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

Department of Computer Engineering

Batch:___A2_____ Roll No.:____1911020____

Experiment No. 2

Title: Creation of a private block chain cryptocurrency

Objective:

To understand and implement a private block chain cryptocurrency and understand the concepts used at the lower level that enable the functionalities and features of blockchain technology.

Expected Outcome of Experiment:

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

Books/ Journals/ Websites referred:

1. https://www.ijsr.net/get_abstract.php?paper_id=SR201215015012
2. https://ieeexplore.ieee.org.library.somaiya.edu/document/7906988
3. https://www.investopedia.com/how-to-make-a-cryptocurrency-5215343
4. https://readwrite.com/relationship-between-blockchain-and-cryptocurrency/
5. https://en.wikipedia.org/wiki/Bitcoin
6. https://en.wikipedia.org/wiki/Ethereum
7. https://www.forbes.com/advisor/in/investing/cryptocurrency/what-is-cryptocurrency-and-how-does-it-work/

Abstract: -

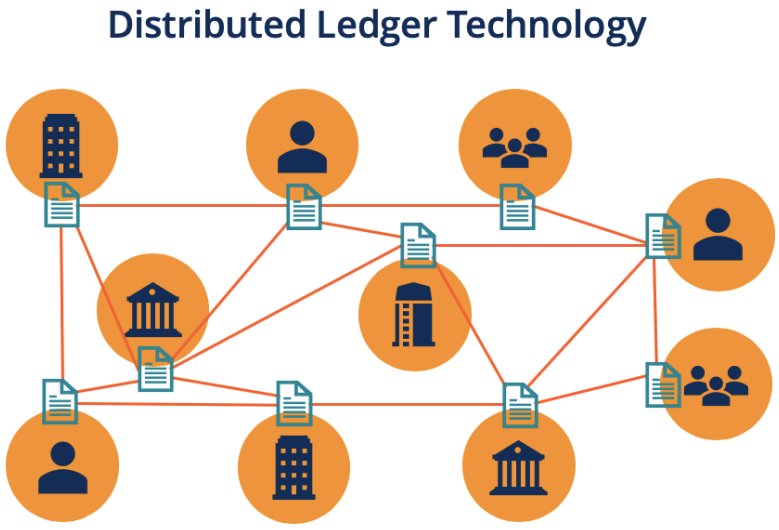
Cryptocurrencies are internet-based virtual currencies and exist without centralized regulating authorities. They are launched in the internet ecosystem and are used primarily outside of the traditional banking system. They are used for transfer and exchange of value over the internet. Cryptocurrencies have emerged as important financial software systems. They rely on a secure distributed ledger data structure and mining is an integral part of such systems. Mining adds records of past transactions to the distributed ledger known as Blockchain, allowing users to reach secure, robust consensus for each transaction. Mining also introduces wealth in the form of new units of currency. Cryptocurrencies lack a central authority to mediate transactions because they were designed as peer-to-peer systems. They rely on miners to validate transactions. Cryptocurrencies require strong, secure mining algorithms.

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.

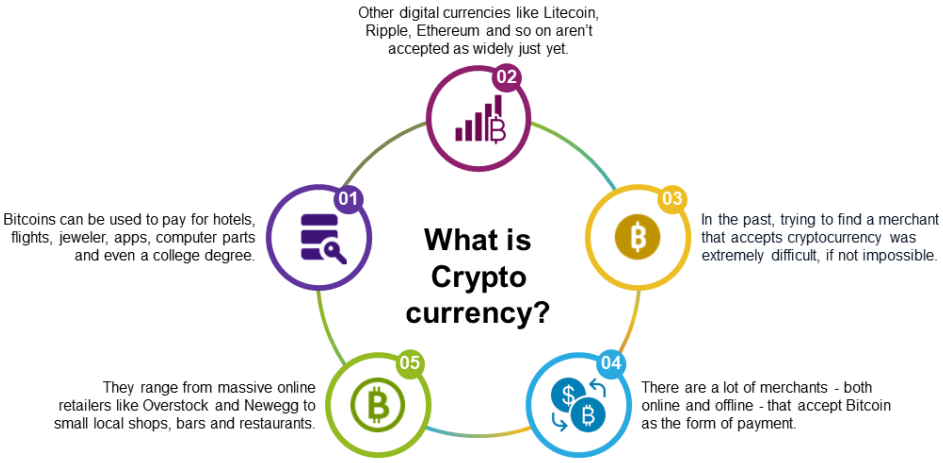
A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction 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.



