Batch: BCT_1 Roll No.: 1911027

Experiment No. 2

Title: Creation of a private block chain cryptocurrency

Objective: To implement private blockchain cryptocurrency and to explore how bitcoin and ethereum are executed at the bottommost level.

Expected Outcome of Experiment:

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

Books/ Journals/ Websites referred:

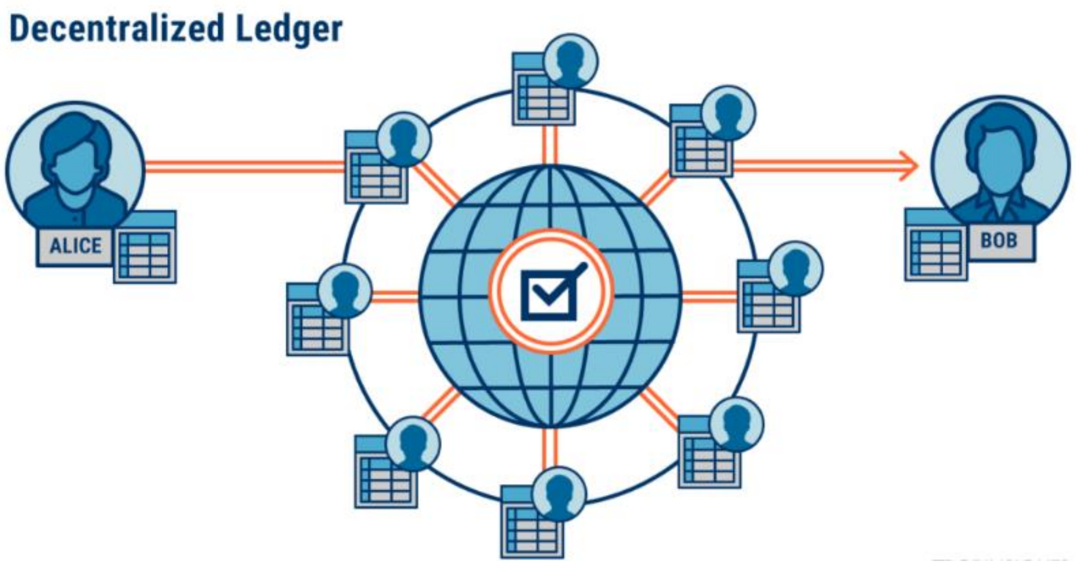
1. https://www.investopedia.com/how-to-make-a-cryptocurrency-5215343
2. https://readwrite.com/relationship-between-blockchain-and-cryptocurrency/
3. https://en.wikipedia.org/wiki/Bitcoin
4. https://en.wikipedia.org/wiki/Ethereum
5. https://www.forbes.com/advisor/in/investing/cryptocurrency/what-is-cryptocurrency-and-how-does-it-work/

Abstract:-

Anyone can create a cryptocurrency, but the process requires commitments of time, money, and other resources, in addition to advanced technical knowledge. The main options are creating your own blockchain, modifying an existing blockchain, establishing a coin on an existing blockchain, or hiring a blockchain developer. Making a cryptocurrency is the easy part. Maintaining and growing it over time is usually more challenging. Whenever the word blockchain is used, cryptocurrency automatically comes to mind, and it is true the other way as well. Many people believe that the two are synonymous and, thus, are often used interchangeably, but it couldn't be more wrong. Cryptocurrencies are a type of money that use blockchain technology to operate. Cryptocurrency is decentralized digital money that is based on blockchain technology and secured by cryptography. To understand cryptocurrency, one needs to first understand three terminologies – blockchain, decentralization, and cryptography.

Related Theory: -

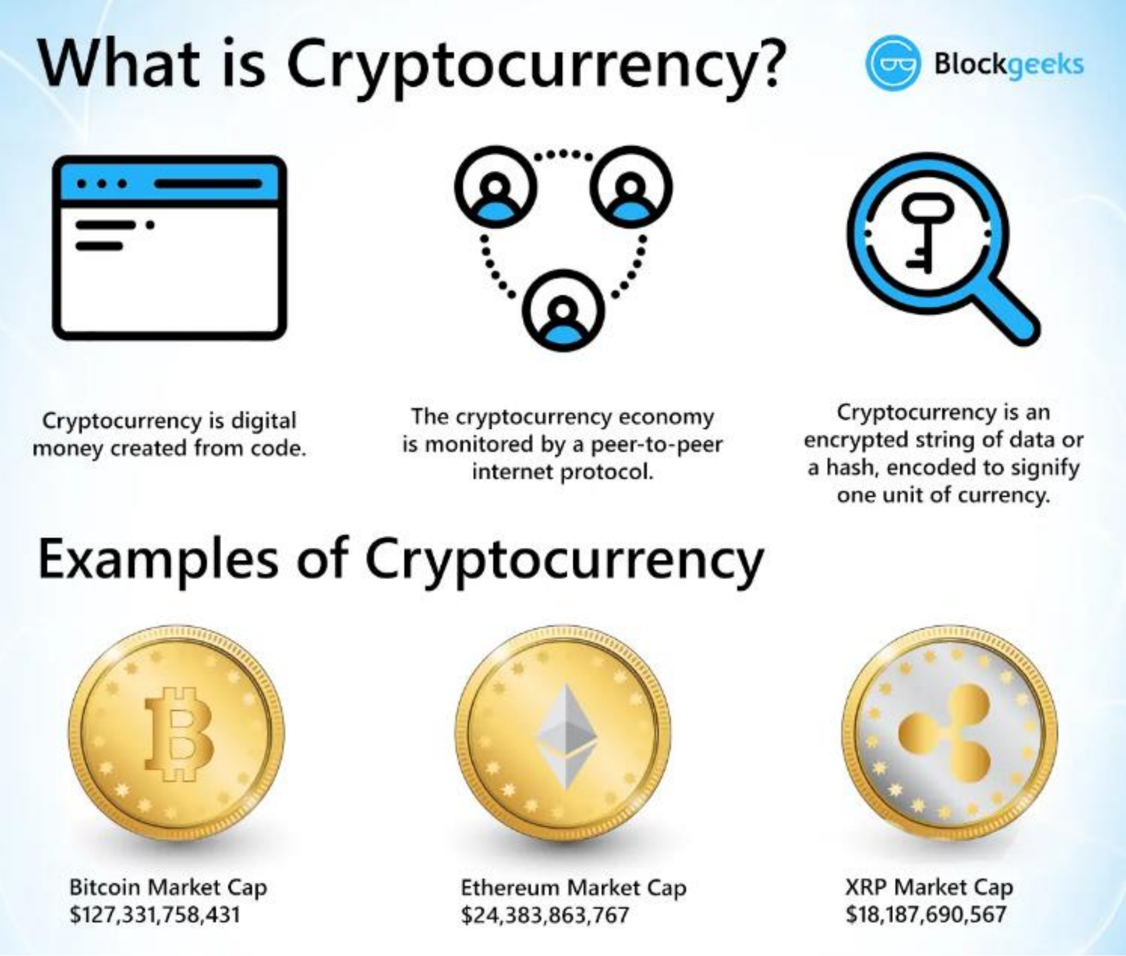
Blockchain was first introduced with the debut of Bitcoin. Bitcoin was a cryptocurrency, and from then on, myths spread that blockchain and cryptocurrencies are the same. Blockchain is a decentralized ledger that keeps the records of transactions, and these ledgers cannot be altered. So, once a transaction has been approved and included in a block, it becomes permanent. Now it will always exist in the blockchain. What makes blockchain technology different is that it is completely decentralized means there is no central authority that owns it or manages it. It is for consumers and belongs to them. The data is saved on blocks. Each block is made up of a certain number of transactions. When a block is completed, the network approves it, and it is added to the blockchain, making it unchangeable.



