area). Click on validate button on the bottom when you think that you're done.

Final Solution:

A vertical stack of 12 yellow rectangular boxes containing the following text from top to bottom:

- After validation of hash, miners adds the block to their blockchain(ledger)
- One of the nodes(miner) is chosen for validation, known as validator node, based on staked amount by each node.
- One of the miner has found the correct hash.
- The validator node is given a reward.
- Block is ready to be published
- Other Miners validates the hash that was generated by one of the miner.
- Other nodes adds the block validated by validator node in their blockchain
- Miner who found the correct hash, tells it to the other miners.
- Miners starts finding correct hash for the new block(mining).
- Miner who found the correct hash, is given mining reward.
- The chosen node validates the block and tells it to other nodes.

A vertical stack of 6 grey rectangular boxes containing the following text from top to bottom:

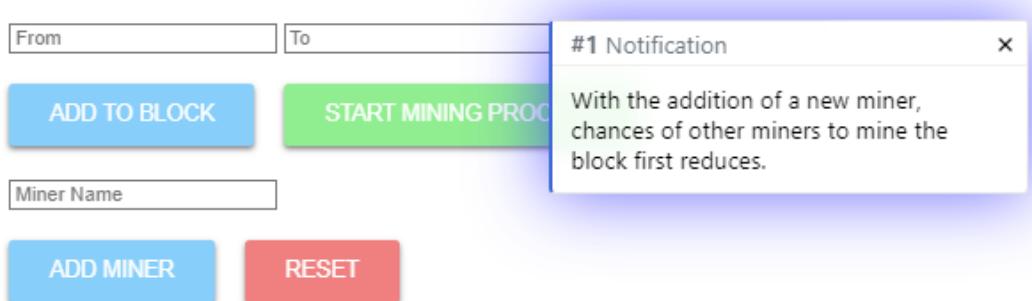
- #1 Notification
Block is ready to be published
Correct!
- One of the nodes(miner) is chosen for validation, known as validator node, based on staked amount by each node.
- The chosen node validates the block and tells it to other nodes.
- Other nodes adds the block validated by validator node in their blockchain
- The validator node is given a reward.

VALIDATE
HINT

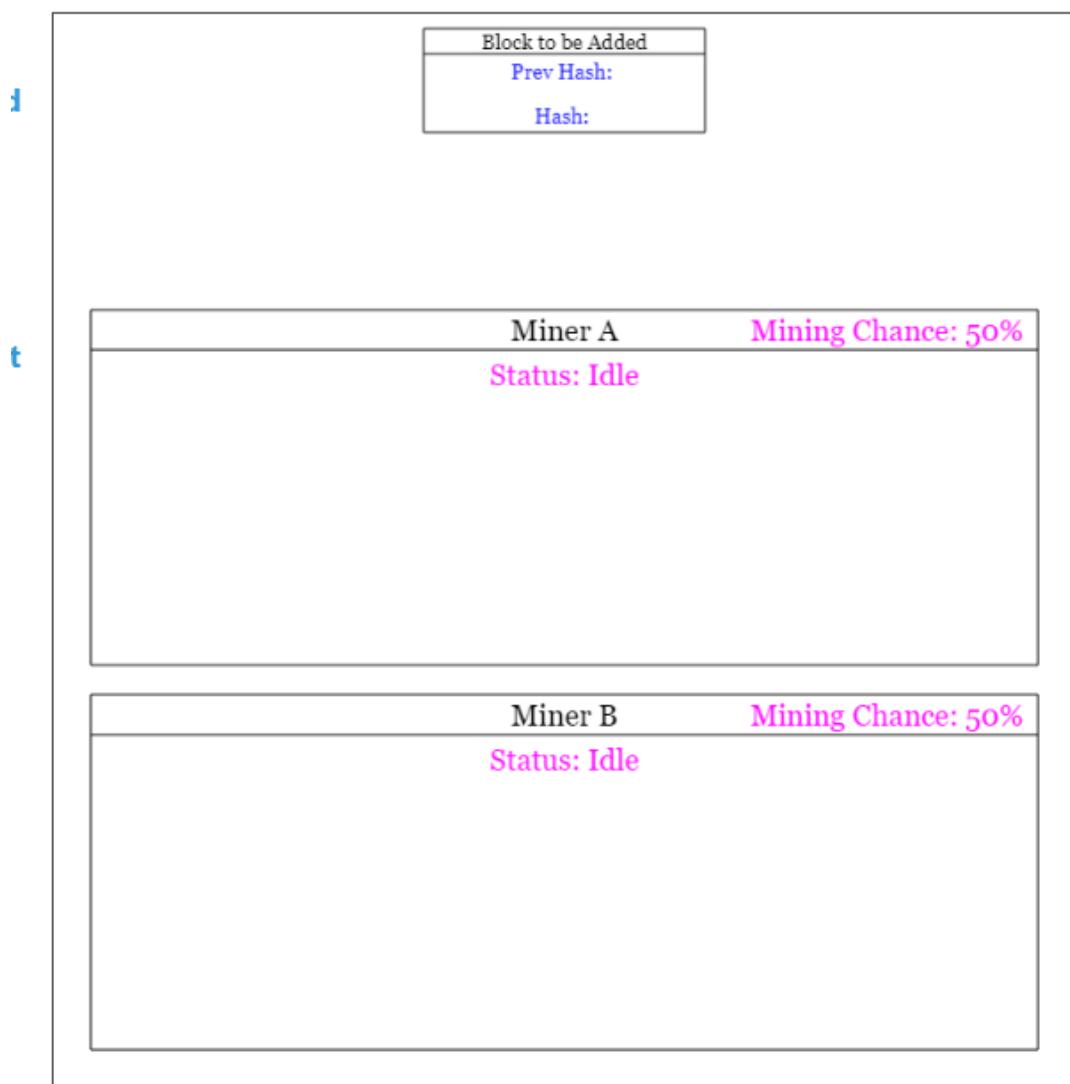
Proof of work activity:

1) Miner B added:

Proof of Work



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



2) New block to be added will be staged and one of the miners will calculate the hash.

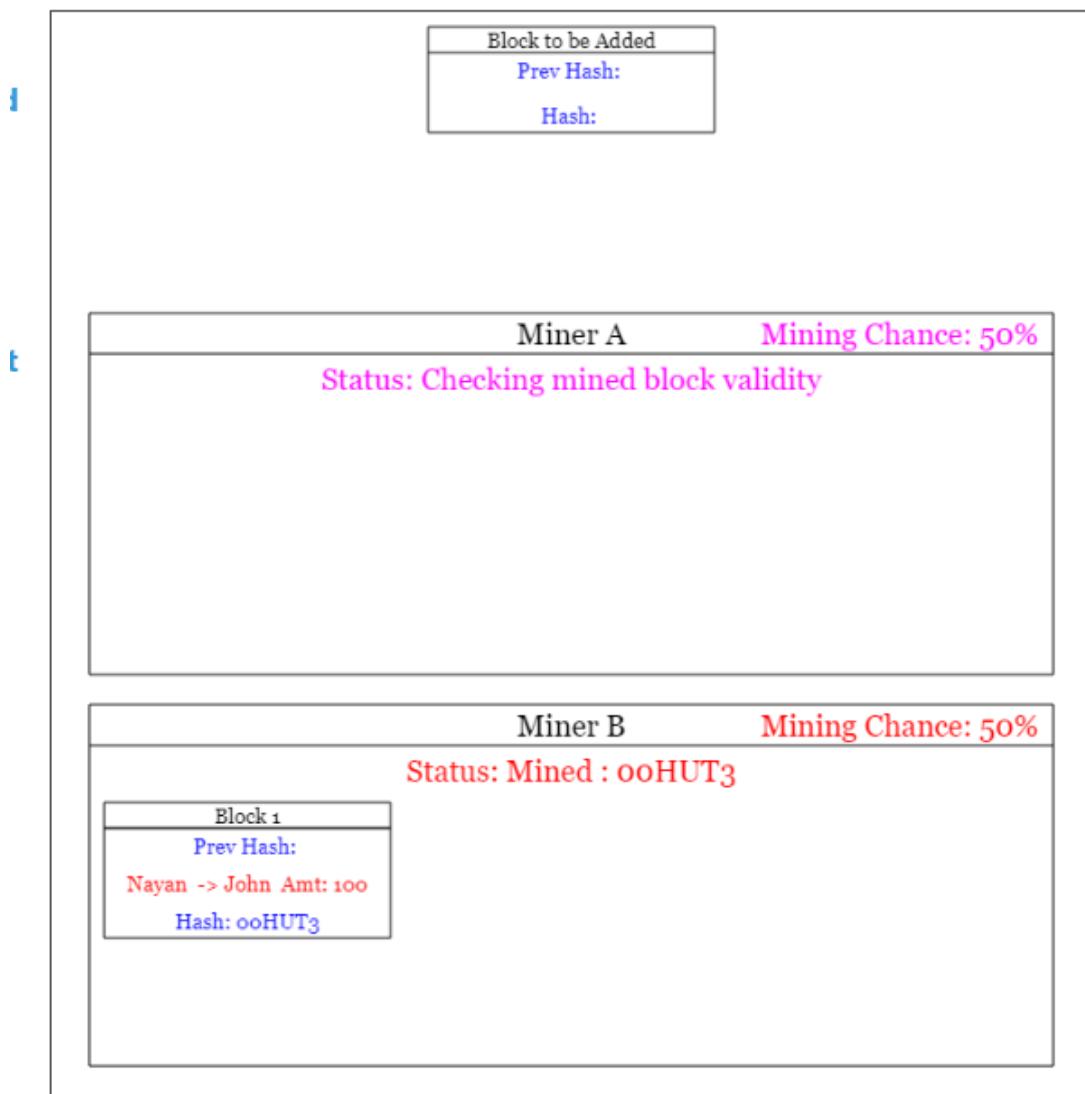
Proof of Work

From	To		
		ADD TO BLOCK	START MINING PROC
Miner Name			
ADD MINER		RESET	

#2 Notification ×

Miner B has mined the new block, now other blocks will check validity of the mined block!

Mining Chance for each miner = $(1 / \text{Total no. of Miners}) \times 100$



3) Block announced to all the miners.

Proof of Work

<input type="text" value="From"/> <input type="text" value="To"/> <div style="display: flex; justify-content: space-around;"> ADD TO BLOCK START MINING PROC </div> <input type="text" value="Miner Name"/> <div style="display: flex; justify-content: space-around;"> ADD MINER RESET </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> #3 Notification × <p>Other blocks have validated the newly mined block, so they have added it to their ledgers now! Miner B has also been given miner reward as a result.</p> </div> <div style="border: 1px solid #ccc; padding: 5px;"> #2 Notification × <p>Miner B has mined the new block, now other blocks will check validity of the mined block!</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Block to be Added</p> <p>Prev Hash: System -> Miner B Amt: 5 Hash:</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Miner A Mining Chance: 50%</p> <p>Status: Idle</p> <p>Block 1</p> <p>Prev Hash: Nayan -> John Amt: 100 Hash: ooHUT3</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Miner B Mining Chance: 50%</p> <p>Status: Idle</p> <p>Block 1</p> <p>Prev Hash: Nayan -> John Amt: 100 Hash: ooHUT3</p> </div>