Cryptocurrency:

A Cryptocurrency is a peer-to-peer digital exchange system in which cryptography is used to generate and distribute currency units. This process requires distributed verification of transactions without a central authority. Transaction verification confirms transaction amounts, and whether the payer owns the currency they are trying to spend while ensuring that currency units are not spent twice. This verification process is called *mining*. Cryptocurrencies use a variety of mining technologies, according to their particular requirements. For instance, certain Cryptocurrencies focus on restricting the number of transactions validated per unit time, while others concentrate on achieving fast, lightweight services. Some mining algorithms are deliberately memory intensive; others are computationally expensive. Some examples of cryptocurrency systems are as follows: Bitcoin, Litecoin, Peercoin, Ethereum, Ripple, Namecoin, Auroracoin, Blackcoin, Dash, Decred, and Permacoin. These Cryptocurrencies are the most interesting, widely used, and with the greatest capital and transaction rates.



General Blockchain Terminology:

- **Block**: a data structure containing transaction data.
- **Blockchain**: a public ledger of all transactions that have ever been executed. It consists of a distributed, chronological chain of blocks and constantly growing as *completed* blocks are added to it with a new set of records. Blocks comprise transactions and information from previous blocks. A unique linear path from the first block ever posted to the current block exists because every block includes the hash of the previous block.

- **Mining**: a required verification step for a Cryptocurrency transaction and for adding transaction records to the public ledger (the Blockchain). Mining also introduces new Cryptocurrency units in the system.
- **Hash**: a one-way function that takes data of any size as input and produces a fixed length output. Hash computation should be fast and easy, while reversing the process should be expensive and difficult. Reversal should require a brute force algorithm. Any change in the input should propagate through the entire output, so that outputs for similar input have no predictable similarity.
- **Nonce**: a number, usually chosen at random used once for a specific purpose then discarded. Nonce collisions, which happen when two randomly chosen nonces turn out to be the same, are ignored.
- **Fork**: a quantity generated when two blocks are created a few seconds apart. Forks are resolved by adding the block received first to the Blockchain. Subsequent Blocks are added to the included Block.

History and General Working Principles of Cryptocurrencies

The first fully implemented decentralized Cryptocurrency was Bitcoin, published by Nakamoto in 2008−09. Before this there were published articles about peer-to-peer currency systems but none were implemented. Following the success of Bitcoin, several others came into existence.

Chaum created an anonymous electronic money system called eCash in 1983. The key difference between eCash and Cryptocurrencies is that eCash was centralized (via banks). Software on the user's local computer stored money digitally, which was cryptographically signed by a bank.

PayPal is an Online Money Transfer System established in 1998. PayPal provides users with an account, which can be linked with bank accounts and credit cards, and users can pay someone or receive payment through the PayPal accounts. PayPal does not have a its own currency.

M-Pesa was established by Vodafone initially in Africa, which later spread to other continents. M-Pesa is a mobile, online payment system in which the user can deposit money into an account stored in their cell phones and send PIN-secured SMS texts to other users in order to send money.

All these online monetary systems were based on flat currencies, whereas a Cryptocurrency has its own currency.

Cryptocurrencies work functionally as follows:

- The user has a wallet with a generated address. This address acts as a public key.
- The wallet also contains a generated private key, which is used to sign transactions, proving ownership.
- The payer sends money to the payee's address, and signs it using the payer's private key.
- The transaction is verified by mining.

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.
- **No refund or cancellation policy:** If there is a dispute between concerning parties, or if someone mistakenly sends funds to a wrong wallet address, the coin cannot be retrieved by the sender. This can be used by many people to cheat others out of their money. Since there are no refunds, one can easily be created for a transaction whose product or services they never received.