What Is Cryptocurrency?

Cryptocurrency is made up of two words- crypto and currency. While the meaning of currency is clear that it is money, crypto means encrypted or written in codes. So, the meaning of a cryptocurrency is that it is a digital asset that has a value like money. It is created to foster easy exchange, and that’s where blockchain comes into the picture. All the crypto transactions that take place are recorded using blockchain technology. The first ever cryptocurrency was Bitcoin, which became synonymous with blockchain. Since then, thousands of cryptocurrencies have entered the market. In simple words, blockchain in the context of cryptocurrency is a digital ledger whose access is distributed among authorized users. This ledger records transactions related to a range of assets, like money, house, or even intellectual property. The access is shared between its users and any information shared is transparent, immediate, and “immutable”. Immutable means anything that blockchain records is there for good and cannot be modified or tampered with – even by an administrator. Centralized money refers to the regular money that we use, which is governed by authorities like the

Reserve Bank of India. Decentralization in cryptocurrency means there is no similar authority that can be held responsible for supervising the rise and fall of a particular cryptocurrency. This has many benefits over centralized money.


What is Cryptocurrency?
Blockgeeks
Cryptocurrency is digital money created from code.
The cryptocurrency economy is monitored by a peer-to-peer internet protocol.
Cryptocurrency is an encrypted string of data or a hash, encoded to signify one unit of currency.
Examples of Cryptocurrency
Bitcoin Market Cap $127,331,758,431
Ethereum Market Cap $24,383,863,767
XRP Market Cap $18,187,690,567

How Blockchain and Cryptocurrencies Complement Each Other?

Cryptocurrencies and blockchain work together to create a chain of transactions that is decentralized, secure, and completely digital. There is no office, a warehouse where the servers are kept, or any other place where the operations are carried out. The similarities between the two are discussed below:

- **Advanced Technologies:** Both blockchain and cryptocurrencies are advanced technologies that are still a matter of curiosity for many. The reason that there is no authority to supervise irks many. Cryptocurrencies are also an advanced technology that did not make sense when they made their debut. People were skeptical as to how they could undertake transactions using a type of money that didn't exist physically. But today, they are widely accepted.
- **Intangible:** Both the blockchain and cryptocurrencies are intangible. There is no server or computer from which you can access the entire data. Thus, there is

no blockchain ownership as it is a distributed ledger. The same goes for cryptocurrency because it is so unlike a fiat currency. You can't touch or hold it physically.

- **Interdependent:** Blockchain technology was created to support Bitcoin. Or it can be said that if there had been no blockchain, Bitcoin would not have come into existence. Thus, blockchain is the foundation for cryptocurrency. Both technologies are interdependent.
- **To Ease Exchange and Transfer:** Blockchain will drive the future of the financial sector. The aim of the financial sector is to facilitate easy transfers and exchanges, but traditional banking methods are time-consuming, whereas blockchain transactions are easier, fast, and more secure. Plus, they eliminate the need for intermediaries like banks and offer users the ease of transacting directly with each other. Furthermore, since all the transactions are recorded and irreversible, it increases transparency and security.
- **Cybersecurity:** Since blockchain technology is decentralized, there is no single point that a hacker can target. The data is distributed, and it makes blockchains the safest storage. Plus, if an unauthorized change is made, it is easily traceable.
- **Smart Contracts:** The latest blockchain technologies have introduced smart contracts which are transparent, self-executing, and safe. These smart contracts record the terms of the agreement, and as and when the parties fulfill the conditions of the contract, they execute automatically. As a result, they can be used for many purposes, which can significantly cut down on business costs.

How Does Cryptocurrency Work?

Cryptocurrencies are not controlled by the government or central regulatory authorities. As a concept, cryptocurrency works outside of the banking system using different brands or types of coins – Bitcoin being the major player.

1. **Mining:** Cryptocurrencies (which are completely digital) are generated through a process called "mining". This is a complex process. Basically, miners are required to solve certain mathematical puzzles over specially equipped computer systems to be rewarded with bitcoins in exchange.
2. **Buying, selling, and storing:** Users today can buy cryptocurrencies from central exchanges, brokers, and individual currency owners or sell it to them. Exchanges or platforms like Coinbase are the easiest ways to buy or sell cryptocurrencies.
3. **Transacting or investing:** Cryptocurrencies like Bitcoins can be easily transferred from one digital wallet to another, using only a smartphone. Once

you own them, your choices are to: a) use them to buy goods or services b) trade in them c) exchange them for cash. If you are using Bitcoin for purchases, the easiest way to do that is through debit-card-type transactions. You can also use these debit cards to withdraw cash, just like at an ATM. Converting cryptocurrency to cash is also possible using banking accounts or peer-to-peer transactions.

How Are Cryptocurrencies Made?

If you want to create a cryptocurrency, you have a few different options.

1) **Create your own blockchain and native cryptocurrency:** You can write your own code to create a new blockchain that supports a native cryptocurrency. Pursuing this option usually requires extensive technical training to develop coding skills and a fundamental understanding of blockchain technology—but it also affords the greatest amount of design freedom. If you want to create a cryptocurrency that is truly new or innovative in some way, then building your own blockchain to support that coin is probably your best option. You can design your native coin in any way that you like. Native coins, which by definition have their own blockchains, are considered as superior to tokens, which are digital currencies that operate on other blockchain networks.

2) **Modify the code of an existing blockchain:** You can decide to use the source code of another blockchain to create a new blockchain and native cryptocurrency. Pursuing this option still likely requires technical knowledge, as you may choose to modify the source code to satisfy your design objectives. After you download and modify the source code of an existing blockchain, you still need to work with a blockchain auditor and obtain professional legal advice. After that, you are ready to mint your new cryptocurrency.

3) **Establish a new cryptocurrency on an existing blockchain:** You can make a new cryptocurrency without first creating or modifying any blockchain. Platforms like the Ethereum blockchain are designed to host the cryptocurrencies of many different developers. The resulting new currency would be classified as a token, which is any digital money that is not native to the blockchain on which it operates. Creating a token that uses an existing blockchain can require some technical expertise, but anyone with moderate computer knowledge can probably create their own token without too much difficulty.

4) **Hire a blockchain developer to create a cryptocurrency for you:** You can create a new coin or token with any degree of customization by hiring a blockchain development company. Many enterprises, known as blockchain-as-a-service (BaaS) companies, exist to create and maintain new blockchain

networks and cryptocurrencies. Some BaaS companies develop customized blockchains, while others use their own existing blockchain infrastructure. You can also work with a BaaS company to launch a highly customized token on an existing blockchain platform. Some of the most prominent BaaS companies include Amazon Web Services, Microsoft Azure, ChainZilla, and Blockstream.

