Batch: A2 Roll No.: 16010121045

Experiment No. 1

Title: Exploring Blockchain

Objective:

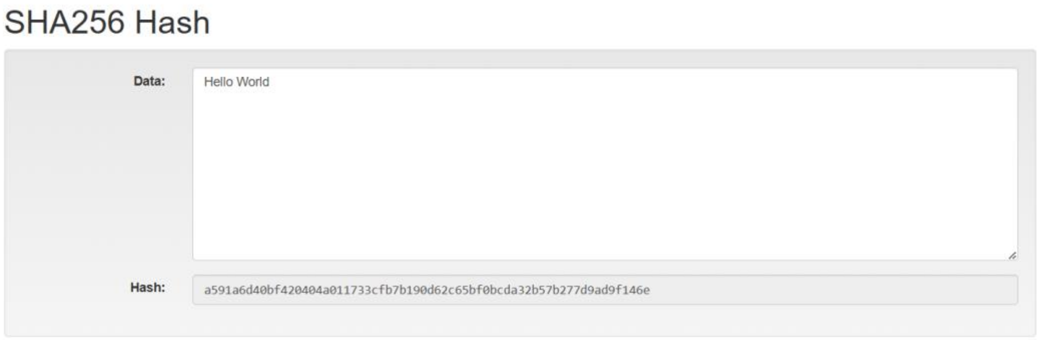
- Learn about blockchain and how it works

Expected Outcome of Experiment:

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

Implementation Details:

1. Enlist all the Steps followed and various options explored

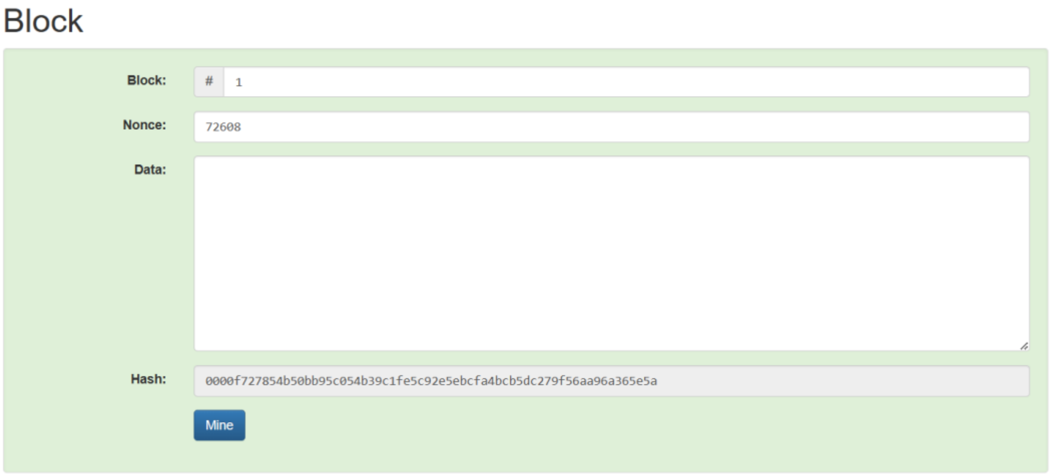


SHA256 Hash

Data: Hello World

Hash: a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

Hash changes when data is changed, the hash function is a mathematical function that is one-way in nature so impractical to reverse the function (i.e. get input from output)



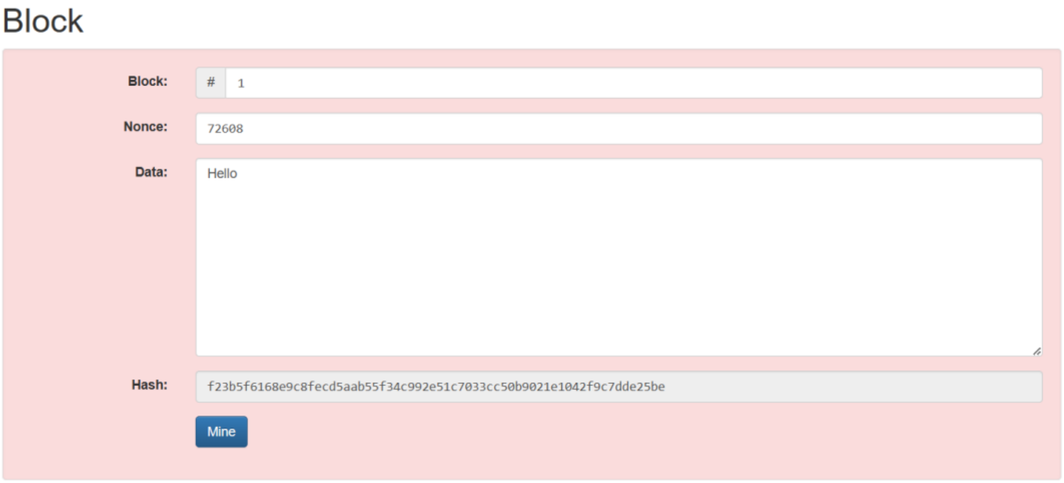
Block

Block: # 1

Nonce: 72608

Data:

Hash: 0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a



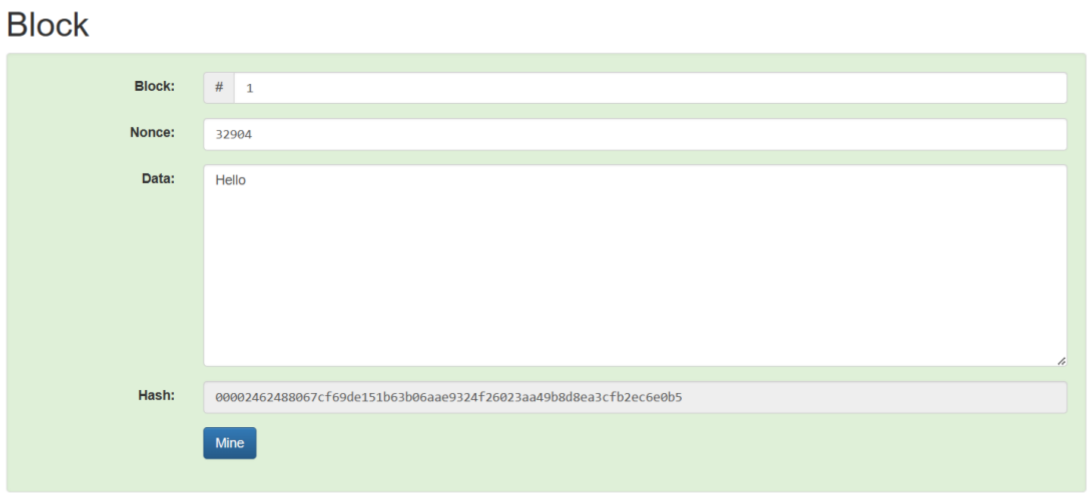
Block

Block: # 1

Nonce: 72608

Data: Hello

Hash: f23b5f6168e9c8fecd5aab55f34c992e51c7033cc50b9021e1042f9c7dde25be



Block

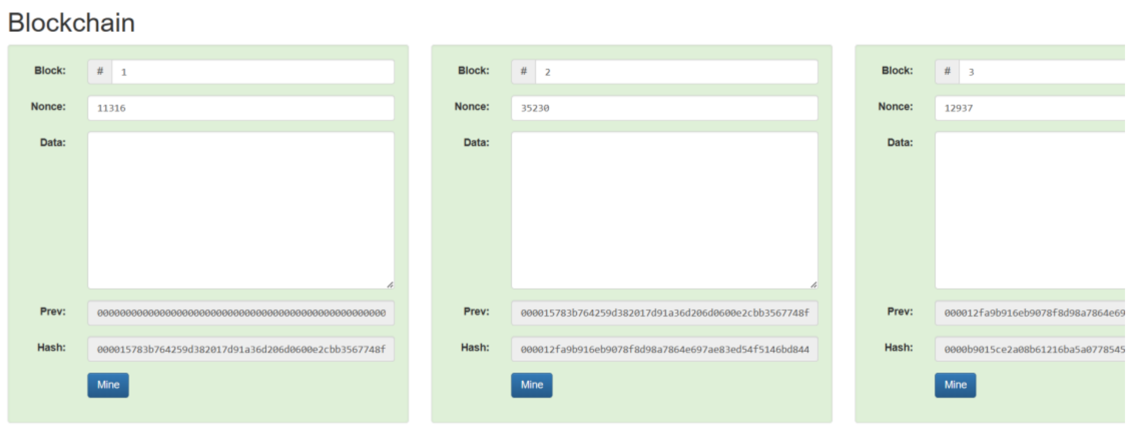
Block: # 1

Nonce: 32904

Data: Hello

Hash: 00002462488067cf69de151b63b06aae9324f26023aa49b8d8ea3cfb2ec6e0b5

We can see that, when data is changed the hash changes and so block is invalid. We can then use the 'Mine' button to mine for a new nonce value that would give us a hash value that lies below the target value (i.e. three zeroes start in this case)

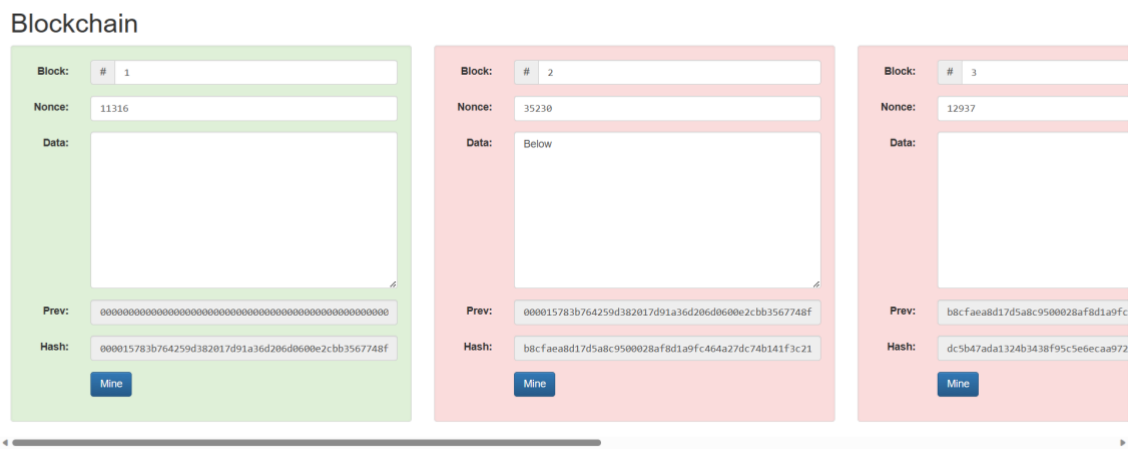


Blockchain

Block: # 1
Nonce: 11316
Data:
Prev: 000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd844

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7864e69
Hash: 0000b9015ce2a08b61216ba5a0778545

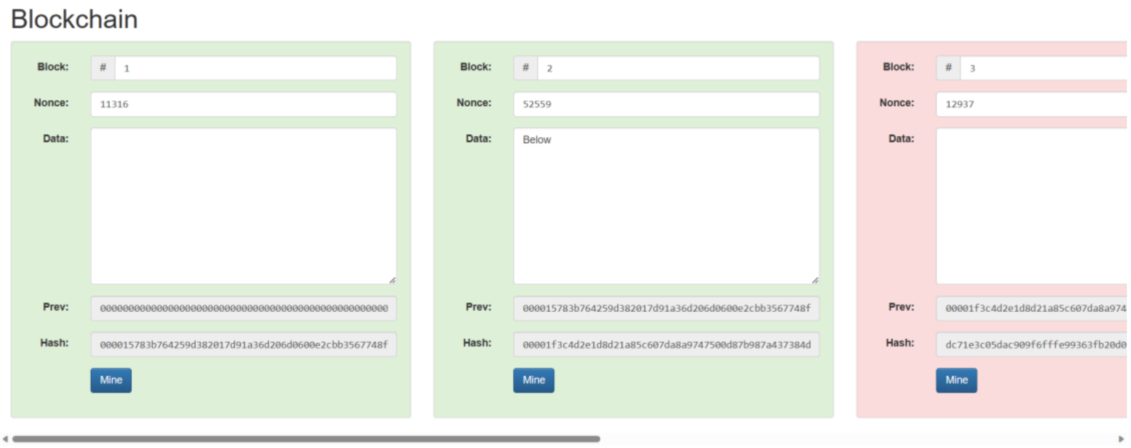


Blockchain

Block: # 1
Nonce: 11316
Data:
Prev: 000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f

Block: # 2
Nonce: 35230
Data: Below
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f
Hash: b8cfaea8d17d5a8c9500028af8d1a9fc464a27dc74b141f3c21

Block: # 3
Nonce: 12937
Data:
Prev: b8cfaea8d17d5a8c9500028af8d1a9fc
Hash: dc5b47ada1324b3438f95c5e6ecaa972



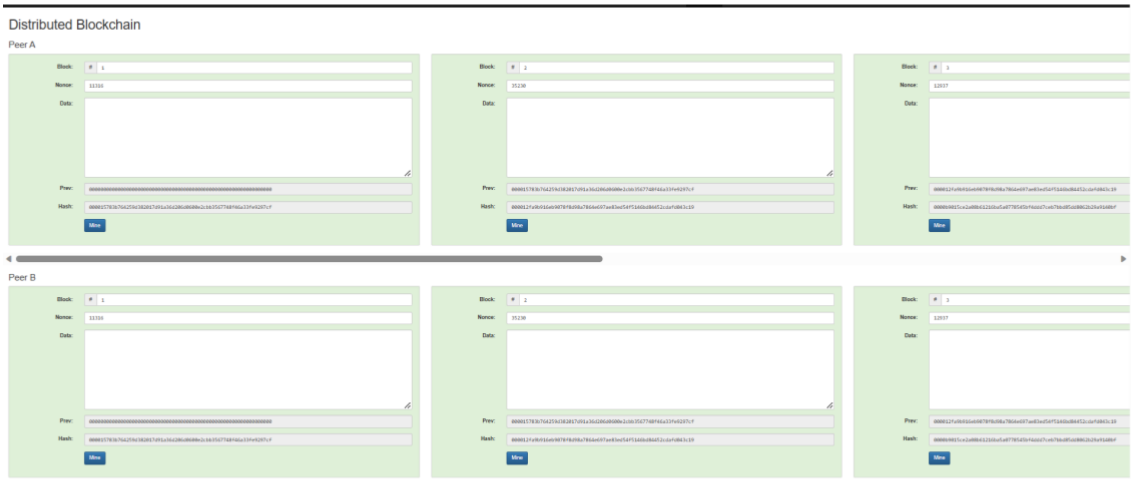
Blockchain

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f

Block: # 2
Nonce: 52559
Data: Below
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f
Hash: 00001f3c4d2e1d8d21a85c607da8a9747500d87b987a437384d

Block: # 3
Nonce: 12937
Data:
Prev: 00001f3c4d2e1d8d21a85c607da8a974
Hash: dc71e3c05dac909f6fffe99363fb20d0

Here, we can see a blockchain, and see how changing the data value of one block makes all the following blocks in the chain invalid (which is the reason blockchains are immutable). We can see that, even after mining that particular block where data was changed, the further blocks are still invalid and will all need to be mined to reach target value and become valid.