Code:

Colab link:
https://colab.research.google.com/drive/1l2Q9HjN6oO2lw444gJEsPim661oYvu07?usp=sharing

Output:

```
__________USERS__________
0xa5c5b3b2eac4c4d5
0x96432480ed236472
0x322ba15873091320
0xb96a22ca513a746d



__________UTXO__________
0 | 0x322ba15873091320 - 18
1 | 0xa5c5b3b2eac4c4d5 - 14
2 | 0xb96a22ca513a746d - 10
3 | 0x96432480ed236472 - 29
4 | 0xb96a22ca513a746d - 23



__________________RANDOMNLY GENERATING
TRANSACTIONS_____________________________
Transaction digitally signed
New verified transaction :  0x322ba15873091320 -->
0xa5c5b3b2eac4c4d5 : 5 [Transaction fees : 0.05]
      0x322ba15873091320 --> 0x322ba15873091320 : 12.95
Transaction digitally signed
New verified transaction :  0x96432480ed236472 -->
0xa5c5b3b2eac4c4d5 : 5 [Transaction fees : 0.05]
      0x96432480ed236472 --> 0x96432480ed236472 : 23.95
Transaction digitally signed
New verified transaction :  0x96432480ed236472 -->
0x322ba15873091320 : 2 [Transaction fees : 0.02]
      0x96432480ed236472 --> 0x96432480ed236472 : 26.98
Transaction digitally signed
New verified transaction :  0x96432480ed236472 -->
0xa5c5b3b2eac4c4d5 : 5 [Transaction fees : 0.05]
      0x96432480ed236472 --> 0x96432480ed236472 : 23.95
Transaction digitally signed
New verified transaction :  0xa5c5b3b2eac4c4d5 -->
0x96432480ed236472 : 2 [Transaction fees : 0.02]
      0xa5c5b3b2eac4c4d5 --> 0xa5c5b3b2eac4c4d5 : 11.98
Transaction digitally signed
New verified transaction :  0xa5c5b3b2eac4c4d5 -->
0x322ba15873091320 : 2 [Transaction fees : 0.02]
```

```
      0xa5c5b3b2eac4c4d5 --> 0xa5c5b3b2eac4c4d5 : 11.98
_____________________________________________________________


_________________MINING STARTS_____________________________
Transaction selected by miner (0x322ba15873091320) :
0xa5c5b3b2eac4c4d5 --> 0x322ba15873091320 : 2 [Transaction fees :
0.02]
      0xa5c5b3b2eac4c4d5 --> 0xa5c5b3b2eac4c4d5 : 11.98
Transaction digital signature verified by miner


__________Blockchain__________
_________Block 0_________
Prev block hash : 00000000000000000000000000000000
Nonce : 195
Transaction hash :
d662b4843211798779ab6ef9fe6d2026d28f1347174aaaf4efbcd11408dde240
Timestamp : 1667848570.8690848
Miner address : 0x322ba15873091320
Block Hash :
00056c48576304143b50487e0a588df4d3555972f651b3d86b7dbbaaa1aeb4da
Transaction : 0xa5c5b3b2eac4c4d5 --> 0x322ba15873091320 : 2
[Transaction fees : 0.02]
      0xa5c5b3b2eac4c4d5 --> 0xa5c5b3b2eac4c4d5 : 11.98
_____________________


__________UTXO__________
0 | 0x322ba15873091320 - 18
2 | 0xb96a22ca513a746d - 10
3 | 0x96432480ed236472 - 29
4 | 0xb96a22ca513a746d - 23
15 | 0x322ba15873091320 - 2
16 | 0xa5c5b3b2eac4c4d5 - 11.98
17 | 0x322ba15873091320 - 0.02
18 | 0x322ba15873091320 - 8


_____________________________________________________________


_________________MINING STARTS_____________________________
Transaction selected by miner (0x96432480ed236472) :
0x96432480ed236472 --> 0x322ba15873091320 : 2 [Transaction fees :
0.02]
      0x96432480ed236472 --> 0x96432480ed236472 : 26.98
Transaction digital signature verified by miner


__________Blockchain__________
_________Block 0_________
Prev block hash : 00000000000000000000000000000000