---	---

4) Another block added.

Proof of Work

From To

ADD TO BLOCK **START MINING PROCESS**

Miner Name

ADD MINER **RESET**

Mining Chance for each miner = (1 / Total Miners)

#5 Notification ×

Other blocks have validated the newly mined block, so they have added it to their ledgers now! Miner B has also been given miner reward as a result.

#4 Notification ×

Miner B has mined the new block, now other blocks will check validity of the mined block!

d

Block to be Added	
Prev Hash:	
System -> Miner B Amt: 5	
Hash:	

it

Miner A		Mining Chance: 50%
Status: Idle		
Block 1	Block 2	
Prev Hash:	Prev Hash: ooHUT3	
Nayan -> John Amt: 10	System -> Miner B Amt: 5	
Hash: ooHUT3	John -> Steward Amt: 5	
	Hash: ooNLI	

Miner B		Mining Chance: 50%
Status: Idle		
Block 1	Block 2	
Prev Hash:	Prev Hash: ooHUT3	
Nayan -> John Amt: 10	System -> Miner B Amt: 5	
Hash: ooHUT3	John -> Steward Amt: 5	
	Hash: ooNLI	

Department of Computer Engineering

Proof of stake activity:

1) Node B added to the chain:

Proof of Stake

From To Amount

ADD TO BLOCK **PUBLISH BLOCK**

Node Name Amount to stake

ADD NODE **RESET**

Block to be Added

Prev Hash:
Hash:

Node A -- Stake Amount: 100

Block A
Prev Hash:
A -> B Amt: 10
B -> C Amt: 20
Hash: oocdefgh

Node B -- Stake Amount: 500

Block A
Prev Hash:
A -> B Amt: 10
B -> C Amt: 20
Hash: oocdefgh

#1 Notification x

With the addition of new node, chances of other nodes to be selected as validator changes depending on staked amount of each node.