Distributed Blockchain

Peer A

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f66a33fe9297cf

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f66a33fe9297cf
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd843c19

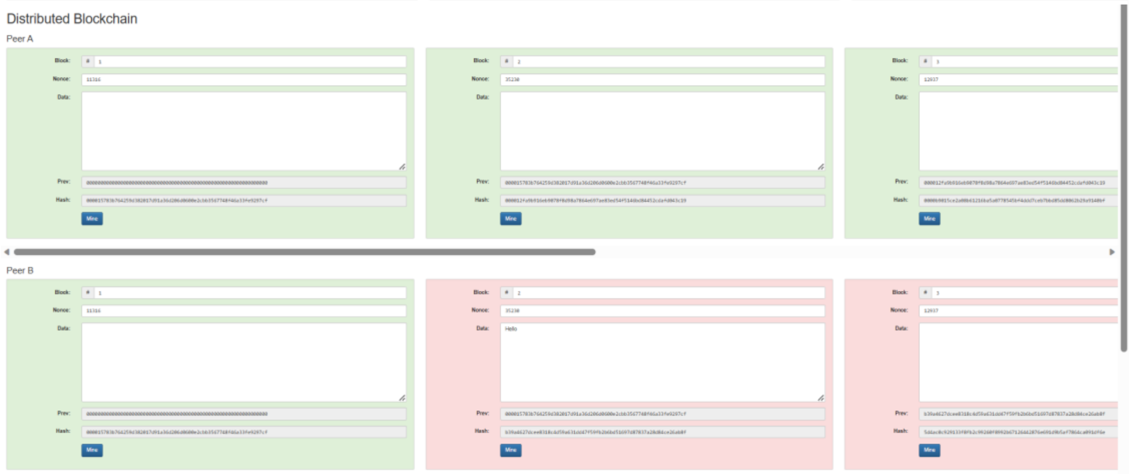
Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd843c19
Hash: 0000b9015ce2a08b61216ba5a0778545bf4ddd7ceb7bbd05dd8062b29a9140bf

Peer B

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f66a33fe9297cf

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f66a33fe9297cf
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd843c19

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd843c19
Hash: 0000b9015ce2a08b61216ba5a0778545bf4ddd7ceb7bbd05dd8062b29a9140bf



Distributed Blockchain

Peer A

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f66a33fe9297cf

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f66a33fe9297cf
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd843c19

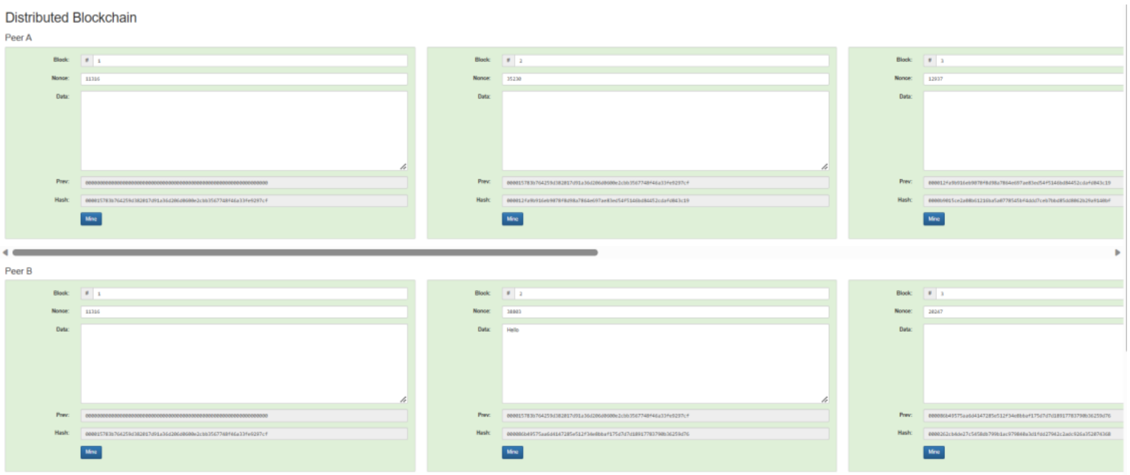
Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd843c19
Hash: 0000b9015ce2a08b61216ba5a0778545bf4ddd7ceb7bbd05dd8062b29a9140bf

Peer B

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f66a33fe9297cf

Block: # 2
Nonce: 35230
Data: Hello
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f66a33fe9297cf
Hash: b39a4627dcee8318c4d59a631ddd7f59fb2b6bd51697d87837a28d84ce26ab8f

Block: # 3
Nonce: 12937
Data:
Prev: b39a4627dcee8318c4d59a631ddd7f59fb2b6bd51697d87837a28d84ce26ab8f
Hash: 5ddac8c929133f8fb2c99260f8992b67126442876e691d9b5af7864ca091df6e



Distributed Blockchain

Peer A

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf
Mine

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf
Hash: 000012fa9b916eb9878f8d98a7864e697ae83ed54f5146bd84452cdafd843c19
Mine

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9878f8d98a7864e697ae83ed54f5146bd84452cdafd843c19
Hash: 0000b9015ce2a00b61216ba5a07785a5b4addd7ceb7bbd85dd0062b29a91a0bf
Mine

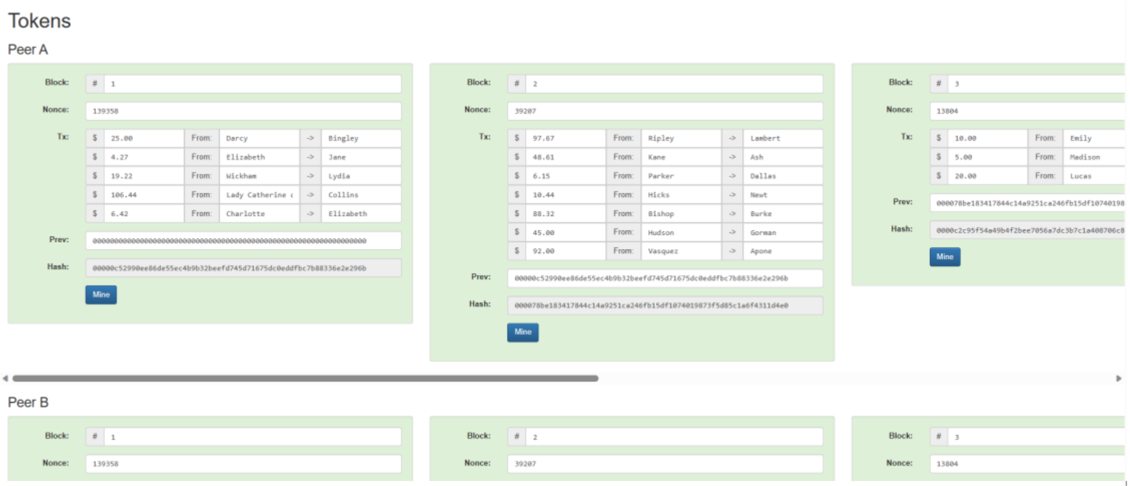
Peer B

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf
Mine

Block: # 2
Nonce: 38803
Data: Hello
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf
Hash: 00008 6b49575aa6d4147285e512f34e8bbaf175d7d7d18917783798b36259d76
Mine