Nonce : 195
```

```
Transaction hash :
d662b4843211798779ab6ef9fe6d2026d28f1347174aaaf4efbcd11408dde240
Timestamp : 1667848570.8690848
Miner address : 0x322ba15873091320
Block Hash :
00056c48576304143b50487e0a588df4d3555972f651b3d86b7dbbaaa1aeb4da
Transaction : 0xa5c5b3b2eac4c4d5 --> 0x322ba15873091320 : 2
[Transaction fees : 0.02]
      0xa5c5b3b2eac4c4d5 --> 0xa5c5b3b2eac4c4d5 : 11.98

_____________________
  |
  |
  |
  v

_________Block 1_________
Prev block hash :
00056c48576304143b50487e0a588df4d3555972f651b3d86b7dbbaaa1aeb4da
Nonce : 464
Transaction hash :
ac17d34116b5baf5e6a63deeeffa071cc201ee86055e6ea3f439613f057fc8b5
Timestamp : 1667848570.8749154
Miner address : 0x96432480ed236472
Block Hash :
00464a77bb42c41d8de0abbf3a07c2ca1c946d7edf46cfac58a7f383fd7509de
Transaction : 0x96432480ed236472 --> 0x322ba15873091320 : 2
[Transaction fees : 0.02]
      0x96432480ed236472 --> 0x96432480ed236472 : 26.98
_____________________


__________UTXO__________
0 | 0x322ba15873091320 - 18
1 | 0xa5c5b3b2eac4c4d5 - 14
2 | 0xb96a22ca513a746d - 10
4 | 0xb96a22ca513a746d - 23
9 | 0x322ba15873091320 - 2
10 | 0x96432480ed236472 - 26.98
19 | 0x96432480ed236472 - 0.02
20 | 0x96432480ed236472 - 8


____________________________________________________________


_________________MINING STARTS_____________________________
Transaction selected by miner (0xb96a22ca513a746d) :
0x322ba15873091320 --> 0xa5c5b3b2eac4c4d5 : 5 [Transaction fees :
0.05]
      0x322ba15873091320 --> 0x322ba15873091320 : 12.95
Transaction digital signature verified by miner


__________Blockchain__________
_________Block 0_________
```

```
Prev block hash : 00000000000000000000000000000000
Nonce : 195
Transaction hash :
d662b4843211798779ab6ef9fe6d2026d28f1347174aaaf4efbcd11408dde240
Timestamp : 1667848570.8690848
Miner address : 0x322ba15873091320
Block Hash :
00056c48576304143b50487e0a588df4d3555972f651b3d86b7dbbaaa1aeb4da
Transaction : 0xa5c5b3b2eac4c4d5 --> 0x322ba15873091320 : 2
[Transaction fees : 0.02]
      0xa5c5b3b2eac4c4d5 --> 0xa5c5b3b2eac4c4d5 : 11.98
_________________________
  |
  |
  |
  v

_________Block 1_________
Prev block hash :
00056c48576304143b50487e0a588df4d3555972f651b3d86b7dbbaaa1aeb4da
Nonce : 464
Transaction hash :
ac17d34116b5baf5e6a63deeeffa071cc201ee86055e6ea3f439613f057fc8b5
Timestamp : 1667848570.8749154
Miner address : 0x96432480ed236472
Block Hash :
00464a77bb42c41d8de0abbf3a07c2ca1c946d7edf46cfac58a7f383fd7509de
Transaction : 0x96432480ed236472 --> 0x322ba15873091320 : 2
[Transaction fees : 0.02]
      0x96432480ed236472 --> 0x96432480ed236472 : 26.98
_________________________
  |
  |
  |
  v

_________Block 2_________
Prev block hash :
00464a77bb42c41d8de0abbf3a07c2ca1c946d7edf46cfac58a7f383fd7509de
Nonce : 36
Transaction hash :
c7ff0dc6b5b8c4babe6ba7c69a43ace1addd0c4fb5daddec7854a61c5ed3b54e
Timestamp : 1667848570.8815835
Miner address : 0xb96a22ca513a746d
Block Hash :
008a74b72fe26631c22c77038a8bf3911b58b3db1761b10ffd2a15dbe0d57dcc
Transaction : 0x322ba15873091320 --> 0xa5c5b3b2eac4c4d5 : 5
[Transaction fees : 0.05]
      0x322ba15873091320 --> 0x322ba15873091320 : 12.95
_________________________


          UTXO
