BlockChainED

BlockChainED

An educational project that teaches the core principles and algorithms of blockchain through establishing a real-time blockchain

Submitted By:

Nusrat Jahan Lia

BSSE-1306

Institute of Information Technology ,
University of Dhaka

Supervised By:

Dr. Ahmedul Kabir

Associate Professor

Institute of Information Technology ,
University of Dhaka

WHY BLOCKCHAIN?

Distributed Ledger

Cryptographic tracsaction

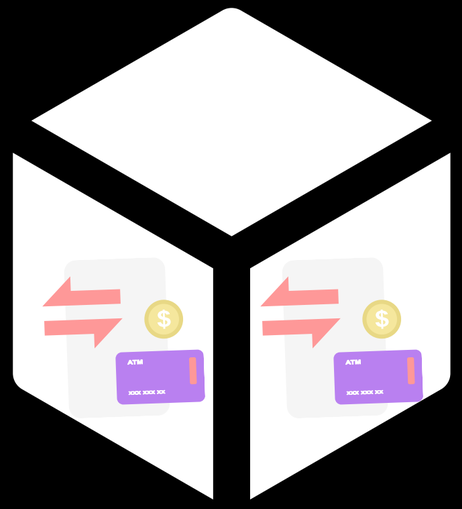
Not trust Based

Transparency and Security

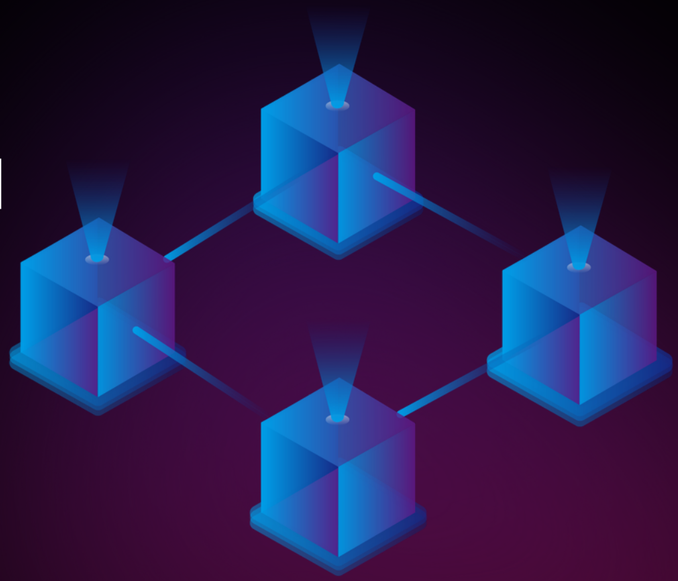
Immutable record

FUNCTIONALITIES

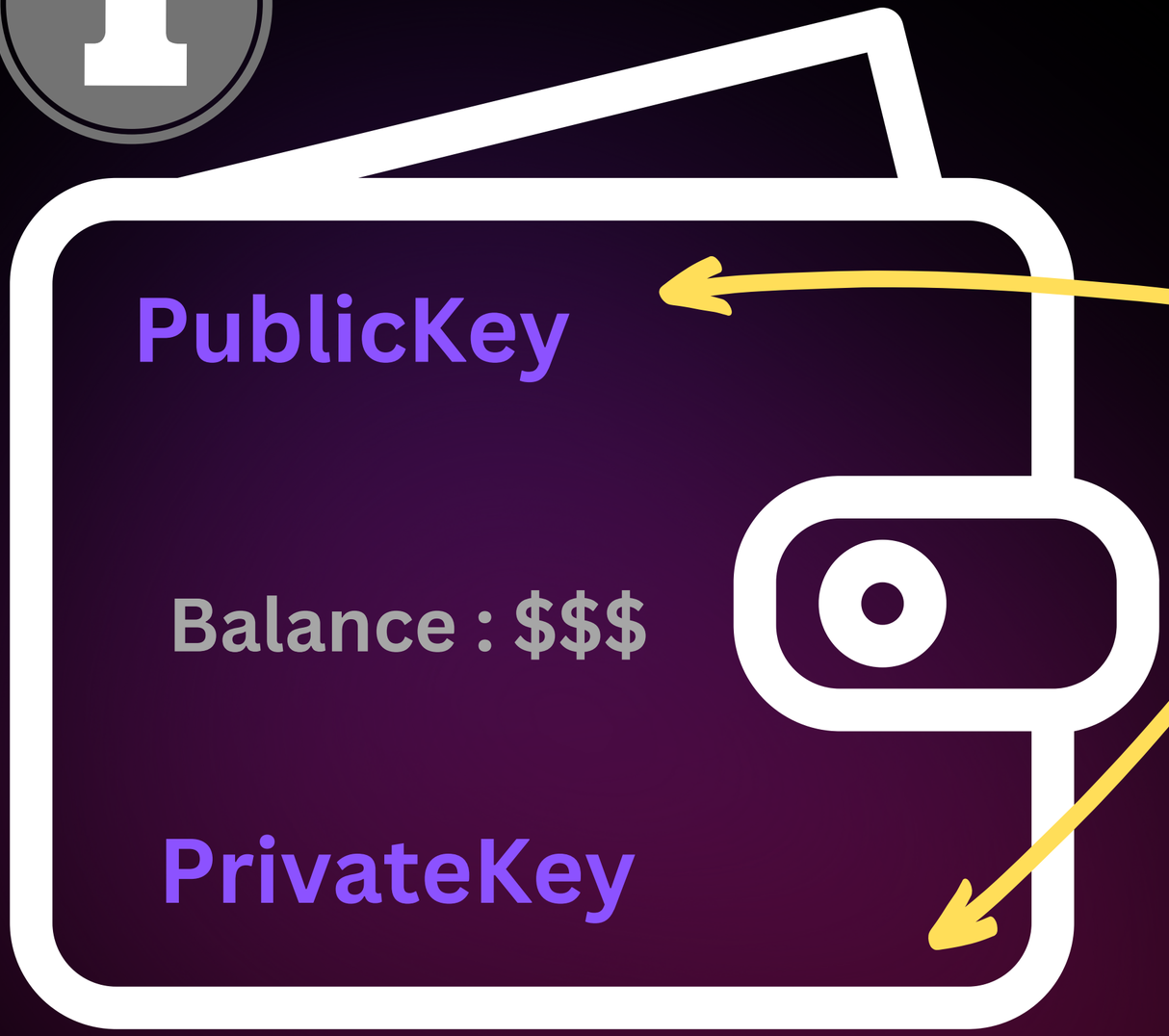
Transaction