Advantages of cryptocurrency:

- **They are private and secure:** The blockchain technology that fuels cryptocurrencies ensures user anonymity. It also assures high levels of security through cryptography, which we discussed before.
- **They are decentralized, immutable, and transparent:** The entire system functions on shared ownership, where data is available to all permissioned members and is tamper-proof.
- **They are a hedge against inflation:** Cryptocurrency makes for a great investment in times of inflation. For example, investors often compare cryptocurrency to gold.
- **Cost-effective mode of transaction:** One of the major uses of cryptocurrencies is to send money across borders. With the help of cryptocurrency, the transaction fees paid by a user is reduced to a negligible or zero amount.
- **A fast way to transfer funds:** Cryptocurrencies have always kept itself as an optimal solution for transactions. Transactions, whether international or domestic in cryptocurrencies, are lightning-fast.

Disadvantages of cryptocurrency:

- **They are not widely understood:** They are a relatively new concept and the long-term sustainability of cryptocurrencies remains to be seen.
- **They are prone to high risks:** Needless to say, cryptocurrencies bring in as many rewards as risks. Their highly volatile and speculative nature makes them prone to sharp downward spirals. Investing in cryptocurrency can be risky for many reasons.
- **Decentralized but still operated by some organization:** The cryptocurrencies are known for its feature of being decentralized. But, the flow and amount of some currencies in the market are still controlled by their creators and some organizations.

- **Adverse Effects of mining on the environment:** Mining cryptocurrencies require a lot of computational power and electricity input, making it highly energy-intensive. The biggest culprit in this is Bitcoin. Mining Bitcoin requires advanced computers and a lot of energy. It cannot be done on ordinary computers.

Implementation Details:

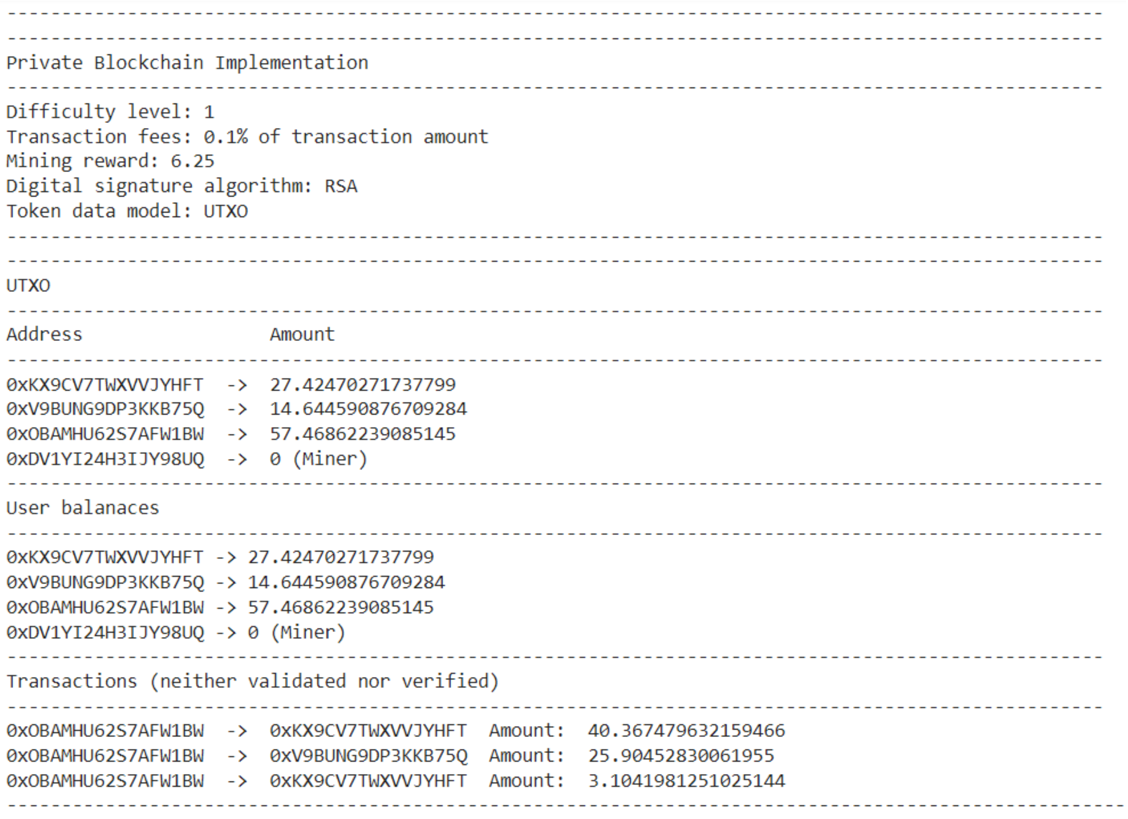
Code:

Github link: https://github.com/nixen2802/Blockchain-Python.git

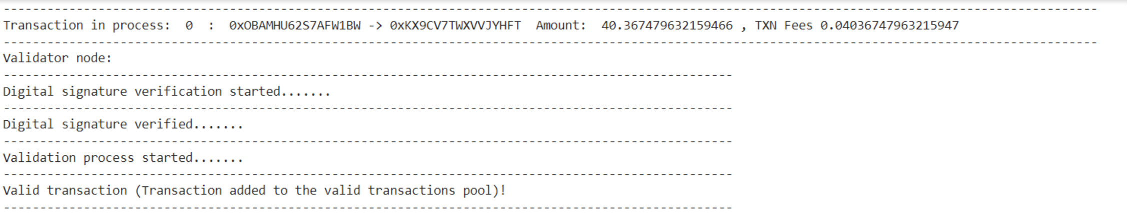
Google colab link:

https://colab.research.google.com/drive/18FLMgyEm4Rb7n2AXEDfJ1GFGnhuT3Tnf?usp=sharing

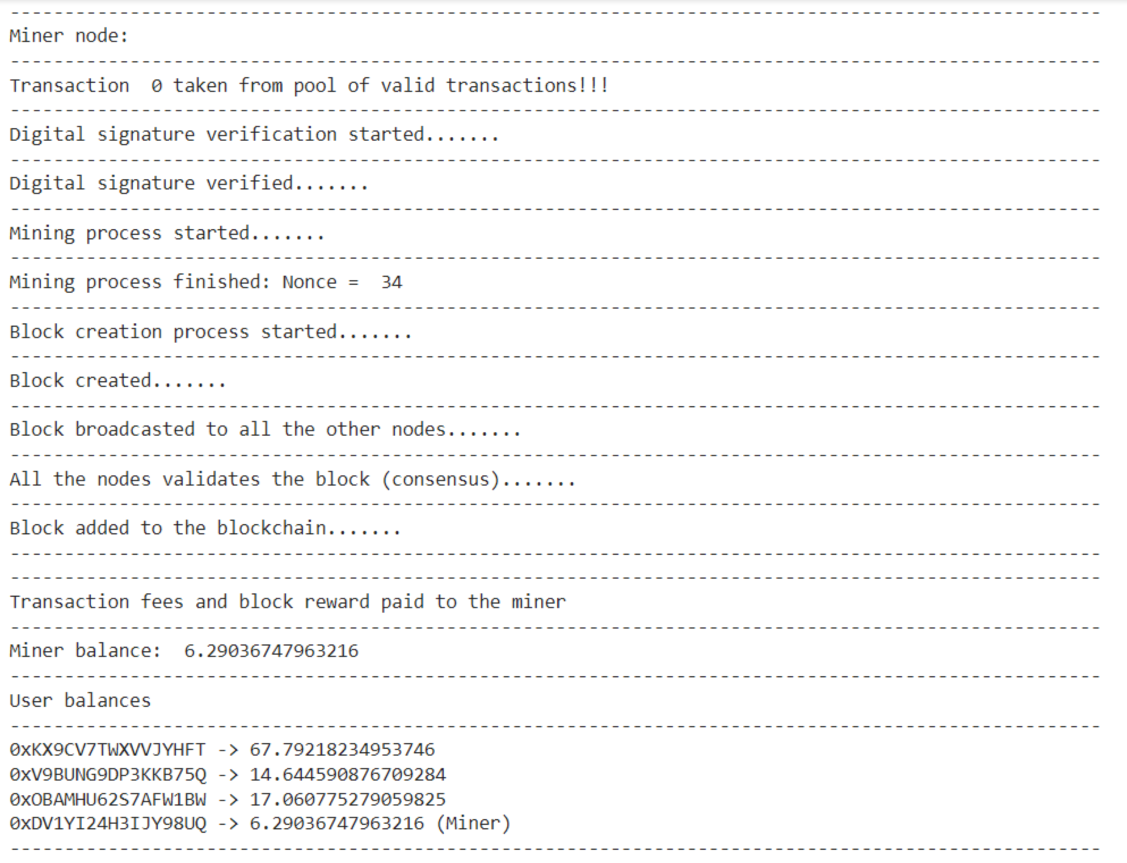
Output:



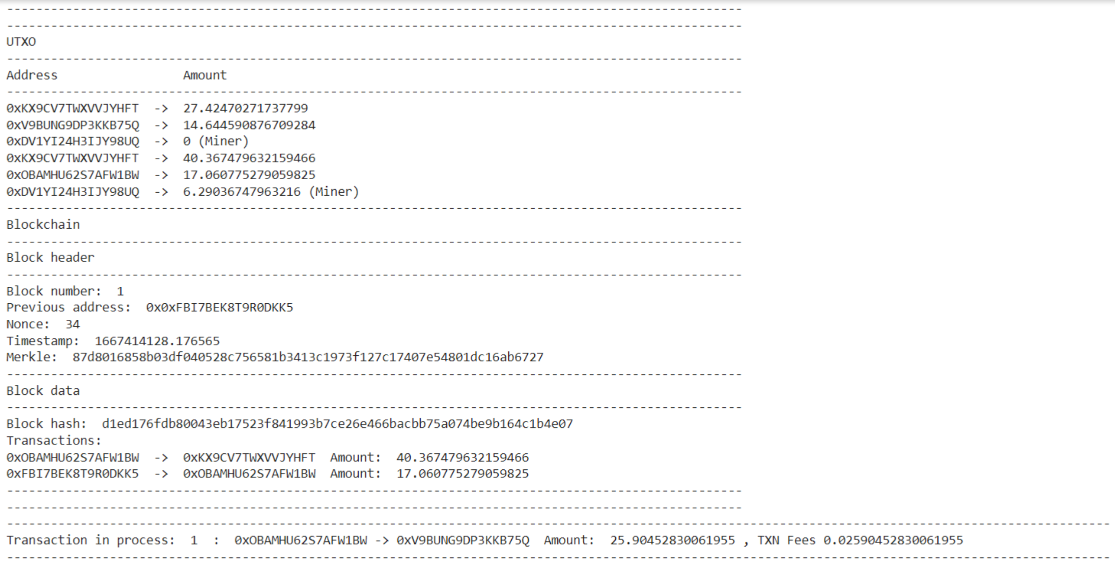
```
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
Private Blockchain Implementation
-----------------------------------------------------------------------------------------
Difficulty level: 1
Transaction fees: 0.1% of transaction amount
Mining reward: 6.25
Digital signature algorithm: RSA
Token data model: UTXO
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
UTXO
-----------------------------------------------------------------------------------------
Address                 Amount
-----------------------------------------------------------------------------------------
0xKX9CV7TWXVVJYHFT  ->  27.42470271737799
0xV9BUNG9DP3KKB75Q  ->  14.644590876709284
0xOBAMHU62S7AFW1BW  ->  57.46862239085145
0xDV1YI24H3IJY98UQ  ->  0 (Miner)
-----------------------------------------------------------------------------------------
User balanaces
-----------------------------------------------------------------------------------------
0xKX9CV7TWXVVJYHFT -> 27.42470271737799
0xV9BUNG9DP3KKB75Q -> 14.644590876709284
0xOBAMHU62S7AFW1BW -> 57.46862239085145
0xDV1YI24H3IJY98UQ -> 0 (Miner)
-----------------------------------------------------------------------------------------
Transactions (neither validated nor verified)
-----------------------------------------------------------------------------------------
0xOBAMHU62S7AFW1BW  ->  0xKX9CV7TWXVVJYHFT  Amount:  40.367479632159466
0xOBAMHU62S7AFW1BW  ->  0xV9BUNG9DP3KKB75Q  Amount:  25.90452830061955
0xOBAMHU62S7AFW1BW  ->  0xKX9CV7TWXVVJYHFT  Amount:  3.1041981251025144
-------------------------------------------------------------------------------------------
```



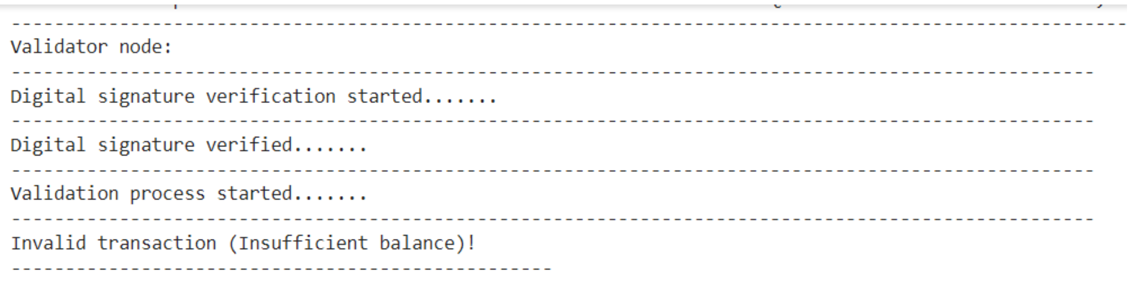
```
-----------------------------------------------------------------------------------------------------------------------------------------
Transaction in process:  0  :  0xOBAMHU62S7AFW1BW -> 0xKX9CV7TWXVVJYHFT  Amount:  40.367479632159466 , TXN Fees 0.04036747963215947
-----------------------------------------------------------------------------------------------------------------------------------------
Validator node:
-------------------------------------------------------------------------------------------
Digital signature verification started.......
-------------------------------------------------------------------------------------------
Digital signature verified.......
-------------------------------------------------------------------------------------------
Validation process started.......
-------------------------------------------------------------------------------------------
Valid transaction (Transaction added to the valid transactions pool)!
-------------------------------------------------------------------------------------------
```