__________________________
1 | 0xa5c5b3b2eac4c4d5 - 14
2 | 0xb96a22ca513a746d - 10
3 | 0x96432480ed236472 - 29
```

```
4 | 0xb96a22ca513a746d - 23
5 | 0xa5c5b3b2eac4c4d5 - 5
6 | 0x322ba15873091320 - 12.95
21 | 0xb96a22ca513a746d - 0.05
22 | 0xb96a22ca513a746d - 8


_____________________________________________________


_________________MINING STARTS_____________________________
Transaction selected by miner (0x96432480ed236472) :
0xa5c5b3b2eac4c4d5 --> 0x96432480ed236472 : 2 [Transaction fees :
0.02]
      0xa5c5b3b2eac4c4d5 --> 0xa5c5b3b2eac4c4d5 : 11.98
Transaction digital signature verified by miner


__________Blockchain__________
_________Block 0_________
Prev block hash : 00000000000000000000000000000000
Nonce : 195
Transaction hash :
d662b48432117987 79ab6ef9fe6d2026d28f1347174aaaf4efbcd11408dde240
Timestamp : 1667848570.8690848
Miner address : 0x322ba15873091320
Block Hash :
00056c48576304143b50487e0a588df4d3555972f651b3d86b7dbbaaa1aeb4da
Transaction : 0xa5c5b3b2eac4c4d5 --> 0x322ba15873091320 : 2
[Transaction fees : 0.02]
      0xa5c5b3b2eac4c4d5 --> 0xa5c5b3b2eac4c4d5 : 11.98
_________________________
  |
  |
  |
  v

_________Block 1_________
Prev block hash :
00056c48576304143b50487e0a588df4d3555972f651b3d86b7dbbaaa1aeb4da
Nonce : 464
Transaction hash :
ac17d34116b5baf5e6a63deeeffa071cc201ee86055e6ea3f439613f057fc8b5
Timestamp : 1667848570.8749154
Miner address : 0x96432480ed236472
Block Hash :
00464a77bb42c41d8de0abbf3a07c2ca1c946d7edf46cfac58a7f383fd7509de
Transaction : 0x96432480ed236472 --> 0x322ba15873091320 : 2
[Transaction fees : 0.02]
      0x96432480ed236472 --> 0x96432480ed236472 : 26.98
_________________________
  |
  |
  |
  v
```

```
_________Block 2_________
Prev block hash :
00464a77bb42c41d8de0abbf3a07c2ca1c946d7edf46cfac58a7f383fd7509de
Nonce : 36
Transaction hash :
c7ff0dc6b5b8c4babe6ba7c69a43ace1addd0c4fb5daddec7854a61c5ed3b54e
Timestamp : 1667848570.8815835
Miner address : 0xb96a22ca513a746d
Block Hash :
008a74b72fe26631c22c77038a8bf3911b58b3db1761b10ffd2a15dbe0d57dcc
Transaction : 0x322ba15873091320 --> 0xa5c5b3b2eac4c4d5 : 5
[Transaction fees : 0.05]
      0x322ba15873091320 --> 0x322ba15873091320 : 12.95
_____________________
  |
  |
  |
  v

_________Block 3_________
Prev block hash :
008a74b72fe26631c22c77038a8bf3911b58b3db1761b10ffd2a15dbe0d57dcc
Nonce : 177
Transaction hash :
c4ab865a837db65fba0f691ef357929e411aa87f8b8036286b99f96bd893f1d7
Timestamp : 1667848570.8845437
Miner address : 0x96432480ed236472
Block Hash :
00125140f4951158d98b09292ef2677e971cbc978e666a9dcdf0871640f71411
Transaction : 0xa5c5b3b2eac4c4d5 --> 0x96432480ed236472 : 2
[Transaction fees : 0.02]
      0xa5c5b3b2eac4c4d5 --> 0xa5c5b3b2eac4c4d5 : 11.98
_____________________


__________UTXO__________
0 | 0x322ba15873091320 - 18
2 | 0xb96a22ca513a746d - 10
3 | 0x96432480ed236472 - 29
4 | 0xb96a22ca513a746d - 23
13 | 0x96432480ed236472 - 2
14 | 0xa5c5b3b2eac4c4d5 - 11.98
23 | 0x96432480ed236472 - 0.02
24 | 0x96432480ed236472 - 8


____________________________________________________


_________________MINING STARTS_____________________
Transaction selected by miner (0x96432480ed236472) :
