

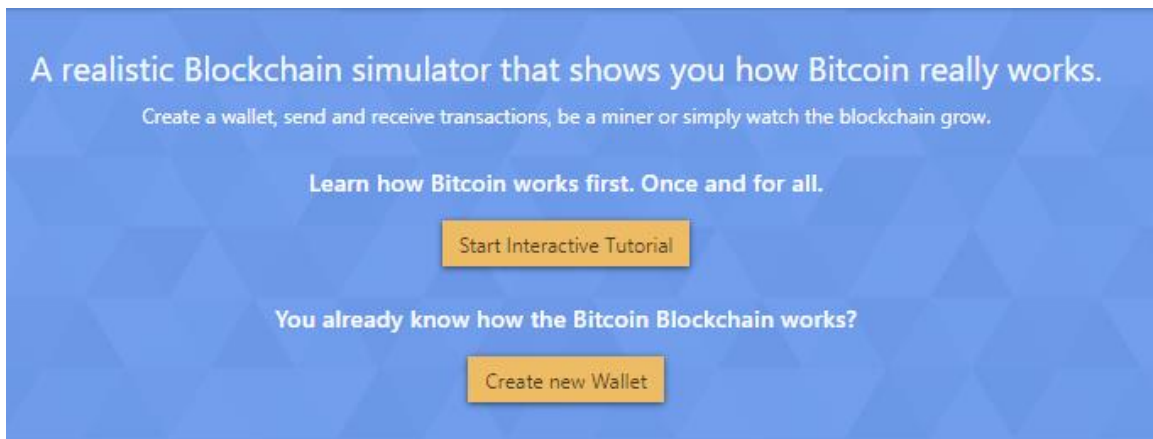
Activity: Blockchain Simulator

In this exercise you will be running a simulator to create private group chain for a group. Select a group to join, and all the members will share a private group that is only accessible for group members.


Follow the instructions below:

Open the website at: <https://www.bitcoinsimulator.tk/blockchain?chain=public>

Creating Wallet



Click Create a new Wallet.

Connected to **Public** Blockchain  **Switch**

Generate new Wallet

A random pair of keys (256 bit) will be generated. For simplicity, you can enter a unique username linked to your public key.

Username

Load existing Wallet

Enter your private key to retrieve an existing wallet.

Private Key

Enter a Username and it will generate a private key for your wallet.

Activity: Blockchain simulation.

joey's Wallet

The private key is a 256bit random number. The public key was calculated using Elliptic Curve Cryptography.

Public Key

946318a6975429259c1fad5fb671beaf00e37349974d0a1fdc6b9e9555c99

Private Key

268aa989984a838e142fa1add04183b81389dccc17d1e2a4be9bf8d85b2f9da0

Caution: Keep your private key in a secure place. Don't share it with anyone. If you lose this key, all your Bitcoin (in this simulation) are permanently lost. For simplicity, this key is stored in the local storage of your Browser, so you don't have to reenter it every time you reload the page.

What you can do now:

- Mine a block to receive your first Bitcoin as a reward
- Sign transactions and send Bitcoin to other wallets
- Create your own private blockchain and use the simulator with non-public groups or school classes
- Create fake transactions under a false name and try to obtain Bitcoin by fraud
- Perform a 51% attack to subsequently manipulate the blockchain
- Tell other people about it. The more understand how Bitcoin works, the better.

Got it

Click **Got it**. You will be connected to a **public blockchain**

Blockchain

Block Mining

New Transaction

Block 922

7/3/21 18:31:17

Miner: gfdgfdgdfgd

Set as 'Last Block'
(only if you know what you do)

longest chain

1 Transaction

New

Block Reward

→

gfdgfdgdfgd

89da9dc418...

6.25

BTC

Hash of the previous Block

00005efb02303b4d03949218ee8d0ace0cfe88de48ebf19b5ac60979919b7f

Nonce: 33933

Hash

00008254a2ac4b9ef32ef751b83bd72f22d66c4115eb32052f212685746b2fd1

Block 923

9/3/21 22:12:45

Miner: prueba

Mining based on this Block

longest chain

1 Transaction

New

Block Reward

→

prueba

730ca0f479...

6.25

BTC


Hash of the previous Block

00008254a2ac4b9ef32ef751b83bd72f22d66c4115eb32052f212685746b2fd1

Nonce: 12

Hash

000006802ba82d68ac5c1914cf97049761943024c8329346327d4bf22ea19e0e

Connected to **Public** Blockchain  Switch

Blockchain

Block Mining

New Transaction


Block 923 9/3/21 22:12:45

Miner: prueba

Mining based on this Block

longest chain

1 Transaction

New		prueba	6.25
Block Reward		730ca0f479...	BTC

Hash of the previous Block

00008254a2ac4b9ef32ef751b83bd72f22d66c4115eb32052f212685746b2fd1

Nonce: 12

Hash

000006802ba82d68ac5c1914cf97049761943024c8329346327d4bf22ea19e0e

Creating Private Blockchain

Click **Switch**. So that you can create a private blockchain.

IMPORTANT: Only of your group members will create this private blockchain. So let only one create first, then the rest follow by typing the same name after it has been created!!

Switch Blockchain

Connect to an existing blockchain or start a new one

Enter the name of the blockchain you want to connect to. If it doesn't exist you can create a new one. You will then be able to interact with all computers that are connected to the blockchain with the same name.

[Connect to Public Blockchain](#)[Connect](#)

After creating a private blockchain and joining, you will see: (depends on your blockchain name)

Connected to **ntust** Blockchain [Switch](#)

[Blockchain](#)[Block Mining](#)[New Transaction](#)

Mining Coins

Click on Mining: Auto Mining

The mining operations looks at hashing operations that results in a number of zeroes in front of the hash digest.

So the mining operation is going by brute force testing all the nonce (random number) with the transactions that will generate the hash with the correct number of zeros.

Each time you succeed, you will earn a coin. This is called **mining**.

The mempool stores the current transactions that has yet to be validated and included into the blockchain.

Activity: Blockchain simulation.

Block 3

building on joey's Block 2

Hash of the previous Block

000ed96d4d8af4e6f05c428d03ca5c4e907502e23ec0e4722b591232f39604f2

Transactions

Sender	Receiver	Amount
new	joey	10
Block Reward	946318a6975429259c...	BTC

Although it's perfectly fine to start mining a block that solely contains your reward transaction, you may want to consider adding pending transactions from the Mempool below. The more transactions you include in your block, the more transaction fees you can collect in addition to your block reward.

Mining: Calculate the Hash of this Block.

The hash of a block is calculated from the included transactions, the hash of the previous block, the current time and a random number (Nonce). Find a number such that the Hash of this block starts with 3 zeros.

Start Mining by typing random numbers...

☐ Auto Mining

Sit back and let the Computer do the work. This can take a while depending on how lucky you are. Average number of tries: 4096 Nonces

Sending Coin and Creating a new transaction

Click on New Transaction

New Transaction

Send Bitcoin to another wallet in this simulated network.

joey

946318a697...

Change

→

Recipient name

BTC

Sign Transaction

Observe what happens to the mempool on your computer and on your group members mempool.

Some Questions

What is the purpose of the mempool?

When is the transaction added to the blockchain?

What is the real purpose of mining? Why do we need it?

Why do we use the hash puzzle for mining?

How do we ensure all the copies of blockchain are the same?

How do we ensure that each block has the same transactions?