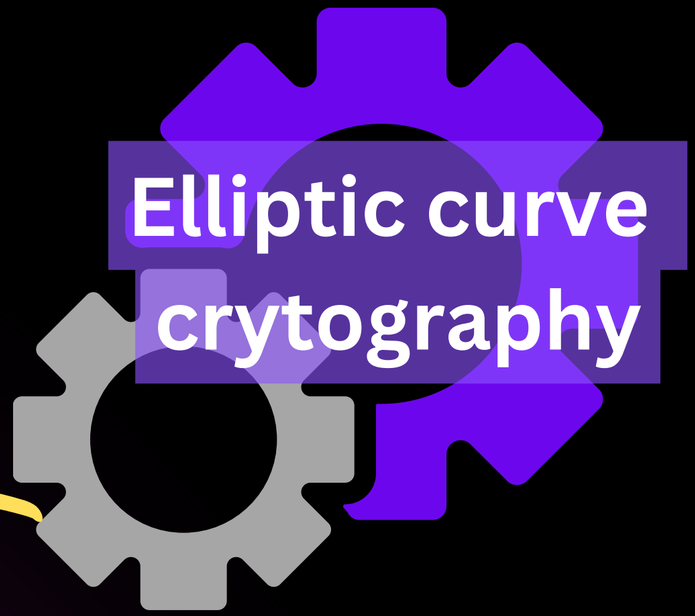


Block Mined

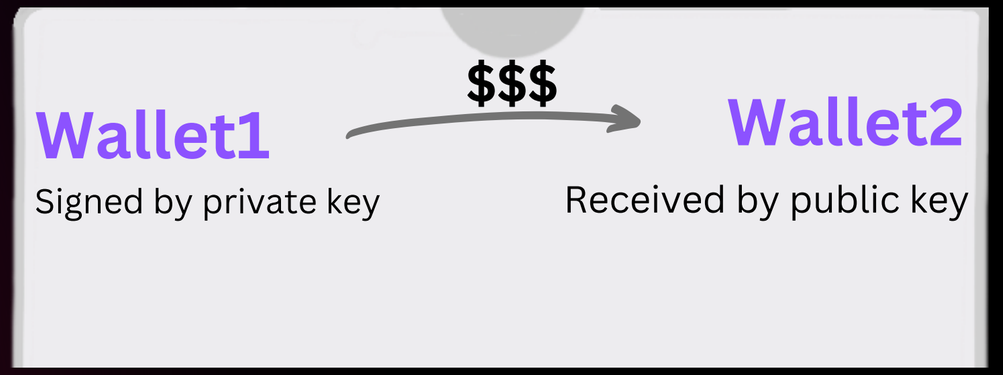


1





TRANSACTION



2

Transaction 1

Transaction 2

Transaction 3

Collects Transactions into block

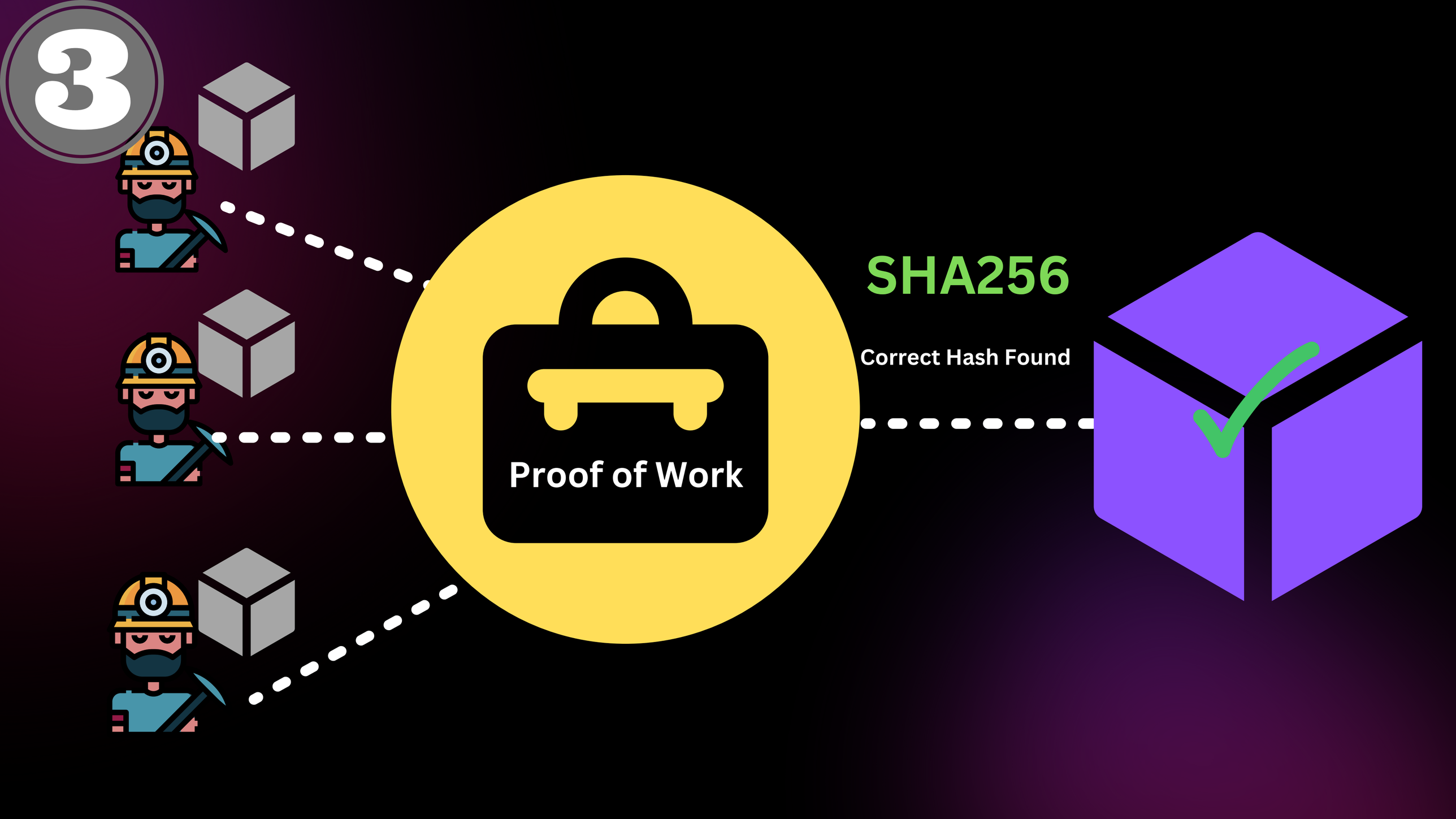
Previous BlockHash

Transaction 1

Transaction 3

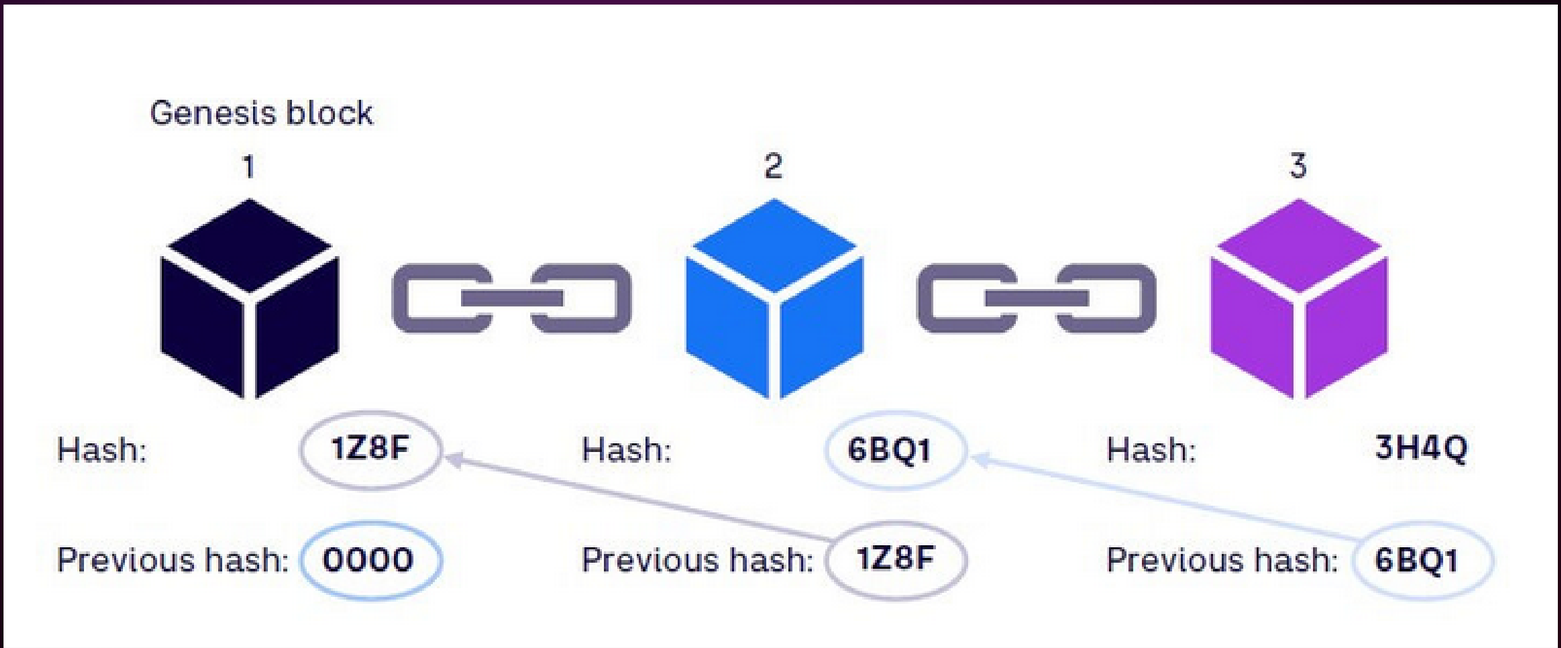
Miner

Verifies Transaction


3
Proof of Work
SHA256
Correct Hash Found

4

Block added to mainchain



User

Start BlockChainED

Create Blockchain

A decentralized network initiated with designated users and miners

Key-pair generated

Transactions done and distributed to miners in network

Miners perform Proof-of-Work, BlockHash found .