0x96432480ed236472 --> 0xa5c5b3b2eac4c4d5 : 5 [Transaction fees :
0.05]
      0x96432480ed236472 --> 0x96432480ed236472 : 23.95
```

```
Transaction digital signature verified by miner


__________Blockchain__________
_________Block 0_________
Prev block hash : 00000000000000000000000000000000
Nonce : 195
Transaction hash :
d662b4843211798779ab6ef9fe6d2026d28f1347174aaaf4efbcd11408dde240
Timestamp : 1667848570.8690848
Miner address : 0x322ba15873091320
Block Hash :
00056c48576304143b50487e0a588df4d3555972f651b3d86b7dbbaaa1aeb4da
Transaction : 0xa5c5b3b2eac4c4d5 --> 0x322ba15873091320 : 2
[Transaction fees : 0.02]
      0xa5c5b3b2eac4c4d5 --> 0xa5c5b3b2eac4c4d5 : 11.98
_________________________
  |
  |
  |
  v

_________Block 1_________
Prev block hash :
00056c48576304143b50487e0a588df4d3555972f651b3d86b7dbbaaa1aeb4da
Nonce : 464
Transaction hash :
ac17d34116b5baf5e6a63deeeffa071cc201ee86055e6ea3f439613f057fc8b5
Timestamp : 1667848570.8749154
Miner address : 0x96432480ed236472
Block Hash :
00464a77bb42c41d8de0abbf3a07c2ca1c946d7edf46cfac58a7f383fd7509de
Transaction : 0x96432480ed236472 --> 0x322ba15873091320 : 2
[Transaction fees : 0.02]
      0x96432480ed236472 --> 0x96432480ed236472 : 26.98
_________________________
  |
  |
  |
  v

_________Block 2_________
Prev block hash :
00464a77bb42c41d8de0abbf3a07c2ca1c946d7edf46cfac58a7f383fd7509de
Nonce : 36
Transaction hash :
c7ff0dc6b5b8c4babe6ba7c69a43ace1addd0c4fb5daddec7854a61c5ed3b54e
Timestamp : 1667848570.8815835
Miner address : 0xb96a22ca513a746d
Block Hash :
008a74b72fe26631c22c77038a8bf3911b58b3db1761b10ffd2a15dbe0d57dcc
Transaction : 0x322ba15873091320 --> 0xa5c5b3b2eac4c4d5 : 5
[Transaction fees : 0.05]
      0x322ba15873091320 --> 0x322ba15873091320 : 12.95
_________________________
  |
```

```
   |
   |
   v

_________Block 3_________
Prev block hash :
008a74b72fe26631c22c77038a8bf3911b58b3db1761b10ffd2a15dbe0d57dcc
Nonce : 177
Transaction hash :
c4ab865a837db65fba0f691ef357929e411aa87f8b8036286b99f96bd893f1d7
Timestamp : 1667848570.8845437
Miner address : 0x96432480ed236472
Block Hash :
00125140f4951158d98b09292ef2677e971cbc978e666a9dcdf0871640f71411
Transaction : 0xa5c5b3b2eac4c4d5 --> 0x96432480ed236472 : 2
[Transaction fees : 0.02]
      0xa5c5b3b2eac4c4d5 --> 0xa5c5b3b2eac4c4d5 : 11.98
_________________________
   |
   |
   |
   v

_________Block 4_________
Prev block hash :
00125140f4951158d98b09292ef2677e971cbc978e666a9dcdf0871640f71411
Nonce : 68
Transaction hash :
5d1cea795e40be334e41e9df86d8d4a1bac8104aa6f6e415f867d900ddf1a995
Timestamp : 1667848570.8895414
Miner address : 0x96432480ed236472
Block Hash :
0080506c3a8509e2c1fb03237fdaf8f2bff2c5180c104c8777583be66a501a86
Transaction : 0x96432480ed236472 --> 0xa5c5b3b2eac4c4d5 : 5
[Transaction fees : 0.05]
      0x96432480ed236472 --> 0x96432480ed236472 : 23.95
_________________________


__________UTXO__________
0 | 0x322ba15873091320 - 18
1 | 0xa5c5b3b2eac4c4d5 - 14
2 | 0xb96a22ca513a746d - 10
4 | 0xb96a22ca513a746d - 23
11 | 0xa5c5b3b2eac4c4d5 - 5
12 | 0x96432480ed236472 - 23.95
25 | 0x96432480ed236472 - 0.05
26 | 0x96432480ed236472 - 8


____________________________________________________________
```