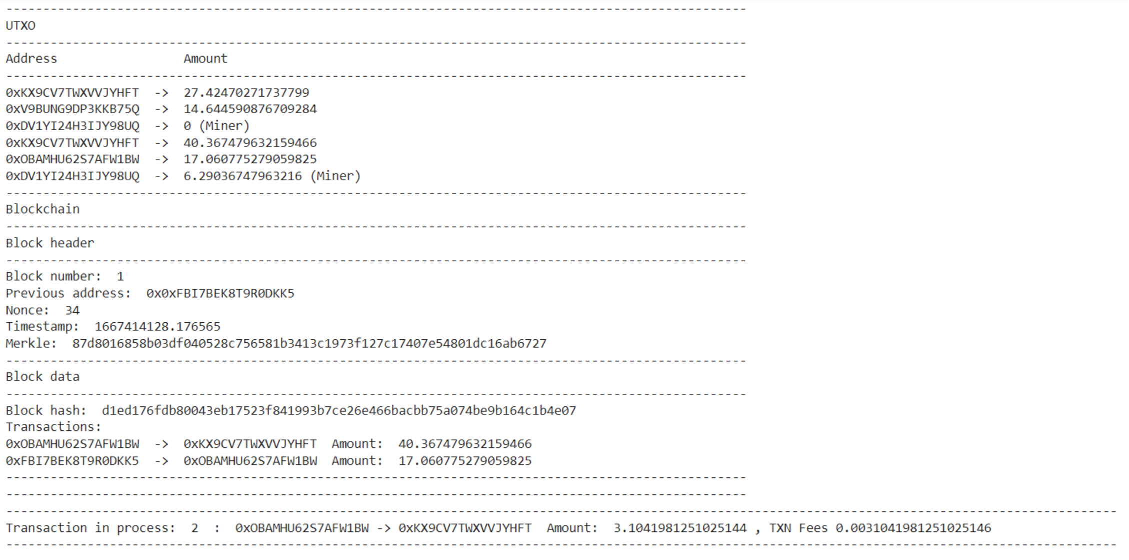
```
----------------------------------------------------------------------------------------------------
Miner node:
----------------------------------------------------------------------------------------------------
Transaction  0 taken from pool of valid transactions!!!
----------------------------------------------------------------------------------------------------
Digital signature verification started.......
----------------------------------------------------------------------------------------------------
Digital signature verified.......
----------------------------------------------------------------------------------------------------
Mining process started.......
----------------------------------------------------------------------------------------------------
Mining process finished: Nonce =  34
----------------------------------------------------------------------------------------------------
Block creation process started.......
----------------------------------------------------------------------------------------------------
Block created.......
----------------------------------------------------------------------------------------------------
Block broadcasted to all the other nodes.......
----------------------------------------------------------------------------------------------------
All the nodes validates the block (consensus).......
----------------------------------------------------------------------------------------------------
Block added to the blockchain.......
----------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------
Transaction fees and block reward paid to the miner
----------------------------------------------------------------------------------------------------
Miner balance:  6.29036747963216
----------------------------------------------------------------------------------------------------
User balances
----------------------------------------------------------------------------------------------------
0xKX9CV7TWXVVJYHFT -> 67.79218234953746
0xV9BUNG9DP3KKB75Q -> 14.644590876709284
0xOBAMHU62S7AFW1BW -> 17.060775279059825
0xDV1YI24H3IJY98UQ -> 6.29036747963216 (Miner)
----------------------------------------------------------------------------------------------------
```



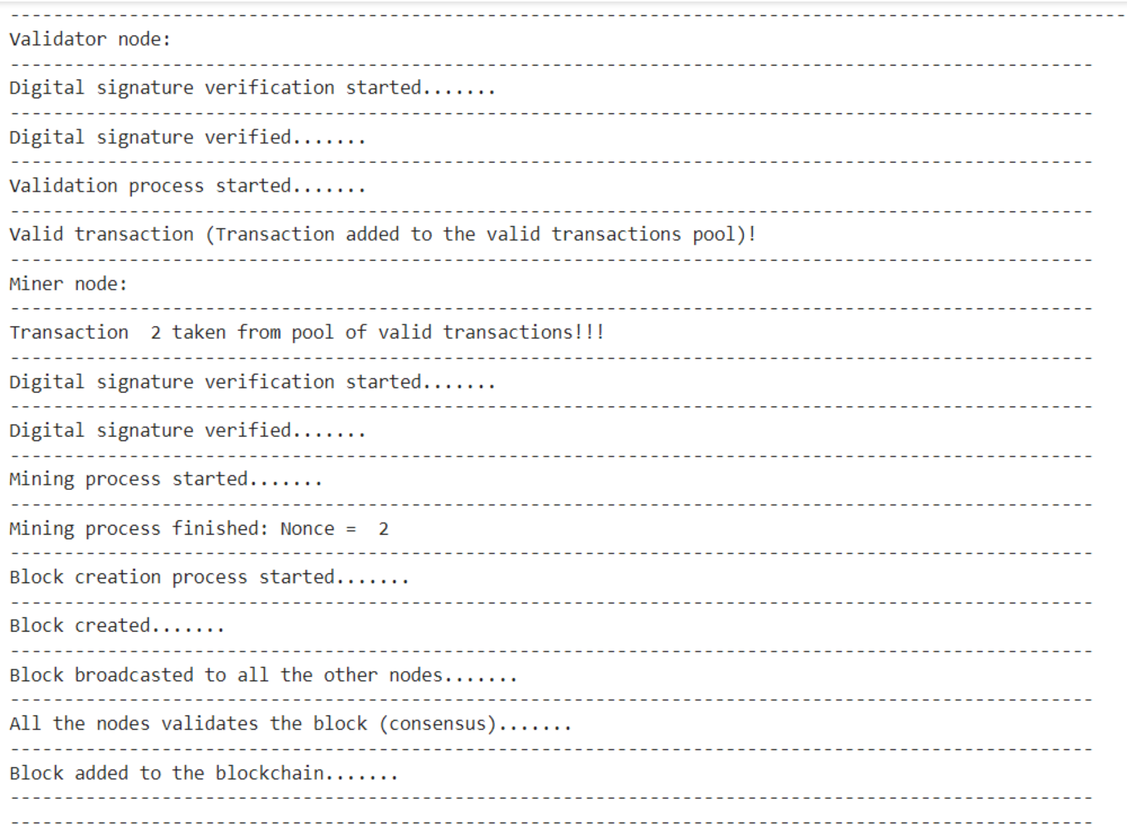
```
----------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------
UTXO
----------------------------------------------------------------------------------------------------
Address                 Amount
----------------------------------------------------------------------------------------------------
0xKX9CV7TWXVVJYHFT  ->  27.42470271737799
0xV9BUNG9DP3KKB75Q  ->  14.644590876709284
0xDV1YI24H3IJY98UQ  ->  0 (Miner)
0xKX9CV7TWXVVJYHFT  ->  40.367479632159466
0xOBAMHU62S7AFW1BW  ->  17.060775279059825
0xDV1YI24H3IJY98UQ  ->  6.29036747963216 (Miner)
----------------------------------------------------------------------------------------------------
Blockchain
----------------------------------------------------------------------------------------------------
Block header
----------------------------------------------------------------------------------------------------
Block number:  1
Previous address:  0x0xFBI7BEK8T9R0DKK5
Nonce:  34
Timestamp:  1667414128.176565
Merkle:  87d8016858b03df040528c756581b3413c1973f127c17407e54801dc16ab6727
----------------------------------------------------------------------------------------------------
Block data
----------------------------------------------------------------------------------------------------
Block hash:  d1ed176fdb80043eb17523f841993b7ce26e466bacbb75a074be9b164c1b4e07
Transactions:
0xOBAMHU62S7AFW1BW  ->  0xKX9CV7TWXVVJYHFT  Amount:  40.367479632159466
0xFBI7BEK8T9R0DKK5  ->  0xOBAMHU62S7AFW1BW  Amount:  17.060775279059825
----------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------------------------------------
Transaction in process:  1  :  0xOBAMHU62S7AFW1BW -> 0xV9BUNG9DP3KKB75Q  Amount:  25.90452830061955 , TXN Fees 0.025904528300619555
------------------------------------------------------------------------------------------------------------------------------------------------------
```



