Coding Your Crypto with Ethereum

K Kiruba and R Selvaganapathy

June 12, 2022

Coding Your Crypto with Ethereum

Kiruba.K[1], Selvaganapathy.R[2]
Assistant Professor[1], UGScholar[2]
Department of Computer Science and Engineering
IFET College of Engineering, Villupuram
kirubadeepiit@gmail.com[1], selvaganapathy098@gmail.com[2]

Abstract*-Blockchain technology, which is used by cryptocurrencies such as Bitcoin and Ethereum, is recognized for delivering considerable security benefits. However, Bitcoin and Ethereum do not end there. To authenticate users, they employ digital signatures. A digital signature makes significant use of cryptography. It consists of two types of keys: public and private. A Bitcoin user has a bitcoin wallet, and the public key is the address of that wallet. Anyone wishing to send Bitcoin should do so at this address. Blockchain is the process of storing information that makes it difficult or impossible to change, hack, or fool the system. In this project, we will create our cryptocurrency (a crypto token) that fulfills the ERC 20 standard and can be exchanged and sold in a crowd sale on the Ethereum network. Token attributes such as token transfer, the total amount of tokens, and so on are defined by the ERC 20 standard. The operation of the tokens will be governed and regulated by smart contracts built with Solidity. Tokens are created using a test-driven process. The term "test-driven" refers to the creation of test cases before the construction of smart contracts.

Keywords: Blockchain, Cryptocurrency, Bitcoin, Crypto Tokens, Ethereum, ERC, Solidity, Smart Contracts

I. INTRODUCTION

Blockchain technology has gone a long way since Satoshi Nakamoto's first idea was released in the Bitcoin white paper in 2008. The terms "bitcoin," "blockchain," and "cryptocurrency" are all over the place. Companies and governments have begun to adopt blockchain technology in earnest and will continue to do so soon. Since its inception, blockchain has contained both a social promise and new technology. Blockchains were first presented as a solution for Bitcoin's monetary record-keeping system but are now utilized to hold the records of many sorts of applications.[1] The bitcoin business has increased quickly. This policy enables businesses to generate funds without the participation of private investors and to exchange without the need to be posted on the mainboard. The virtual currency economy's broad range of tokens includes well-known assets such as Bitcoin, Tether, Solana, Avalanche, Litecoin, Ripple, Chainlink, Monero, Hedera, and Ethereum as well as many more unknown cryptocurrencies.[2] Vitalik Buterin, a cryptocurrency analyst and software developer, introduced Ethereum in 2013. The initial creation discharge occurred in 2015. Ethereum is a blockchain implementation that is open-source, public, and decentralized. Ethereum gained popularity because of the features of its smart contracts. Engineers may build their smart contracts and execute them on the blockchain stage to make the most of the blockchain's varied capabilities. As previously stated, Bitcoin makes use of blockchain technology to facilitate payments using bitcoins as a currency. Bitcoin also has a programming language, which allows you to write small programs.[3] Cryptos are digital payments platforms that use digital "tokens" which are symbolized by ledger accounts within the platform. The name "crypto" indicates the encrypted data and encryption algorithms used only to safeguard such data, which include elliptical curve encoding, asymmetric key combinations, and hashing algorithms. As part of this paper, we will establish our cryptocurrency (a crypto token) that meets the ERC 20 standard on the Ethereum blockchain and can be transferred and sold in a crowd sale. The ERC 20 standard defines token properties such as token transfer, the total quantity of tokens, and so on.

II. EXISTING SYSTEM

Banks that market and distribute IPOs, along with dealers who advise customers wishing to buy stocks, all seem to be members of the Ethereum - based IPO. These enterprises' user interfaces are their own web pages, with the associated cloud services acting as users in the Fabric blockchain network. When a financial institution manager posts the latest IPO on the company's website, the web server notifies its colleagues, who then record the IPO's information on the blockchain. Investors can then log in to their cash accounts and make purchases for shares in the impending IPO. Investors make orders by describing a graph about how many stocks they are prepared to buy for each price bracket. The statistic is then distributed to all partners by the investor's web server, which encodes each partner's contribution with its digital certificate. Also, it encodes the whole transaction with something like a private key that the user may use to receive the transaction from the website later. [4] An initial public offering (IPO) is the process through which a private corporation offers crypto assets from its business to the public in new issuance. The method allows a cryptocurrency firm to receive funds from public investors, but it must adhere to laws that require increased disclosures and openness. A corporation is deemed private before an IPO and is held by a small number of stakeholders. Early investors like founders, the founders' family, and friends, or venture capitalists who offer to fund firms with strong growth potential are examples of stakeholders. An IPO is a significant step for any company, and it is seen as a regulatory milestone for enterprises in the cryptocurrency field. Because cryptocurrencies were first perceived as frauds or get-rich-quick schemes, organizations working with cryptocurrency were viewed as fraudulent projects. To launch an IPO, a cryptocurrency firm must work with underwriters or investment banks, who are companies that analyze and accept risks in return for a fee, to bring its coins to the public eye. Underwriting is the process through which an investment bank (the underwriter) acts as a middleman between the issuing firm and the public to help the issuing firm sell its initial batch of coins. Centralized Online Real-time Exchange (CORE) is an abbreviation that refers to Centralized Online Real-time Exchange. A central authority that combines and links multiple banking operations and procedures across banking institutions seems to be the CORE (Centralized Online Real-time Exchange) banking solution. A centralized banking system helps banks to streamline client onboarding, account administration, payment processing, and loan distribution procedures. Other possible advantages of centralized infrastructure in financial institutions include better data management, lower setup costs, and a higher likelihood of preserving data integrity owing to the availability of a single data record. Centralized architecture is vital in the preservation of banking services since it allows such institutions to significantly increase and expand their operations and profit base. [5]