Block: # 3
Nonce: 28247
Data:
Prev: 00008 6b49575aa6d4147285e512f34e8bbaf175d7d7d18917783798b36259d76
Hash: 0000262cb4de27c5458db799b1ac979848a3d1fdd27942c2adc926a3528743
Mine

Here, we can see the example of a distributed blockchain where the same case as before happens. After mining (when changes are done), everything seems to be valid however we can see that nonce and hash values for block 2 onwards are different for Peer A and B, and so this means errors can be caught once the blockchain is decentralised (since it is public and peers can vote which chain they believe is the correct one).



Tokens

Peer A

Block: # 1
Nonce: 139358
Tx:

$	25.00	From:	Darcy	->	Bingley
$	4.27	From:	Elizabeth	->	Jane
$	19.22	From:	Wickham	->	Lydia
$	106.44	From:	Lady Catherine c	->	Collins
$	6.42	From:	Charlotte	->	Elizabeth

Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfbc7b88336e2e296b
Mine

Block: # 2
Nonce: 39207
Tx:

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

Prev: 00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfbc7b88336e2e296b
Hash: 000078be183417844c14a9251ca246fb15df1074019873f5d85c1a6f4311d4e0
Mine

Block: # 3
Nonce: 13804
Tx:

$	10.00	From:	Emily
$	5.00	From:	Madison
$	20.00	From:	Lucas

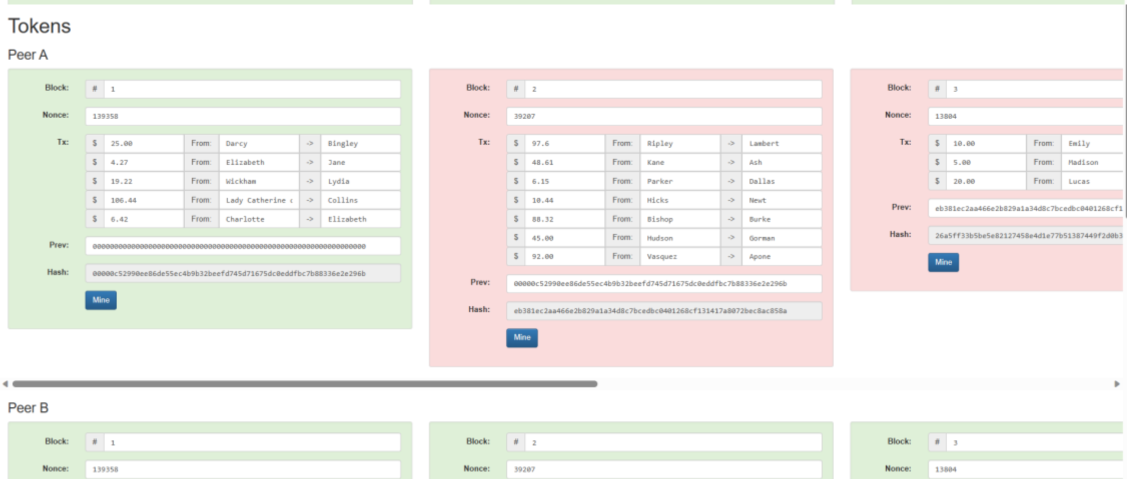
Prev: 000078be183417844c14a9251ca246fb15df10740198
Hash: 0000c2c95f54a49b4f2bee7056a7dc3b7c1a408706c8
Mine

Peer B

Block: # 1
Nonce: 139358

Block: # 2
Nonce: 39207

Block: # 3
Nonce: 13804



Tokens

Peer A

Block: # 1
Nonce: 139358
Tx:

$	25.00	From:	Darcy	->	Bingley
$	4.27	From:	Elizabeth	->	Jane
$	19.22	From:	Wickham	->	Lydia
$	106.44	From:	Lady Catherine c	->	Collins
$	6.42	From:	Charlotte	->	Elizabeth

Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfbc7b88336e2e296b
Mine

Block: # 2
Nonce: 39207
Tx:

$	97.6	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: 00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfbc7b88336e2e296b
Hash: eb381ec2aa466e2b829a1a34d8c7bcedbc0401268cf131417a8072bec8ac858a
Mine

Block: # 3
Nonce: 13804
Tx:

$	10.00	From:	Emily
$	5.00	From:	Madison
$	20.00	From:	Lucas

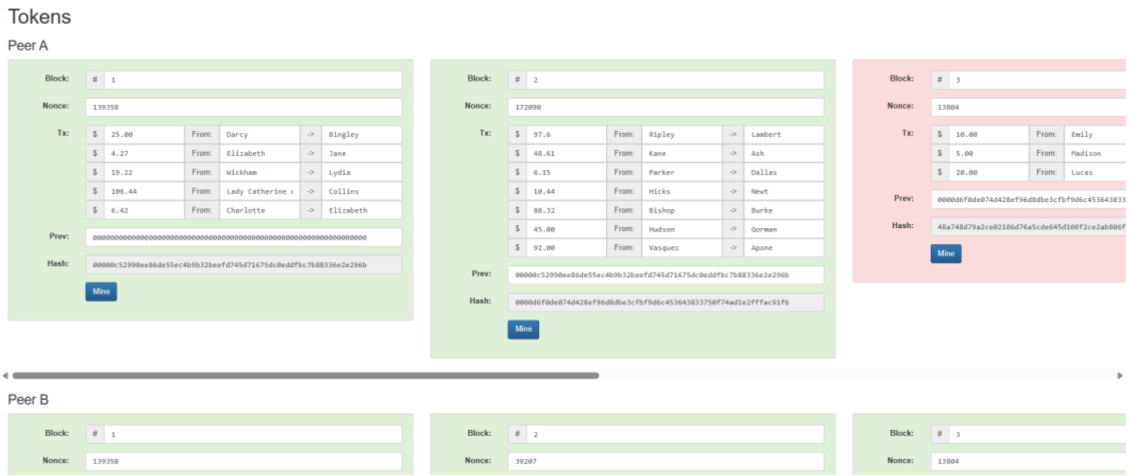
Prev: eb381ec2aa466e2b829a1a34d8c7bcedbc0401268cf1
Hash: 26a5ff33b5be5e82127458e4d1e77b51387449f2d0b3
Mine

Peer B

Block: # 1
Nonce: 139358

Block: # 2
Nonce: 39207

Block: # 3
Nonce: 13804



Tokens

Peer A

Block: # 1
Nonce: 139358
Tx:
$ 25.00 From: Darcy -> Bingley
$ 4.27 From: Elizabeth -> Jane
$ 19.22 From: Wickham -> Lydia
$ 106.44 From: Lady Catherine (-> Collins
$ 6.42 From: Charlotte -> Elizabeth
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfbc7b88336e2e296b