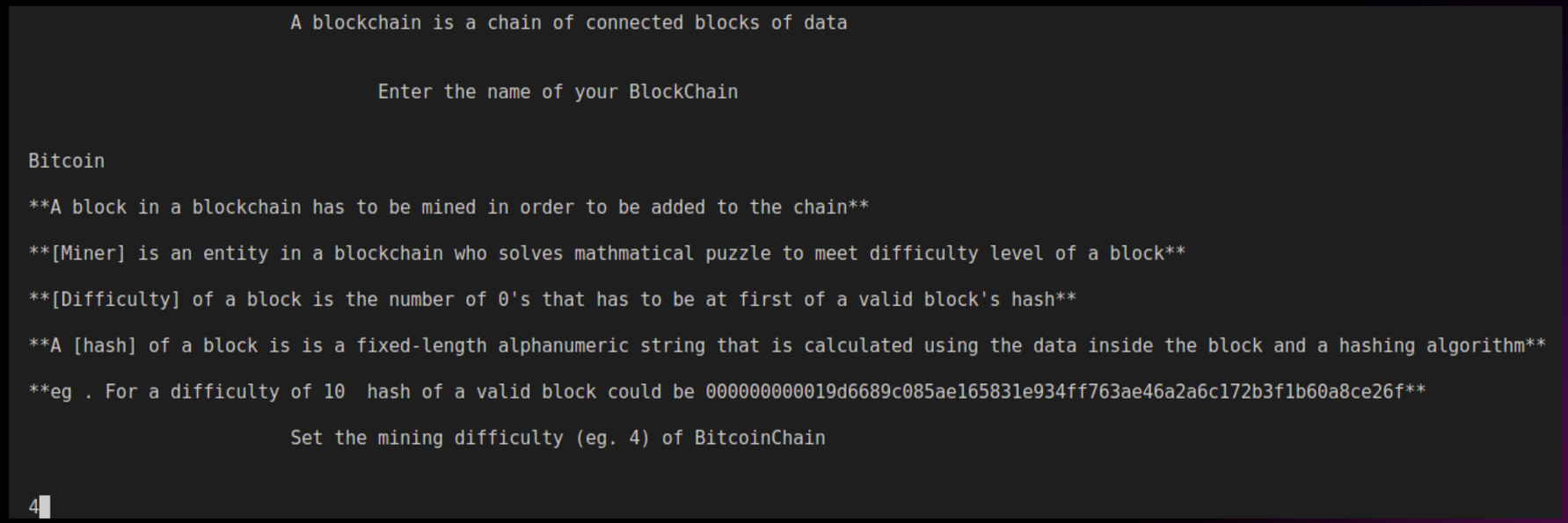
Block added to chain

Inspect / Attack BlockChain

Every step including functional calculation is shown to users

1. Start with creating your own blockchain.

2. Name your chain and add difficulty level



GenesisBlock
(the first block in blockchain) created !

```
                                BitcoinChain initiated !!


**Creating GenesisBlock(The first block of a blockchain).....**


**Adding a null Transaction...**

Transaction hash : e7042ac7d09c7bc41c8cfa5749e41858f6980643bc0db1a83cc793d3e24d3f77

**Adding Default Miner in the chain with MinerId-0...**

**DefaultMiner adding null Transaction to a block...**

Valid block hash has to have 4 0s on front

Nonce(Number used only once) combined with blokc's information , is used to generate valid block hash

Miner performing computational work to find the block nonce

! Nonce found !

**DefaultMiner Mined the Genesis Block...**

************************
 <---Genesis Block--->

************************
-------------------------------------------------------------------------------------------
| Index              : 0
| Previous BlockHash : 0
| BlockHash          : 00004b172a6ec1341b4ba8cb1e7cbc022858e273b3796d6d43e31e1093abbbd4
| Nonce              : 59265
| Difficulty         : 4
| MerkleRoot         : e7042ac7d09c7bc41c8cfa5749e41858f6980643bc0db1a83cc793d3e24d3f77
| Timestamp          : 1684865609
|
|
| Transactions       :
|
| Transaction Index -> 0
| TransactionHash   -> e7042ac7d09c7bc41c8cfa5749e41858f6980643bc0db1a83cc793d3e24d3f77
| SenderKeyPair     -> 0 0
| RecieverrKeyPair  -> 0 0
| Sent Amount       -> 0
|
-------------------------------------------------------------------------------------------
```

Create Wallets

```
*****************************************************************
        Let's star adding UserWallets to your Blockchain
*****************************************************************

When a user creates a wallet in a blockchain network, the wallet generates a pair of cryptographic keys: a public key and a private key.

Private Key : A secret code used to access and manage the funds stored in wallet.

Private Key of the Sender will work as the Digital Signature of a Transaction

Public Key  : Derived from the private key using complex Cryptographic function
                that Represants a wallet in open transactions in blockchain without revealing sensitive information about wallet

How many wallets do you want do add ?
2

Enter UserName   : Alice
Allocate Balance :45
Rremember Alice's  Private Key to verify transactions requested from this  wallet !!  : 30322
Account address :  954c4d20e2dd40112c1fb11881c0eab03b1146391894d5952557b69f7009eab3 created!
Public Key is   : 88221 274657

Enter UserName   : Bob
Allocate Balance :46
Rremember Bob's  Private Key to verify transactions requested from this  wallet !!  : 131177
Account address :  47d378a144d7a496ecb394c43e4414db58728e604f2713f6f68c7c2d3baea3ae created!
Public Key is   : 130607 -455979
```

