**Topic:** Blockchain and Cryptocurrency

**Members:** Vishesh Bhandare-2011020

Hrishikesh Ghanti-2011049

**Introduction**

The goal is to build a cryptocurrency using blockchain technology which can be used for exchanges across different decentralized platforms. This project will serve as a demonstration for implementing cryptocurrency and its mining using Hash Cryptography (SHA256), Immutable Ledger and a distributed peer-to-peer network.

A Cryptocurrency can be defined as a digital currency relying on encryption to generate new units and confirm the transactions. It has all the functions of a currency with the difference of running outside of a single centralized platform, such as a bank. These cryptocurrency have to be maintained using a single immutable ledger using the blockchain. Cryptocurrency mining is done in order to verify the ledger where all the nodes (peers) connected on the network use standard consensus protocols for verifying various transactions carried out by the users.

Upon completion the project will successfully simulate the working of Bitcoin cryptocurrency, following all its consensus protocols. Different users will anonymously join the network and start mining the transactions and after successfully verifying the ledger they will be rewarded with new coins. This is called as proof-of-work (POW).

**Scope**

* Generate user’s public and private key to authenticate and perform transactions
* Allow peers to join network and start mining the cryptocurrency
* Generate new coins after every successful verification of transactions
* Users can view all the transactions recorded in the blockchain
* Every node must have the same replica of the block.
* Provide encryption (SHA-256) security for all transactions and user data.

**Technologies**

Front-End: HTML, CSS, Bootstrap, javascript

Back-End: Python

Framework: Flask

Encryption: SHA-256 Cryptography.

**Bitcoin Blockchain Regulations**

**Step 1. Decide on a Consensus Mechanism**

A [consensus mechanism](https://www.sofi.com/learn/content/blockchain-consensus-mechanism/) is the protocol that determines whether or not the network will consider a particular transaction. All the nodes have to confirm a transaction for it to go through. This is also known as “achieving consensus.” You will need a mechanism to determine how the nodes will go about doing this.

The first consensus mechanism was Bitcoin’s proof-of-work. [Proof-of-Stake](https://www.sofi.com/learn/content/proof-of-stake-explained/) is another popular consensus mechanism. There are many others as well.

**Step 2. Choose a Blockchain**

This goes back to the three methods mentioned earlier. A coin or token needs a place to live, and deciding in which blockchain environment the coin will exist is a crucial step. The choice will depend on your level of technical skill, your comfort level, and your project goals.

**Step 3. Create the Nodes**

Nodes are the backbone of any distributed ledger technology (DLT), including blockchains. As a cryptocurrency creator, you must determine how your nodes will function. Do they want the blockchain to be permissioned or permission less? What would the hardware details look like? How will hosting work?

**Step 4. Build the Blockchain Architecture**

Before launching the coin, developers should be 100% certain about all the [functionality of the blockchain](https://www.sofi.com/learn/content/what-is-blockchain-technology/) and the design of its nodes. Once the mainnet has launched, there’s no going back, and many things cannot be changed. That’s why it’s common practice to test things out on a testnet beforehand. This could include simple things like the cryptocurrency’s address format as well as more complex things like integrating the inter-blockchain communication (IBC) protocol to allow the blockchain to communicate with other blockchains.

**Step 5. Integrate APIs**

Not all platforms provide application programming interfaces (APIs). Making sure that a newly created cryptocurrency has APIs could help make it stand out and increase adoption. There are also some third-party blockchain API providers who can help with this step.

**Step 6. Design the Interface**

There’s little point in creating a cryptocurrency if people find it too difficult to use. The web servers and file transfer protocol (FTP) servers should be up-to-date and the programming on both the front and backends should be done with future developer updates in mind.

**Step 7. Make the Cryptocurrency Legal**

Failing to consider this last step led to trouble for many who initiated or promoted ICOs back in 2017 and 2018. At that time, cryptocurrency was in a kind of legal grey area, and they may not have realized that creating or promoting new coins could result in fines or criminal charges depending on the circumstances. Before launching a new coin, it might be a good idea to research the laws and regulations surrounding securities offerings and related topics. Given the complexity of the issues and their regular updates, you might consider hiring a lawyer with expertise in the area to help guide you through this step.