Block: # 2
Nonce: 172090
Tx:
$ 97.6 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: 00000c52990ee86de55ec4b9b32beefd745d71675dc0eddfbc7b88336e2e296b
Hash: 0000d6f0de074d428ef96d8dbe3cfbf9d6c453643833750f74ad1e2fffac91f6

Block: # 3
Nonce: 13804
Tx:
$ 10.00 From: Emily
$ 5.00 From: Madison
$ 20.00 From: Lucas
Prev: 0000d6f0de074d428ef96d8dbe3cfbf9d6c453643833
Hash: 48a748d79a2ce02186d76a5cde645d108f2ce2ab806f

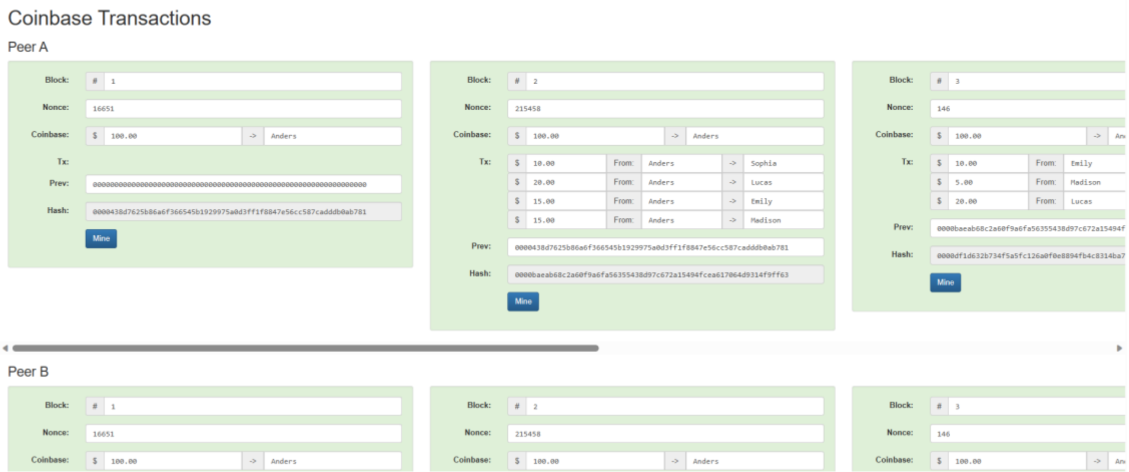
Peer B

Block: # 1
Nonce: 139358

Block: # 2
Nonce: 39207

Block: # 3
Nonce: 13804

This example is of a distributed blockchain as well, just that this one involves transactions (of tokens) data instead of normal textual data in the previous examples. The conditions and immutability features remain the same.



Coinbase Transactions

Peer A

Block: # 1
Nonce: 16651
Coinbase: $ 100.00 -> Anders
Tx:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 0000438d7625b86a6f366545b1929975a0d3ff1f8847e56cc587cadddb0ab781

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: 0000438d7625b86a6f366545b1929975a0d3ff1f8847e56cc587cadddb0ab781
Hash: 0000baeab68c2a60f9a6fa56355438d97c672a15494fcea617064d9314f9ff63

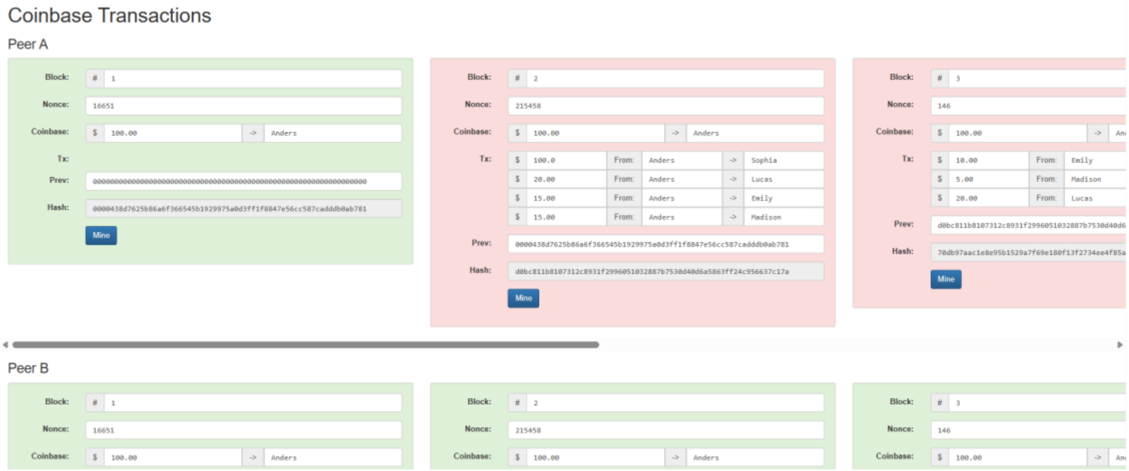
Block: # 3
Nonce: 146
Coinbase: $ 100.00 -> An
Tx:
$ 10.00 From: Emily
$ 5.00 From: Madison
$ 20.00 From: Lucas
Prev: 0000baeab68c2a60f9a6fa56355438d97c672a15494f
Hash: 0000df1d632b734f5a5fc126a0f0e8894fb4c8314ba7

Peer B

Block: # 1
Nonce: 16651
Coinbase: $ 100.00 -> Anders

Block: # 2
Nonce: 215458
Coinbase: $ 100.00 -> Anders

Block: # 3
Nonce: 146
Coinbase: $ 100.00 -> An



Coinbase Transactions

Peer A

Block: # 1
Nonce: 16651
Coinbase: $ 100.00 -> Anders
Tx:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 0000438d7625b86a6f366545b1929975a0d3ff1f8847e56cc587cadddb0ab781

Block: # 2
Nonce: 215458
Coinbase: $ 100.00 -> Anders
Tx:
$ 100.0 From: Anders -> Sophia
$ 20.00 From: Anders -> Lucas
$ 15.00 From: Anders -> Emily
$ 15.00 From: Anders -> Madison
Prev: 0000438d7625b86a6f366545b1929975a0d3ff1f8847e56cc587cadddb0ab781
Hash: d0bc811b8107312c8931f2996051032887b7530d40d6a5863ff24c956637c17a