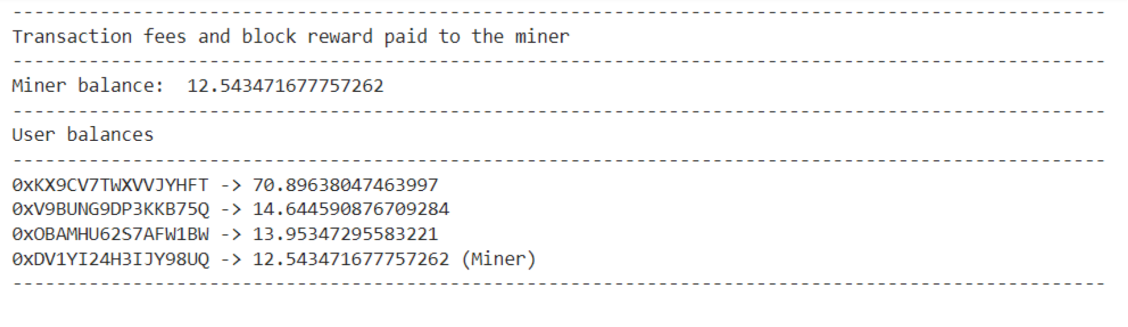
```
-----------------------------------------------------------------------------------------------
Validator node:
-----------------------------------------------------------------------------------------------
Digital signature verification started.......
-----------------------------------------------------------------------------------------------
Digital signature verified.......
-----------------------------------------------------------------------------------------------
Validation process started.......
-----------------------------------------------------------------------------------------------
Invalid transaction (Insufficient balance)!
--------------------------------------------------
```



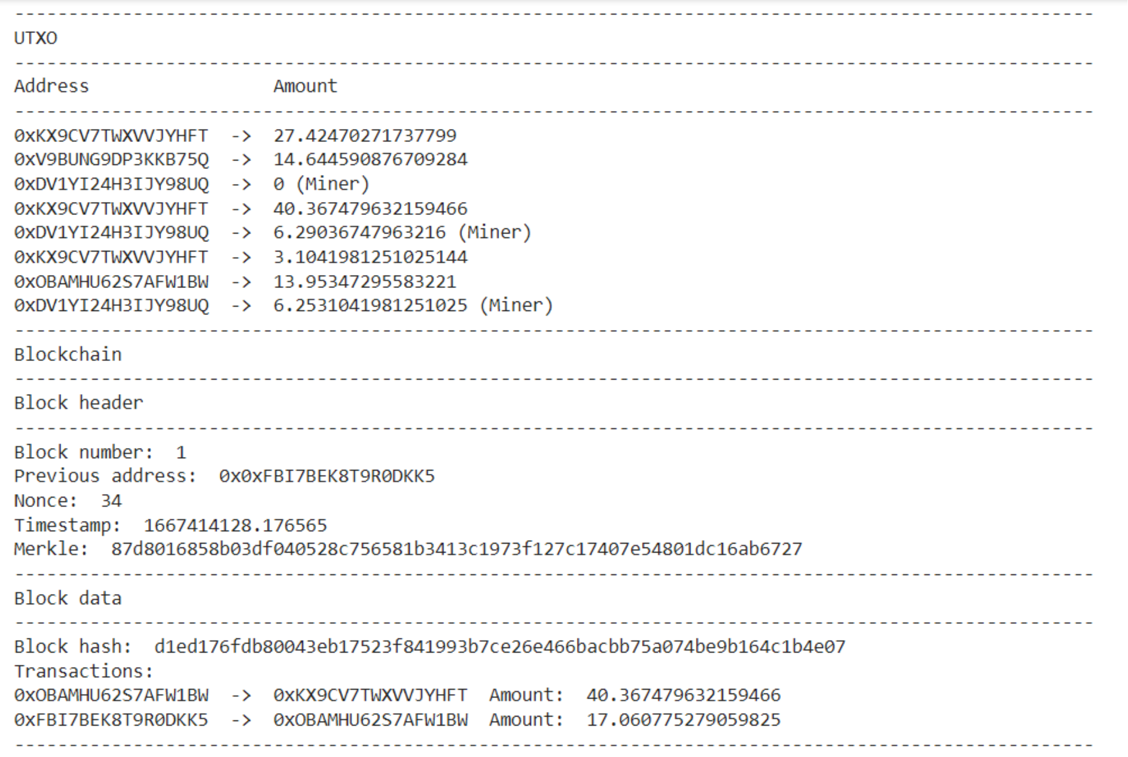
```
------------------------------------------------------------------------------------------------
UTXO
------------------------------------------------------------------------------------------------
Address                  Amount
------------------------------------------------------------------------------------------------
0xKX9CV7TWXVVJYHFT  ->  27.42470271737799
0xV9BUNG9DP3KKB75Q  ->  14.644590876709284
0xDV1YI24H3IJY98UQ  ->  0 (Miner)
0xKX9CV7TWXVVJYHFT  ->  40.367479632159466
0xOBAMHU62S7AFW1BW  ->  17.060775279059825
0xDV1YI24H3IJY98UQ  ->  6.29036747963216 (Miner)
------------------------------------------------------------------------------------------------
Blockchain
------------------------------------------------------------------------------------------------
Block header
------------------------------------------------------------------------------------------------
Block number:  1
Previous address:  0x0xFBI7BEK8T9R0DKK5
Nonce:  34
Timestamp:  1667414128.176565
Merkle:  87d8016858b03df040528c756581b3413c1973f127c17407e54801dc16ab6727
------------------------------------------------------------------------------------------------
Block data
------------------------------------------------------------------------------------------------
Block hash:  d1ed176fdb80043eb17523f841993b7ce26e466bacbb75a074be9b164c1b4e07
Transactions:
0xOBAMHU62S7AFW1BW  ->  0xKX9CV7TWXVVJYHFT  Amount:  40.367479632159466
0xFBI7BEK8T9R0DKK5  ->  0xOBAMHU62S7AFW1BW  Amount:  17.060775279059825
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------
Transaction in process:  2  :  0xOBAMHU62S7AFW1BW -> 0xKX9CV7TWXVVJYHFT  Amount:  3.1041981251025144 , TXN Fees 0.0031041981251025146
--------------------------------------------------------------------------------------------------------------------------------------------------
```