Make Transactions

```
*******************************
Let's make Transactions !!...
*******************************

How many Transactions do you want to make ?

2

Sender Public Key                       : 88221 274657

Reciever Public Key                     : 130607 -455979

Amount to be sent                       : 15

Digital Signature(Sender's PrivateKey)  : 30322

Offered Transaction fee                 : 3

Transaction hash : 6d31afe4ef0ff7b5ecf21653e9da648c5c17101aca2fac0f4e744866de875007

Sender Public Key                       : 130607 -455979

Reciever Public Key                     : 88221 274657

Amount to be sent                       : 48

Digital Signature(Sender's PrivateKey)  : 131177

Offered Transaction fee                 : 5

Transaction hash : 8d744b6d1085a85f45fe81b15ade9545a02838546650630a766a30d16b2623e3
```

```
**************************
Let's start mining Blocks !
**************************
. . .

Enter Miner ID to appoint miner for mining block   :

1

Miner ID1 Collecting Transactions from the network with higher fees
Block being created with ..
Tx hash            : 8d744b6d1085a85f45fe81b15ade9545a02838546650630a766a30d16b2623e3
Tx hash            : 6d31afe4ef0ff7b5ecf21653e9da648c5c17101aca2fac0f4e744866de875007

Network difficulty : 4
Previous blockhash : 0000f66df4a46077837ae13f678809a3094ca1bdb9cb48c4312521a9e560dd0f

Miner ID-1  started verifying block's transactions...
Wallet 47d378a144d7a496ecb394c43e4414db58728e604f2713f6f68c7c2d3baea3ae does not have sufficient balance
Miner removing 8d744b6d1085a85f45fe81b15ade9545a02838546650630a766a30d16b2623e3 from the chain
Transaction: 6d31afe4ef0ff7b5ecf21653e9da648c5c17101aca2fac0f4e744866de875007 verified!

Miner ID1 started mining block
Valid block hash has to have 4 0s on front

Nonce(Number used only once) combined with blokc's information , is used to generate valid block hash

Miner performing computational work to find the block nonce

! Nonce found !

Block mined with nonce 71335
Transaction 6d31afe4ef0ff7b5ecf21653e9da648c5c17101aca2fac0f4e744866de875007successful !
New balance of sender wallet954c4d20e2dd40112c1fb11881c0eab03b1146391894d5952557b69f7009eab3 : 27
New balance of reciever wallet47d378a144d7a496ecb394c43e4414db58728e604f2713f6f68c7c2d3baea3ae : 61
Transaction fee 3 added to Miner ID 1's balance

Block added to the chain successfully !
**********************
```

Create Block with available transactions and mine the blocks

Mined block added to your chain

```
Block added to the chain successfully !
********************
Here's your chain !
********************
--------------------------------------------------------------------------------
| Index              : 0
| Previous BlockHash : 0
| BlockHash          : 0000f66df4a46077837ae13f678809a3094ca1bdb9cb48c4312521a9e560dd0f
| Nonce              : 73846
| Difficulty         : 4
| MerkleRoot         : e7042ac7d09c7bc41c8cfa5749e41858f6980643bc0db1a83cc793d3e24d3f77
| Timestamp          : 1684866660
|
|
| Transactions       :
|
| Transaction Index -> 0
| TransactionHash   -> e7042ac7d09c7bc41c8cfa5749e41858f6980643bc0db1a83cc793d3e24d3f77
| SenderKeyPair     -> 0 0
| RecieverrKeyPair  -> 0 0
| Sent Amount       -> 0
|
--------------------------------------------------------------------------------
^
|
|
--------------------------------------------------------------------------------
| Index              : 1
| Previous BlockHash : 0000f66df4a46077837ae13f678809a3094ca1bdb9cb48c4312521a9e560dd0f
| BlockHash          : 0000355d0abe75dfa4747ea107904066e39703fdf379787c538312ad624fc421
| Nonce              : 71335
| Difficulty         : 4
| MerkleRoot         : 6d31afe4ef0ff7b5ecf21653e9da648c5c17101aca2fac0f4e744866de875007
| Timestamp          : 1684867152
|
|
| Transactions       :
|
| Transaction Index -> 1
| TransactionHash   -> 6d31afe4ef0ff7b5ecf21653e9da648c5c17101aca2fac0f4e744866de875007
| SenderKeyPair     -> 88221 274657
| RecieverrKeyPair  -> 130607 -455979
| Sent Amount       -> 15
|
--------------------------------------------------------------------------------
^
```