Chance of mining a new block: 17%
 Calculations: $(100/600) \times 100 = 17\%$

Chance of mining a new block: 83%
 Calculations: $(500/600) \times 100 = 83\%$

2) New block added (transaction from A to B, amount = 15):

Proof of Stake

From To Amount

ADD TO BLOCK **PUBLISH BLOCK**

Node Name Amount to stake

ADD NODE **RESET**

Block to be Added

Prev Hash:
A -> B Amt: 15
Hash:

Node A -- Stake Amount: 100

Block A
Prev Hash:
A -> B Amt: 10
B -> C Amt: 20
Hash: oocdefgh

Node B -- Stake Amount: 500

Block A
Prev Hash:
A -> B Amt: 10
B -> C Amt: 20
Hash: oocdefgh

#1 Notification x

With the addition of new node, chances of other nodes to be selected as validator changes depending on staked amount of each node.

Chance of mining a new block: 17%
 Calculations: $(100/600) \times 100 = 17\%$

Chance of mining a new block: 83%
 Calculations: $(500/600) \times 100 = 83\%$

Department of Computer Engineering

3) Node A selected as validator node.

Proof of Stake

From To Amount

ADD TO BLOCK PUBLISH BLOCK

Node Name Amount to stake

ADD NODE RESET

#2 Notification ×

Node A has been selected as the validator

Block to be Added

Prev Hash:
A -> B Amt: 10
B -> C Amt: 20
Hash: oocdefgh

Validating Node A -- Stake Amount: 100

Block A

Prev Hash:
A -> B Amt: 10
B -> C Amt: 20
Hash: oocdefgh

Node B -- Stake Amount: 500

Block A

Prev Hash:
A -> B Amt: 10
B -> C Amt: 20
Hash: oocdefgh

Chance of mining a new block: 17%
 Calculations: $(100/600) \times 100 = 17\%$

Chance of mining a new block: 83%
 Calculations: $(500/600) \times 100 = 83\%$

4) Block published to another node.

Proof of Stake

From To Amount

ADD TO BLOCK PUBLISH BLOCK

Node Name Amount to stake

ADD NODE RESET

#3 Notification ×

Node A has now validated the block, it will be added to the ledger. Node A will also be given a validator award as a result.

Block to be Added

Prev Hash:
System -> Node A Amt: 5
Hash: oodS8IRp

Validating Node A -- Stake Amount: 100

Block A

Prev Hash:
A -> B Amt: 10
B -> C Amt: 20
Hash: oocdefgh

Node B -- Stake Amount: 500

Block A

Prev Hash:
A -> B Amt: 10
B -> C Amt: 20
Hash: oocdefgh

Chance of mining a new block: 17%
 Calculations: $(100/600) \times 100 = 17\%$

Chance of mining a new block: 83%
 Calculations: $(500/600) \times 100 = 83\%$

Department of Computer Engineering

5) Another block added to the chain.

Proof of Stake

ADD TO BLOCK
PUBLISH BLOCK

ADD NODE
RESET

#5 Notification

Node B has now validated the block, it will be added to the ledger. Node B will also be given a validator award as a result.

#4 Notification

Node B has been selected as the validator

Block to be Added

Prev Hash:	System -> Node B Amt: 5
Hash:	Hash:

Node A -- Stake Amount: 100

Block A	Block 2	Block 3
Prev Hash: A -> B Amt: 10 B -> C Amt: 20 Hash: oocdefgh	Prev Hash: oodefgh A -> B Amt: 15 Hash: oodS8IRp	Prev Hash: oodSSIRp System -> Node A Amt: 5 B -> C Amt: 7 Hash: oooKwUpR

Chance of mining a new block: 17%

Calculations: $(100/600) \times 100 = 17\%$

Node B -- Stake Amount: 500

Block A	Block 2	Block 3
Prev Hash: A -> B Amt: 10 B -> C Amt: 20 Hash: oocdefgh	Prev Hash: oodefgh A -> B Amt: 15 Hash: oodS8IRp	Prev Hash: oodSSIRp System -> Node A Amt: 5 B -> C Amt: 7 Hash: oooKwUpR

Chance of mining a new block: 83%

Calculations: $(500/600) \times 100 = 83\%$

Difference between proof of work and proof of stake activity:

Move the blocks to the correct section

PoS

PoW

Chances of verification can vary

Chances of verification does not vary

Validation of block is performed

Mining of block is performed

Initial amount is required to start with

VALIDATE
RESET

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

7 out of 7