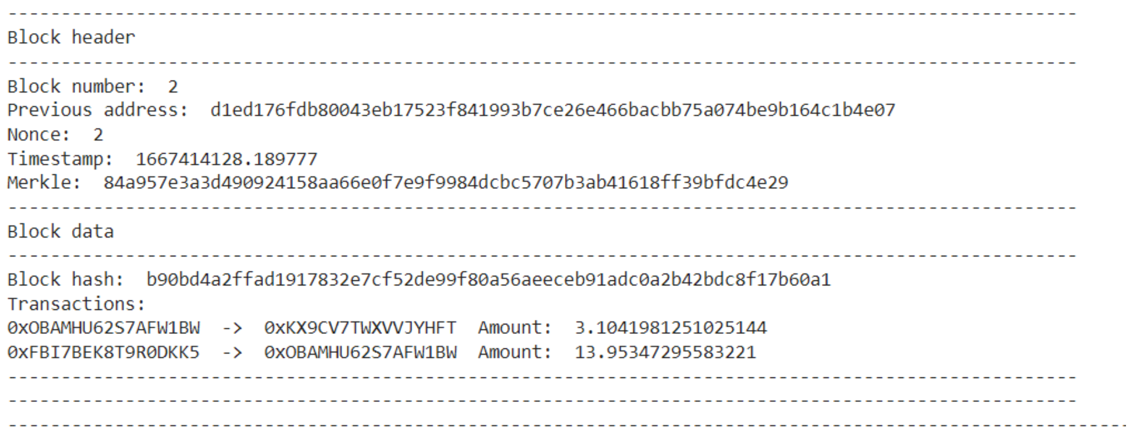
```
-----------------------------------------------------------------------------------------------
Validator node:
-----------------------------------------------------------------------------------------------
Digital signature verification started.......
-----------------------------------------------------------------------------------------------
Digital signature verified.......
-----------------------------------------------------------------------------------------------
Validation process started.......
-----------------------------------------------------------------------------------------------
Valid transaction (Transaction added to the valid transactions pool)!
-----------------------------------------------------------------------------------------------
Miner node:
-----------------------------------------------------------------------------------------------
Transaction  2 taken from pool of valid transactions!!!
-----------------------------------------------------------------------------------------------
Digital signature verification started.......
-----------------------------------------------------------------------------------------------
Digital signature verified.......
-----------------------------------------------------------------------------------------------
Mining process started.......
-----------------------------------------------------------------------------------------------
Mining process finished: Nonce =  2
-----------------------------------------------------------------------------------------------
Block creation process started.......
-----------------------------------------------------------------------------------------------
Block created.......
-----------------------------------------------------------------------------------------------
Block broadcasted to all the other nodes.......
-----------------------------------------------------------------------------------------------
All the nodes validates the block (consensus).......
-----------------------------------------------------------------------------------------------
Block added to the blockchain.......
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
```



```
--------------------------------------------------------------------------------
Transaction fees and block reward paid to the miner
--------------------------------------------------------------------------------
Miner balance:  12.543471677757262
--------------------------------------------------------------------------------
User balances
--------------------------------------------------------------------------------
0xKX9CV7TWXVVJYHFT -> 70.89638047463997
0xV9BUNG9DP3KKB75Q -> 14.644590876709284
0xOBAMHU62S7AFW1BW -> 13.95347295583221
0xDV1YI24H3IJY98UQ -> 12.543471677757262 (Miner)
--------------------------------------------------------------------------------
```



```
--------------------------------------------------------------------------------
UTXO
--------------------------------------------------------------------------------
Address                  Amount
--------------------------------------------------------------------------------
0xKX9CV7TWXVVJYHFT  ->  27.42470271737799
0xV9BUNG9DP3KKB75Q  ->  14.644590876709284
0xDV1YI24H3IJY98UQ  ->  0 (Miner)
0xKX9CV7TWXVVJYHFT  ->  40.367479632159466
0xDV1YI24H3IJY98UQ  ->  6.29036747963216 (Miner)
0xKX9CV7TWXVVJYHFT  ->  3.1041981251025144
0xOBAMHU62S7AFW1BW  ->  13.95347295583221
0xDV1YI24H3IJY98UQ  ->  6.2531041981251025 (Miner)
--------------------------------------------------------------------------------
Blockchain
--------------------------------------------------------------------------------
Block header
--------------------------------------------------------------------------------
Block number:  1
Previous address:  0x0xFBI7BEK8T9R0DKK5
Nonce:  34
Timestamp:  1667414128.176565
Merkle:  87d8016858b03df040528c756581b3413c1973f127c17407e54801dc16ab6727
--------------------------------------------------------------------------------
Block data
--------------------------------------------------------------------------------
Block hash:  d1ed176fdb80043eb17523f841993b7ce26e466bacbb75a074be9b164c1b4e07
Transactions:
0xOBAMHU62S7AFW1BW  ->  0xKX9CV7TWXVVJYHFT  Amount:  40.367479632159466
0xFBI7BEK8T9R0DKK5  ->  0xOBAMHU62S7AFW1BW  Amount:  17.060775279059825
--------------------------------------------------------------------------------
```



```
--------------------------------------------------------------------------------
Block header
--------------------------------------------------------------------------------
Block number:  2
Previous address:  d1ed176fdb80043eb17523f841993b7ce26e466bacbb75a074be9b164c1b4e07
Nonce:  2
Timestamp:  1667414128.189777
Merkle:  84a957e3a3d490924158aa66e0f7e9f9984dcbc5707b3ab41618ff39bfdc4e29
--------------------------------------------------------------------------------
Block data
--------------------------------------------------------------------------------
Block hash:  b90bd4a2ffad1917832e7cf52de99f80a56aeeceb91adc0a2b42bdc8f17b60a1
Transactions:
0xOBAMHU62S7AFW1BW  ->  0xKX9CV7TWXVVJYHFT  Amount:  3.1041981251025144
0xFBI7BEK8T9R0DKK5  ->  0xOBAMHU62S7AFW1BW  Amount:  13.95347295583221
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

1. Enlist all the Steps followed and various options explored

➔ **Steps:**

1) Installing the required libraries for the execution of digital signature algorithms.

2) Importing the libraries and some of their associated functions that will be used in the code.

3) Calculating the base address that will be used for transferring the remaining amount of cryptocurrency after the sender performs some transactions back to the sender.

4) Calculating the previous address that will be used as the previous block address for the first block in the blockchain.

5) Defining user class having fields as user address (a randomly generated hex value), private key and the public key. This class will be useful for storing the user's data.

6) Defining UTXO class having fields as user address and unspent (defining unspent amount). This class will provide template for the UTXO transactions.

7) Defining DB_UTXO class which will have transactions as the only field. This class will be storing the all the objects of the UTXO class.

8) Defining transactions class which will store transactions (randomly generated). This class will have from address, to address, amount and the digital signature as fields defined inside it.

9) Defining block class which will store the blocks in the blockchain. This class will have block number, previous hash, nonce, timestamp, block hash, merkle root and transactions.

10) Randomly generating account balances of users in terms of utxo's. Creating the object of the utxo class with user address and amount and then appending the object in to the utxo db.

11) Randomly generating transactions and constructing the transactions object. After the to and from user addresses are calculated and the amount is generated creating the string value of all the above mentioned fields and signing it using the private key of the from user.

12) Defining the validate function which will be used for verifying the digital signature and checking the availability of funds.

13) First the digital signature will be verified using the public key of the user and then checking whether the amount to send with transaction fees is less than the total amount held by the user.

14) Returning true if verification is successful and false if the digital signature is not verified or the account balance is not sufficient to execute the transaction.

15) Defining the mining function which will be used for digital signature verification and proof of work verification. This function will be used by the miner to calculate the nonce which will satisfy the difficulty level.

16) First the digital signature will be verified and after that from address, to address, amount of transaction in process will be concatenated and hashing process will start until difficulty level is not satisfied (1 leading 0 in the final hash).

17) The function will return the value of nonce.

18) Defining the utxo updation which will be used for updating the utxo after a successful transaction.
19) This function will delete all the previous entries in the utxo which have the user address as the from address of the transaction in process.
20) Defining the balance calculation function which will be useful for calculating the user balance.
21) This function will iterate over all the utxo database entries and calculates the total amount associated with a particular address.
22) This function will return balance associated with a particular user address.
23) Defining the address calculation which will be used for finding the merkle root hash.
24) This function will return the hash generated.
25) Defining the block hash calculator which will be used for calculating the hash of the block.
26) This function will form a string by concatenating block index, previous block hash, nonce, timestamp and merkle root hash and then return the hash of the string formed.
27) Defining the user finder function which will be used for finding the public and private key associated with a particular user address.
28) This function will iterate over all the users and when there is match in the user address and the address passed in the function parameter then this function will return the public and private key associated with the address.