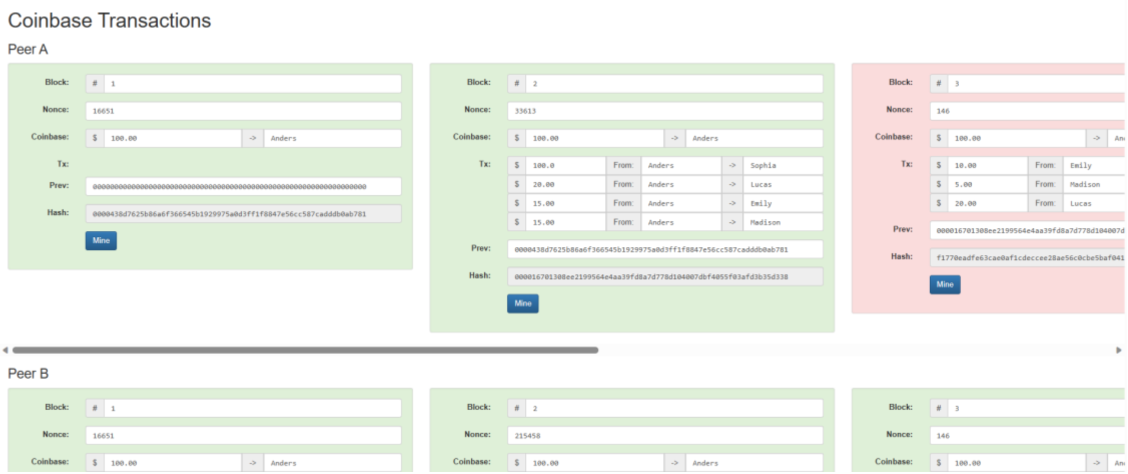
Block: # 3
Nonce: 146
Coinbase: $ 100.00 -> An
Tx:
$ 10.00 From: Emily
$ 5.00 From: Madison
$ 20.00 From: Lucas
Prev: d0bc811b8107312c8931f2996051032887b7530d40d6
Hash: 70db97aac1e8e95b1529a7f69e180f13f2734ee4f85a

Peer B

Block: # 1
Nonce: 16651
Coinbase: $ 100.00 -> Anders

Block: # 2
Nonce: 215458
Coinbase: $ 100.00 -> Anders

Block: # 3
Nonce: 146
Coinbase: $ 100.00 -> An



Coinbase Transactions

Peer A

Block: # 1
Nonce: 16651
Coinbase: $ 100.00 -> Anders
Tx:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 0000438d7625b86a6f366545b1929975a0d3ff1f8847e56cc587cadddb0ab781

Block: # 2
Nonce: 33613
Coinbase: $ 100.00 -> Anders
Tx: $ 100.0 From: Anders -> Sophia
$ 20.00 From: Anders -> Lucas
$ 15.00 From: Anders -> Emily
$ 15.00 From: Anders -> Madison
Prev: 0000438d7625b86a6f366545b1929975a0d3ff1f8847e56cc587cadddb0ab781
Hash: 000016701308ee2199564e4aa39fd8a7d778d104007dbf4055f03afd3b35d338

Block: # 3
Nonce: 146
Coinbase: $ 100.00 -> An
Tx: $ 10.00 From: Emily
$ 5.00 From: Madison
$ 20.00 From: Lucas
Prev: 000016701308ee2199564e4aa39fd8a7d778d104007d
Hash: f1770eadfe63cae0af1cdeccee28ae56c0cbe5baf041

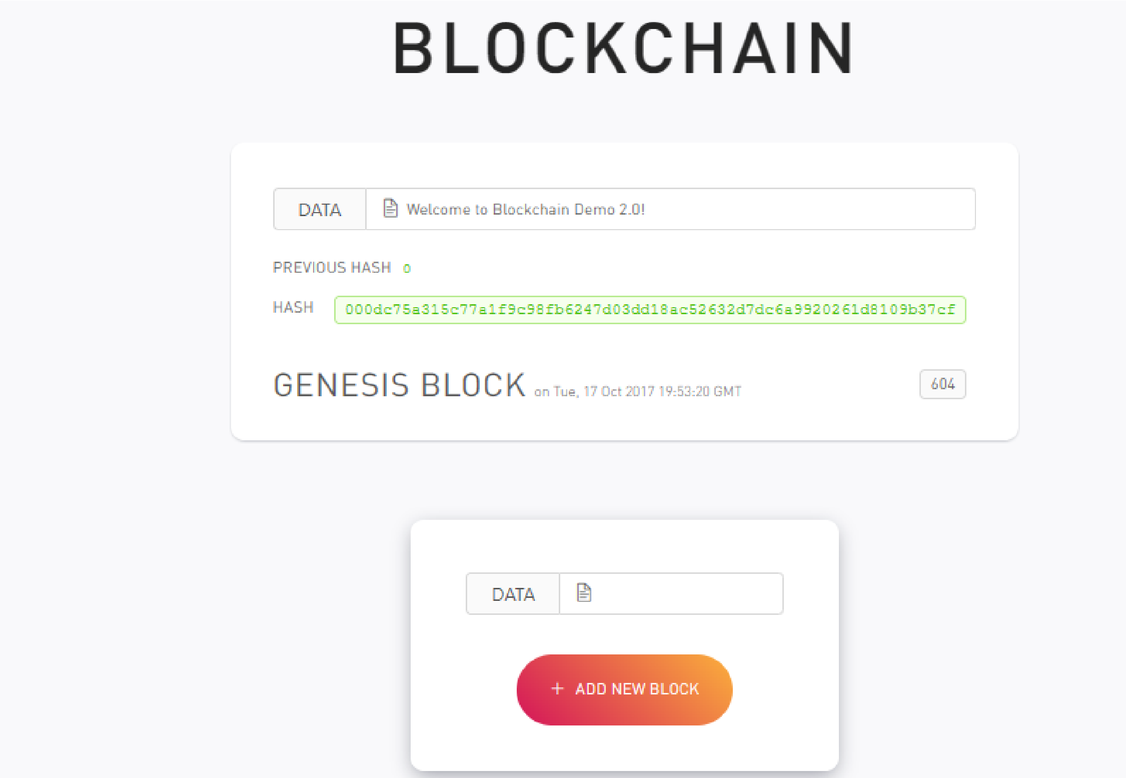
Peer B

Block: # 1
Nonce: 16651
Coinbase: $ 100.00 -> Anders

Block: # 2
Nonce: 215458
Coinbase: $ 100.00 -> Anders

Block: # 3
Nonce: 146
Coinbase: $ 100.00 -> An

This is the same token transactions example, just one that Coinbase uses for example.



BLOCKCHAIN

DATA Welcome to Blockchain Demo 2.0!

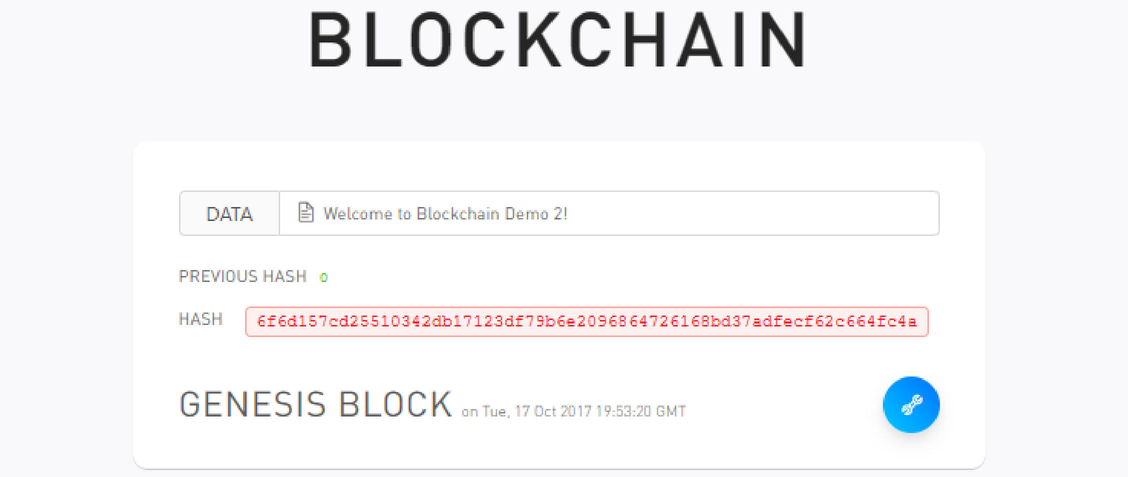
PREVIOUS HASH 0

HASH 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

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

DATA

This is the next blockchain example link.