Stay in creation mode or move to inspect and attack

```
Choose from options :

1 . Add more Wallets

2 . Add more Transactions

3 . Add more Miners

4 . Mine more Blocks

5 . Exit

5

***Exiting from BlockChain Creation Mode***


**************************
Choose from options :

1 . Create  BlockChain

2 . Inspect BlockChain

3 . Attack BlockChain

4 . Exit

**************************
2
```

Inspect Blockchain's elements

```
1 . Check Wallets of My Chain
2 . Check Transactions in My Chain
3 . Check for a Block
4 . Check Full chain
5 . Exit
1
Wallet's  Address     : 954c4d20e2dd40112c1fb11881c0eab03b1146391894d5952557b69f7009eab3
Wallet's  Public  Key : 88221 274657
Wallet's  Balance     : 45
Wallet's  Address     : 47d378a144d7a496ecb394c43e4414db58728e604f2713f6f68c7c2d3baea3ae
Wallet's  Public  Key : 130607 -455979
Wallet's  Balance     : 46
Choose from options :
1 . Check Wallets of My Chain
2 . Check Transactions in My Chain
3 . Check for a Block
4 . Check Full chain
5 . Exit
2
| TransactionHash   -> 6d31afe4ef0ff7b5ecf21653e9da648c5c17101aca2fac0f4e744866de875007
| SenderKeyPair     -> 88221 274657
| RecieverrKeyPair  -> 130607 -455979
| Sent Amount       -> 15
|
Choose from options :
1 . Check Wallets of My Chain
2 . Check Transactions in My Chain
3 . Check for a Block
4 . Check Full chain
5 . Exit
3
Enter the Block's Index :
1
-----------------------------------------------------------------------------------------
| Index              : 1
| Previous BlockHash : 0000f66df4a46077837ae13f678809a3094ca1bdb9cb48c4312521a9e560dd0f
| BlockHash          : 0000355d0abe75dfa4747ea107904066e39703fdf379787c538312ad624fc421
| Nonce              : 71335
| Difficulty         : 4
| MerkleRoot         : 6d31afe4ef0ff7b5ecf21653e9da648c5c17101aca2fac0f4e744866de875007
| Timestamp          : 1684867152
|
|
| Transactions       :
|
| Transaction Index -> 1
| TransactionHash   -> 6d31afe4ef0ff7b5ecf21653e9da648c5c17101aca2fac0f4e744866de875007
| SenderKeyPair     -> 88221 274657
| RecieverrKeyPair  -> 130607 -455979
| Sent Amount       -> 15
|
-----------------------------------------------------------------------------------------
```

Try changing valid Block data

```
Choose from options :

1 . Create  BlockChain

2 . Inspect BlockChain

3 . Attack BlockChain

4 . Exit

************************
3
Enter the index of valid Block you want access to :

1
The block :


--------------------------------------------------------------------------------
| Index              : 1
| Previous BlockHash : 0000f66df4a46077837ae13f678809a3094ca1bdb9cb48c4312521a9e560dd0f
| BlockHash          : 0000355d0abe75dfa4747ea107904066e39703fdf379787c538312ad624fc421
| Nonce              : 71335
| Difficulty         : 4
| MerkleRoot         : 6d31afe4ef0ff7b5ecf21653e9da648c5c17101aca2fac0f4e744866de875007
| Timestamp          : 1684867152
|
|
| Transactions       :
|
| Transaction Index -> 1
| TransactionHash   -> 6d31afe4ef0ff7b5ecf21653e9da648c5c17101aca2fac0f4e744866de875007
| SenderKeyPair     -> 88221 274657
| RecieverrKeyPair  -> 130607 -455979
| Sent Amount       -> 15
|
--------------------------------------------------------------------------------
Enter the index(starting from 1) of valid Transaction in the block you want access to : 1

Choose from options :

1 . Change Sender's   Public Key

2 . Change Reciever's Public Key

3 . Change Sender's   Private Key

4 . Change sentAmout

5 . Exit

4
```