29) Creating a list which will store the blocks object and initialising the block index as 1 which will define the size of the blockchain.
30) Fetching the public and the private of from address using the user finder function.
31) Validating the transaction by using the validate function which will return either true or false.
32) If returned value from the validate function is true which means that the transaction is valid and the processing will start from step 33 and if the transaction is invalid than transaction invalid will be returned and the next transaction will start its processing.
33) Mining process will be started by the miner node using the mining function.
34) Mining function will return the nonce calculated to satisfy the difficulty level.
35) Merkle root hash will be calculated by using the address calculation function.
36) Utxo database will be appended with a entry having the to address of the transaction and the amount transferred by the sender.
37) Balance of the user which has initiated the transaction will be calculated using the balance calculation function.
38) After that all the utxos having the address as the from address will be deleted using utxo updation function and after that utxo database will be appended with a entry having the from address of the transaction and the remaining balance of the user (self transaction from a random address).
39) Constructing the block header and the block data.

40) Calling Block class object with parameters as block number, previous block hash, nonce, timestamp, current block hash, merkle root hash and the transactions.
41) Increasing the block number by 1.
42) Changing the value of previous block hash and updating it to the block hash calculated for the current block.
43) Appending the block constructed into the existing blockchain list.
44) Adding the miners benefits to the utxo database (mining reward and the transaction fees).
45) These above steps will be repeated for all the transactions in the transactions list.
46) At the end printing all the useful information on the console (utxo database, transactions, user balances, nonce and blockchain).

Various options explored:

- The implemented methodology uses the UTXO model for fetching the balance but another method which is based on the account was also explored. The account-based transaction model represents assets as balances within accounts, like bank accounts. Ethereum uses this transaction model. A transaction in the account-based model triggers nodes to decrement the balance of the sender's account and increment the balance of the receiver's account. To prevent replay attacks, each transaction in the account model has a nonce attached. A replay attack is when a payee broadcasts a fraudulent transaction in which they get paid a second time. If the fraudulent transaction were to be successful, the transaction would be executed a second time - it is replayed - and the sender would be charged twice the amount they wanted to transfer. To combat this behaviour, each account in Ethereum has a public viewable nonce that is incremented by one with each outgoing transaction. This prevents the same transaction being submitted to the network more than once.
- For digital signatures, the RSA algorithm is used, but there are other digital signature algorithms that are also available in Python, such as the elliptic curve digital signature algorithm and the digital signature scheme.
- UTXOs are implemented with some different logic. All the entries of a particular user will be deleted from the UTXO database if that user transfers some cryptocurrencies. Other approach to marking spent and unspent transactions were also explored during implementation.
- Each individual component in the implementation is carried out using objects and classes, but instead of that, simple data structures such as arrays, stacks, queues, etc. can also be used for simpler implementation.
- The entire programme is developed by considering the approach followed in Bitcoin, but how Ethereum is developed is also considered while developing the application.

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

➔ **Methods:**

- **RSA.generate():** This function is used to generate a private key using the RSA algorithm. Keys generated using this are used for digital signatures in the implementation. This function usually takes number of bits as the argument which will be used for deriving the sizes of public and private keys.

- **publicKey():** This function is used for deriving the public key from the private key derived from the generate function. The public keys are used for address derivation in the actual implementation of the bitcoin. This function will throw an error if the private key used is not appropriate.

- **sha256():** A family of hash algorithms also called as secure hash algorithms are primary used for hashing purposes. SHA256 is used for calculating the hashes while creating and verifying the digital signatures. This function is also used for mining in the code (nonce generation for satisfying the difficulty level).

- **hexDigest():** The actual digest is a really big number. It is conventionally represented as a sequence of hex digits, as we humans aren't very good at dealing with numbers with more than a handful of digits (and hex has the advantage that it reveals some types of binary patterns really well).

- **encrypt():** Digital signatures are created using this function. This function usually takes the data and the private keys for calculating the digital signatures. Validator and the mining nodes both make use of this function.

- **validate():** This function defines the validator nodes in the blockchain. The main aim of this function is to verify the digital signature and then checking for the validity of transaction. If the account balance of the user is less than that of the amount user wants to transfer then this function will return false, but if everything is validated then this function will return true.

- **decrypt():** Digital signatures are verified using this function. Validator and miner nodes both uses this function to verify the digital signature. This function makes use of the public key to decrypt the digital signature created using the corresponding private key.

- **mining():** This function defines the miner nodes in the blockchain. Function starts with the verification of digital signature and after that the process of calculating nonce is started. This process continues until a valid nonce that satisfies the difficulty level is not obtained. If function finds a valid nonce then it will be returned from the function.

- **utxo_updation():** Whenever a particular user makes a transaction this function will be called for updating that users account balance. Function first finds all the entries of a particular user and deletes it and at the end of the database it will append the remaining balance after transaction.

- **bal_calc():** This function is used to find the account balance of a particular user. This function iterates all the entries in the utxo database and then it will fetch all the entries having a particular user address. At the end it will add all the UTXO amount of a particular user. This function will return the calculated result.

- **address_calculation():** This function uses SHA256 algorithm to calculate the transaction hash. This function is called whenever a new transaction taken for validation.

- **block_hash_calculator():** This function also uses SHA256 algorithm to calculate the block hash. Previous block hash will be modified after execution of this function. This function will be called whenever a new block is added to the blockchain.

- **user_finder():** This function is used to fetch the public and private key of a particular user based on the user address. All the entries in the users table iterated and when the user address and the address passed as the parameter to this function is same the corresponding public and private key will be returned.

- **time():** The timestamp is one of the fields in the block header. This function is used to fetch the current UNIX time. This function will be called whenever a new block is added to the blockchain.

3. Explain the Importance of the approach followed by you

➔ 1) The UTXO based smart contracts are independent of language and allow UTXOs to develop unique consensus mechanisms.

2) With new addresses used for every UTXO transaction, it is impossible to track the transactions. This provides privacy and security.

3) It provides more flexibility than fiat currency.

4) It allows for the simpler parallelization of transactions in the smart contracts.

5) The UTXO model could support atomic swaps, hence enabling peer-to-peer crypto trades without the involvement of a third party. The atomic swap feature of UTXOs offers a better facility for direct cryptocurrency trades between user wallets.

6) Facility or parallel transaction processing reduces computation load on the blockchain networks.

Conclusion:- Understand various concepts related to the implementation of private blockchain cryptocurrency, such as the token data model, transactions, consensus, etc. Explored how bitcoin works internally in terms of transactions and blocks. Implemented a cryptocurrency with a UTXO-based token data model, randomly generated transactions and users, the SHA256 algorithm for hashing, and RSA for digital signatures. A different option for the token data model, i.e., the account-based model, was also explored while implementing the UTXO model, and understood the importance of UTXO over the account-based model.