BLOCKCHAIN

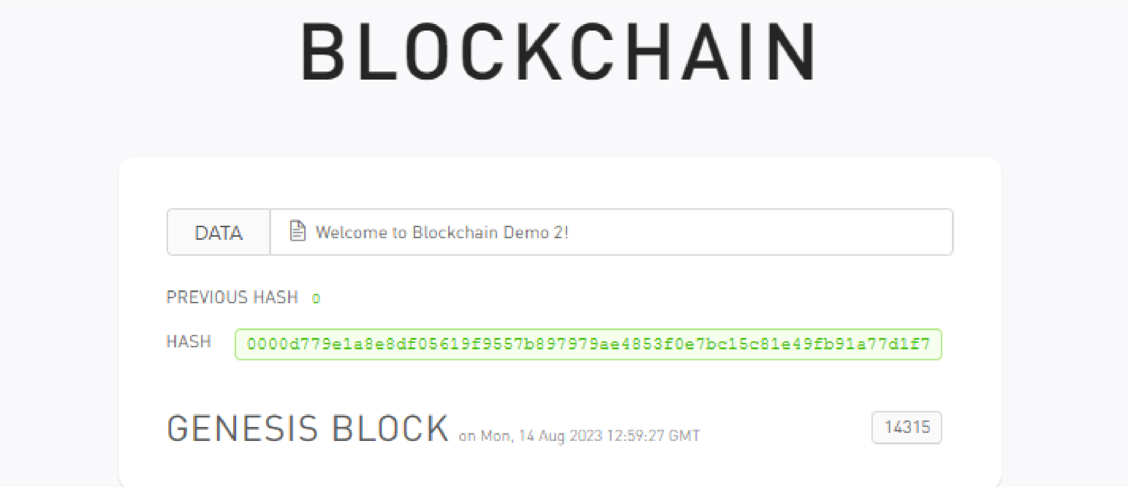
DATA: Welcome to Blockchain Demo 2!

PREVIOUS HASH 0

HASH 6f6d157cd25510342db17123df79b6e2096864726168bd37adfecf62c664fc4a

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

Hash value becomes invalid once the data is changed.



BLOCKCHAIN

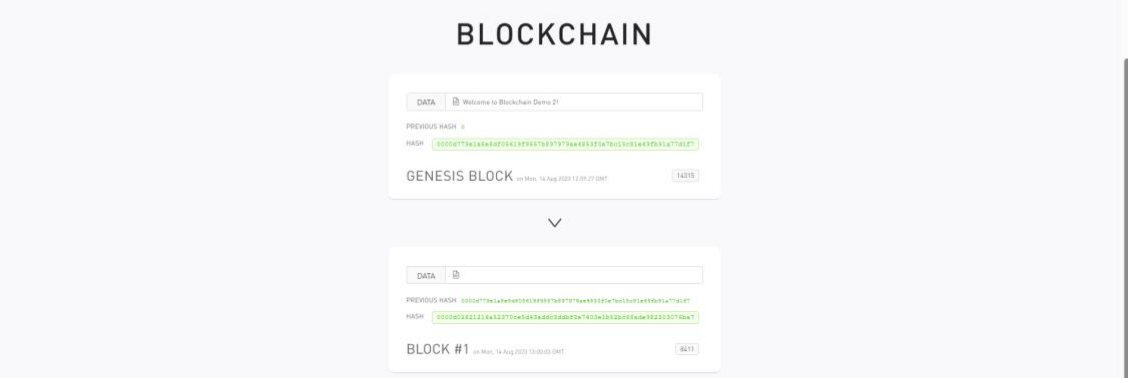
DATA: Welcome to Blockchain Demo 2!

PREVIOUS HASH 0

HASH 0000d779e1a8e8df05619f9557b897979ae4853f0e7bc15c81e49fb91a77d1f7

GENESIS BLOCK on Mon, 14 Aug 2023 12:59:27 GMT 14315

Hash can be made valid by ‘mining’ a new nonce value for the block.



BLOCKCHAIN

DATA: Welcome to Blockchain Demo 2!

PREVIOUS HASH 0

HASH 0000d779e1a8e8df05619f9557b897979ae4853f0e7bc15c81e49fb91a77d1f7

GENESIS BLOCK on Mon, 14 Aug 2023 12:59:27 GMT 14315

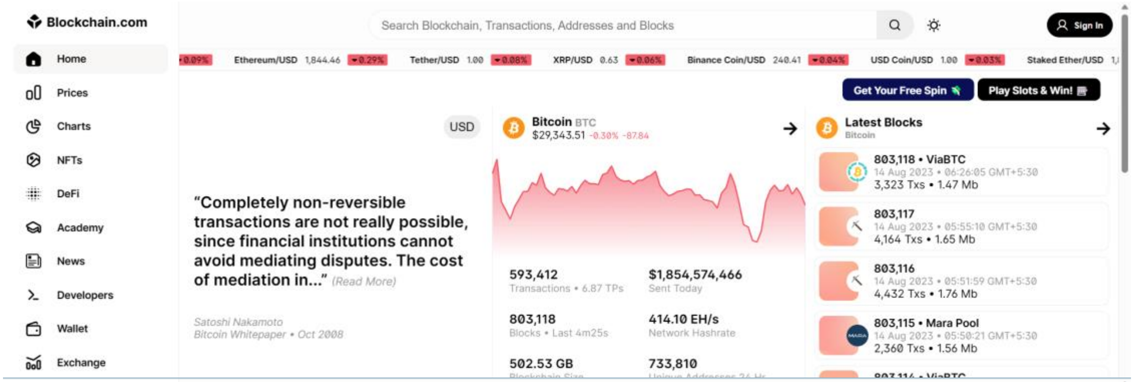
DATA:

PREVIOUS HASH 0000d779e1a8e8df05619f9557b897979ae4853f0e7bc15c81e49fb91a77d1f7

HASH [illegible]

BLOCK #1 on Mon, 14 Aug 2023 13:00:03 GMT 8411

New blocks can be added, and the blockchain can be continued on.