Implementation Details:

1. Enlist all the Steps followed and various options explored

- Firstly, we import the libraries that are utilised to build the private blockchain and support its functionalities.
- We then define globally the the gas fess percentage, the difficulty for implementation of proof of work in mining and the block reward given to the miner for adding a new block to the blockchain.
- We then define functions for displaying users, remaining utxos and the complete blockchain. The users, utxos, and the blockchain are implemented as lists of objects of user's, utxo's and blocks.
- Next we define the user class with the constructor generating a random public key and its corresponding private key using the rsa.newkeys function. The constructor also calculates the users address which is obtained by taking the first 16 characters after hashing the public key of the user.
- The users public key and address are public while the private key is private and cannot be accessed outside the class.
- The user class also has a sign function which accepts some data and then signs the hash digest of the data with the users private key. This is called the digital signature.
- The __str__ method of the user class just returns the users address
- Next we define the transactions class that is the blueprint for all the transactions. It has a constructor that takes the sender (object of User class) who sends the funds, receiver (object of User class) who is the beneficiary receiving the funds, amount that is to be transferred, and the list of users and remaining utxos.
- The transaction object has the attributes of the sender, receiver, amount, transaction fees calculated as the gas fees percent*amount, the senders input utxo's sum and ids calculated using the UTXO.getUserUTXOSum() function, the output utxos generated when the transaction is mined and added to a block of the blockchain and the digital signature of the hash of the transaction obtained using the sign function of the sender on the hash of the transaction string.

- The transaction is signed is also printed. The Transactions class also has a __str__ method which returns the input and output utxos as a string.
- We then define a static method in Transactions class to randomly generate transactions using the users and the existing utxos. Two distinct users are chosen from the users list and a random amount between 1 and 5 is chosen and the transaction fees is also calculated. A transaction object is instantiated with the sender, receiver and random amount. If the amount+transaction fees < total utxo balance of sender then the transaction is valid and returned else an error is thrown.
- Next we define a block class with a class variable as nblocks which is incremented for every new block created. The constructor accepts the utxo list, miner_address, transaction to be added to the block, and prev block hash.
- The nblocks is incremented by 1 in the constructor, and current timestamp is added into the block. The blockHeadstr function's output is hashed and stored as the block_hash.
- The __str__ functions includes the block_no, prev_block_hash, nonce, transaction_hash, timestamp, miner_address, block_hash and transaction as a structured string.
- The blockHeadstr() function includes the block_no, prev_block_hash, nonce, transaction_hash and timestamp as a structured string.
- Then the UTXO class is defined with the utxo_id as a static variable incremented for every new utxo. The constructor takes in the address and the amount and also updates the utxo_id.
- The __str__ method returns the id, address and amount of the utxo as a string.
- The getUserUTXOSum() method is defined as a static method that takes the address of the sender and returns the sum of all the utxo amounts of the utxos associated with the address.
- We then define the mining function that takes the blockchain, transaction_pool, users and utxo as input. A miner is selected from the users randomnly. If the transaction pool is empty a message is thrown and mining is stopped else a transaction is selected at random from the transaction pool. The transaction is hashed and its digital signature is decrypted using the public key. If the two

match the transaction is selected and a message of verification of digital signature is printed else the transaction is removed from the pool and the mining is stopped. The nonce is initialized to 0 and if the blockchain is not empty the block_hash of the prev block is sent to initialize the block object.

- Then the nonce is found for which the difficulty requirements i.e number of leading zeros after hash of data and nonce is satisfied.
- The new block's hash is computed and stored in the block object. The input utxos of the transaction are deleted and the output utxos appended with coinbase transactions of the block reward and transaction fees of the miner are added to the utxos list.
- The block is then appended to the blockchain and the blockchain and the utxos list are displayed.
- Initially random users are created with random utxo list for the users and random transactions in the transaction pool. The mining is done for 5 times and if the pool becomes empty new random transactions are generated and added to the pool.

Options Explored :

- Account based Non UTXO implementation of blockchain was explored but the UTXO based blockchain was implemented to mimic bitcoin.
- For digital signature various different algorithms like elliptic curve were explored but RSA was used for implementation.
- Various hashing algorithms were explored but sha-256 was used for implementation.
- Object oriented approach was used to modularize the implementation and keep objects instead of working with complicated lists.

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

Classes:

- **User :** The user class is used to create new user objects stored in a user list.
  - **Attributes :**
    - __privatekey : This attribute stores the private key of the user generated using the newkeys function.

- public_key : this attribute stores the public key of the user.
- address : This stores the address of the user generated from the hash of the public key of the user prefixed by “0x”.

▪ **Methods :**

- __init__() **:** It generates a public key and private key pair using the rsa.newkeys function. It also obtains the blockchain address of the user by taking the first 16 characters from the hexdigest of the hash of the users public key.
- sign(data) : This function signs the hash digest of the data using the private key of the user by using the rsa.encrypt function.
- __str__() : This function returns the users address as a string.