Attack preventted

```
5 . Exit

4
Amount : 50

Choose from options :

1 . Change Sender's   Public Key

2 . Change Reciever's Public Key

3 . Change Sender's   Private Key

4 . Change sentAmout

5 . Exit

5
--------------------------------------------------------------------------------
| Index              : 0
| Previous BlockHash : 0
| BlockHash          : 0000f66df4a46077837ae13f678809a3094ca1bdb9cb48c4312521a9e560dd0f
| Nonce              : 73846
| Difficulty         : 4
| MerkleRoot         : e7042ac7d09c7bc41c8cfa5749e41858f6980643bc0db1a83cc793d3e24d3f77
| Timestamp          : 1684866660
|
|
| Transactions       :
|
| Transaction Index -> 0
| TransactionHash   -> e7042ac7d09c7bc41c8cfa5749e41858f6980643bc0db1a83cc793d3e24d3f77
| SenderKeyPair     -> 0 0
| RecieverrKeyPair  -> 0 0
| Sent Amount       -> 0
|
--------------------------------------------------------------------------------
^
|
|
^
|
X
|
Invalid block detected ! Connection broke !
|
X
|


***Exiting from Attack Mode***
```

Challenges

Complexity

Consensus Mechanism

Blockchain attacks

Cryptography and hashing

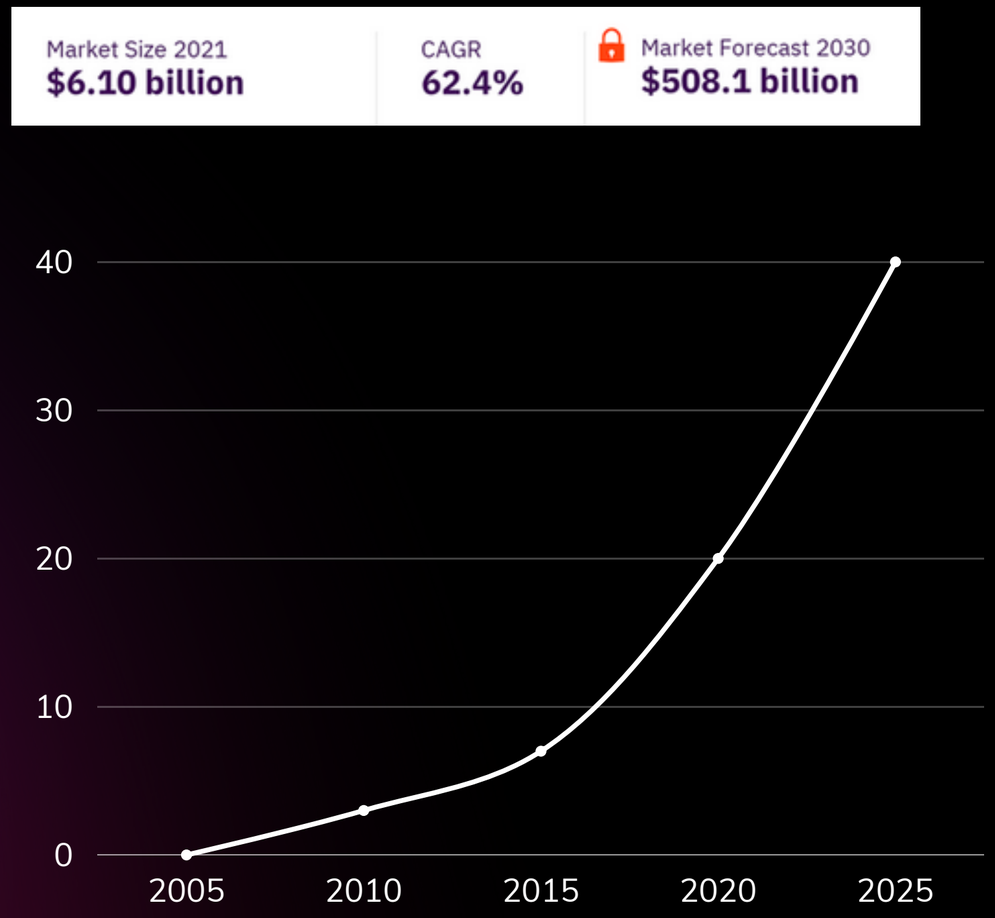
User Experience

Possibilities of the project

- With the increasing popularity and adoption of blockchain, there is a growing demand for individuals with expertise in the field. The project can cater to this demand of learners .

- As the project grows, it can become a hub for individuals and organizations interested in blockchain

- The project can be used by educational institutions to teach students about blockchain and its potential applications in their future careers.



BlockChainED

THANK YOU!!