▾0.09% Ethereum/USD 1,844.46 ▾0.29% Tether/USD 1.00 ▾0.08% XRP/USD 0.63 ▾0.06% Binance Coin/USD 240.41 ▾0.04% USD Coin/USD 1.00 ▾0.03% Staked Ether/USD 1,

"Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation in..." *(Read More)*

Satoshi Nakamoto
Bitcoin Whitepaper • Oct 2008

Bitcoin BTC
$29,343.51 -0.30% -87.84

593,412
Transactions • 6.87 TPs

$1,854,574,466
Sent Today

803,118
Blocks • Last 4m25s

414.10 EH/s
Network Hashrate

502.53 GB

733,810

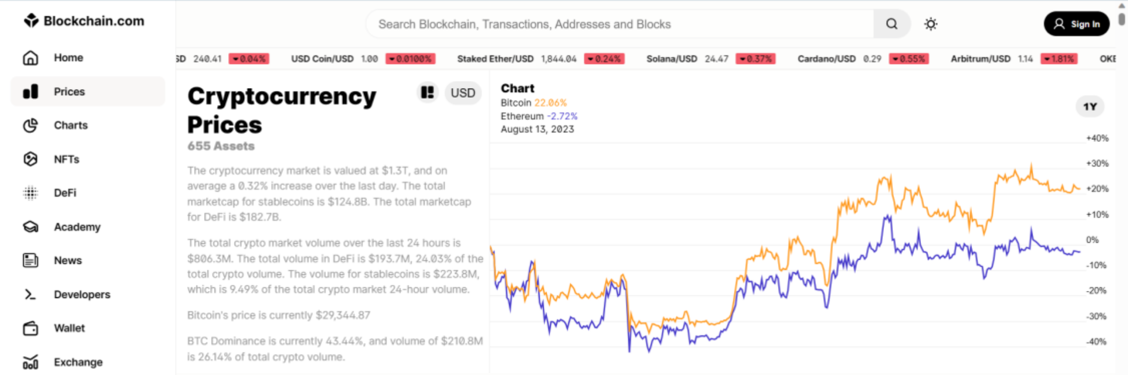
Latest Blocks
Bitcoin

803,118 • ViaBTC
14 Aug 2023 • 06:26:05 GMT+5:30
3,323 Txs • 1.47 Mb

803,117
14 Aug 2023 • 05:55:10 GMT+5:30
4,164 Txs • 1.65 Mb

803,116
14 Aug 2023 • 05:51:59 GMT+5:30
4,432 Txs • 1.76 Mb

803,115 • Mara Pool
14 Aug 2023 • 05:50:21 GMT+5:30
2,360 Txs • 1.56 Mb



SD 240.41 ▾0.04% USD Coin/USD 1.00 ▾0.0100% Staked Ether/USD 1,844.04 ▾0.24% Solana/USD 24.47 ▾0.37% Cardano/USD 0.29 ▾0.55% Arbitrum/USD 1.14 ▾1.81% OKE

Cryptocurrency Prices
655 Assets

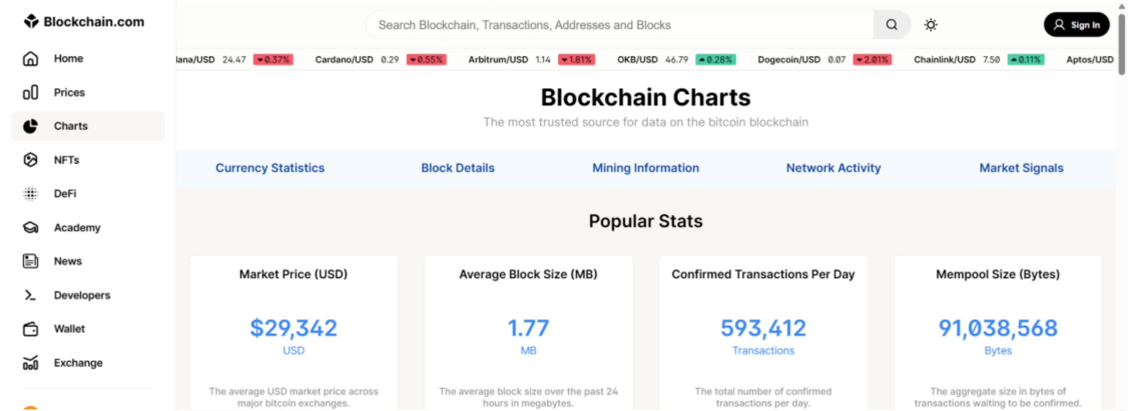
The cryptocurrency market is valued at $1.3T, and on average a 0.32% increase over the last day. The total marketcap for stablecoins is $124.8B. The total marketcap for DeFi is $182.7B.

The total crypto market volume over the last 24 hours is $806.3M. The total volume in DeFi is $193.7M, 24.03% of the total crypto volume. The volume for stablecoins is $223.8M, which is 9.49% of the total crypto market 24-hour volume.

Bitcoin's price is currently $29,344.87

BTC Dominance is currently 43.44%, and volume of $210.8M is 26.14% of total crypto volume.

Chart
Bitcoin 22.06%
Ethereum -2.72%
August 13, 2023

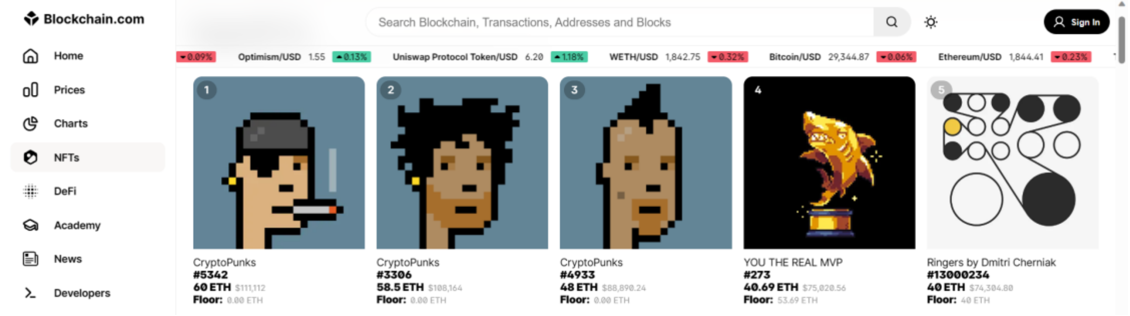


lana/USD 24.47 ▾0.37% Cardano/USD 0.29 ▾0.55% Arbitrum/USD 1.14 ▾1.81% OKB/USD 46.79 ▴0.28% Dogecoin/USD 0.07 ▾2.01% Chainlink/USD 7.50 ▴0.11% Aptos/USD

Blockchain Charts
The most trusted source for data on the bitcoin blockchain

Popular Stats

Market Price (USD)	Average Block Size (MB)	Confirmed Transactions Per Day	Mempool Size (Bytes)
$29,342 USD	1.77 MB	593,412 Transactions	91,038,568 Bytes
The average USD market price across major bitcoin exchanges.	The average block size over the past 24 hours in megabytes.	The total number of confirmed transactions per day.	The aggregate size in bytes of transactions waiting to be confirmed.



▾0.09% Optimism/USD 1.55 ▴0.13% Uniswap Protocol Token/USD 6.20 ▴1.18% WETH/USD 1,842.75 ▾0.32% Bitcoin/USD 29,344.87 ▾0.06% Ethereum/USD 1,844.41 ▾0.23%

CryptoPunks	CryptoPunks	CryptoPunks	YOU THE REAL MVP	Ringers by Dmitri Cherniak
#5342	#3306	#4933	#273	#13000234
60 ETH $111,112	58.5 ETH $108,164	48 ETH $88,890.24	40.69 ETH $75,020.56	40 ETH $74,304.80
Floor: 0.00 ETH	Floor: 0.00 ETH	Floor: 0.00 ETH	Floor: 53.69 ETH	Floor: 40 ETH

These are some screenshots from blockchain.com/explorer/
The website displays cryptocurrency prices, popular NFTs, and other important statistics related to the known blockchain systems.

Conclusion:-

In this experiment, we learnt about blockchains, cryptocurrencies, how blockchains work, their features and their use-cases.