- **Transactions :** The transactions class is used to instantiate new transaction objects stored in the transaction_pool list.

▪ **Attributes :**

- sender : This attribute stores the user class object which sends the utxos.
- receiver : This attribute stores the user class object that receives the funds transferred.
- amount : Stores the amount of currency to be transferred from sender to reciever.
- transaction fees : Stores the transaction fees to be paid by the sender to the miner for adding the transaction in the block.
- input_utxo_sum : It is the total sum of the utxos associated with the sender obtained from the UTXO.getUserUTXOSum() method.
- input_utxo_ids : It is a list of ids of the utxos associated with the sender obtained from the UTXO.getUserUTXOSum() method.
- output_utxos : It is a list of the output utxos including the utxo to the reciever with the amount transferred and a self utxo to the sender of the remaining currency held by the sender.
- digital_signature : It is the signed hash of the transaction string, signed using the sender.sign().

▪ **Methods :**

- __init__() **:** It calculates the amount and the transaction_fees and also the output utxos to be created if the transaction is successfull.
- __str__() : This function returns the transaction string including the fund transfer and the transaction fees from sender to reciever and miner respectively.
- randomly_generate_transactions() : It generates new random transactions between distinct random users for a random amount between 1 and 5. If the transaction is valid a new transaction is created and added to the transaction_pool else an error is thrown.

- **Block :** The block class is used to instantiate new blocks stored in the blockchain list.
  - **Attributes :**
    - block no : This attribute stores the current block number.
    - miner_address : Stores the address of the user mining the current block.
    - transaction : Stores the object of the transaction class which is currently being added to the block to be mined.
    - Timestamp : stores the current unix timestamp.
    - prev_block_hash : stores the block hash of the previous block of the blockchain.
    - Nonce : stores the value of the nonce used to make the block hash digest satisfy the requirements of the proof of work difficulty of leading zeros.
    - transaction_hash : stores the hash of the transaction also known as the merkle tree root hash.
    - block_hash : stores the hash digest of the block header obtained from the blockHeadstr() function.
  - **Methods :**
    - __init__() **:** It the transaction and block hash of the current block and initializes the attributes of the block.
    - __str__() : This function returns the block string including the block header fields and the transaction.

- blockHeadstr() : This function returns the block header in a string format. It includes the block_no, prev_block_hash, nonce, transaction_hash and the timestamp.

- **UTXO :** The utxo class is used to create new UTXO tokens.
  - **Attributes :**
    - address: This attribute stores the address of the user the utxo belongs to.
    - amount : This attribute stores the amount of cryptocurrency held by the utxo.
    - Id : Stores the id of the current utxo.
  - **Methods :**
    - __init__() **:** It initialises the attributes of the class and increments the static variable utxo_id by 1.
    - __str__() : This function returns the utxo in string format.
    - getUserUTXOSum() : This function returns the sum and ids of all the utxos associated with the user address provided as parameter..

Methods:

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

- **decrypt():** Digital signatures are verified using this function. Miner nodes 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():** the mining function that takes the blockchain, transaction_pool, users and utxo as input. A miner is selected from the users randomly. If the transaction pool is empty a message is thrown and mining is stopped else a transaction is selected at random from the transaction pool. The transaction is hashed and its digital signature is decrypted using the public key. If the two match the transaction is selected and a message of verification of digital signature is printed else the transaction is removed from the pool and the mining is stopped. The nonce is initialized to 0 and if the blockchain is not empty the block_hash of the prev block is sent to initialize the block object. Then the nonce is found for which the difficulty requirements i.e. number of leading zeros after hash of data and nonce is satisfied. The new block's hash is computed and stored in the block object. The input utxos of the transaction are deleted and the output utxos appended with coinbase transactions of the block reward and transaction fees of the miner are added to the utxos list. The block is then appended to the blockchain and the blockchain and the utxos list are displayed.

3. Explain the Importance of the approach followed by you.

The approach followed implements a private blockchain with all its features including cryptography and game theory. The approach follows a UTXO based system which allows users to track ownership of portions of cryptocurrency with the anonymity of the user maintained with the public addresses visible to all users. The approach implemented is very similar to the approach followed by bitcoin.

Conclusion:-

Thus we have understood the concepts required for building a private blockchain implementation similar to bitcoin with concepts like hashing, digital signature, UTXO tokens, and proof of work.