III. PROPOSED SYSTEM

Cryptocurrency coins are digital currencies created on another stock's network. A blockchain is a distributed database that stores information in linked blocks. This information can take the shape of transaction records or full-fledged software that runs on the blockchain, known as smart contracts. For example, once a cryptocurrency's transactions are confirmed, they are bundled into a block, which is subsequently added to the blockchain. Every cryptocurrency is founded on a blockchain. If a cryptocurrency does not have its blockchain and instead uses the blockchain of another cryptocurrency, then it is classified as a token. Tokens enable developers to establish a coin without having to build a blockchain for it. This is significant because it accelerates, simplifies, and reduces the cost of generating cryptocurrencies. Blockchain development is a major technological task for developers who wish to create their cryptocurrency. A blockchain must be able to execute transactions fast and cheaply, and it must be resistant to assaults so that hackers cannot steal cryptocurrency. Building the blockchain is also not the end of the process. Every ICO (Initial Coin Offering) starts with a white paper, which is equivalent to a brochure in that it describes the concept and the shareholder rights. A min and max number of tokens must be registered for the operation to go live, according to the white paper. The tokens are usually bought using Bitcoin or Ether. On a blockchain, the provider constructs a smart contract. The smart contract ensures the success of the ICO. The virtual currency is immediately sent to the bank's wallet and the tokens are enrolled in the users' wallets if the minimum number of tokens is satisfied. The smart contract immediately returns the cryptocurrency to the receiver's wallet if the minimum number is not fulfilled. An ICO serves two purposes: it may potentially be used to generate a new virtual currency or to support a project. Considering these two objectives, the assessment of ICOs may differ. [6] A company can start an ICO to raise funds for the development of a new currency, software, or product. The types of ICOs available will vary based on these two objectives. Prospective buyers can purchase a new crypto token from the company through an initial coin offering. This token might be beneficial in relation to the company and its products, or it could simply reflect a stake in the organization or project. An initial coin offering (ICO) is a complicated method that necessitates a high level of technical, financial, and legal competence. The basic concept behind initial coin offerings is to leverage blockchain technology's decentralized system to generate capital in ways that are compatible with the demands of numerous stakeholders. Every initial coin offering (ICO) starts with a bank's idea of raising capital. The next step in the initial coin offering process is token creation. The tokens are both exchangeable and transferable. With exception of shares, tokens seldom provide an ownership stake in a company. Rather, most of the tokens give their holders a piece of a corporation's good or service. On various blockchain technology, tokens are created. Token generation is a relatively simple method since a company does not have to create the software from start, as is the scenario with the production of a new currency. Typically, a company will launch a marketing campaign to attract potential shareholders at the same moment. It should be emphasized that most initiatives are run digitally in the way to attain the largest number of potential stakeholders. However, certain well-known digital sites, like Google and Facebook, have recently made it illegal to advertise ICOs. The tokens are given access to traders when they are created. It's possible that the offering will be separated into many rounds. The company may then use the ICO revenues to develop a new product in the market, while shareholders may either use the tokens they acquired to benefit from this product or wait for the token's value to rise. Crypto tokens are valuable assets because they are cryptocurrencies. They are normally transferable, tradeable, buyable, and sellable, and are held in blockchain wallets. A blockchain wallet is a software or hardware device that stores bitcoin. Transactions involving a crypto token are carried out on the blockchain that it employs. For example, if it's an ERC-20 token generated on Ethereum, all transactions for that token will be handled by the Ethereum blockchain. Tokens can be used to make investments, hold wealth, or make transactions.

The Ethereum - based specification guarantees that a token is suitable for the following usage cases:

- ❖ Transferring tokens from one wallet to another (wallet transfers).
- ❖ Using bitcoin platforms to purchase and sell.
- ❖ Buying tokens from a crowd-sale (ICO).

IV. ARCHITECTURE OF PROPOSED SYSTEM

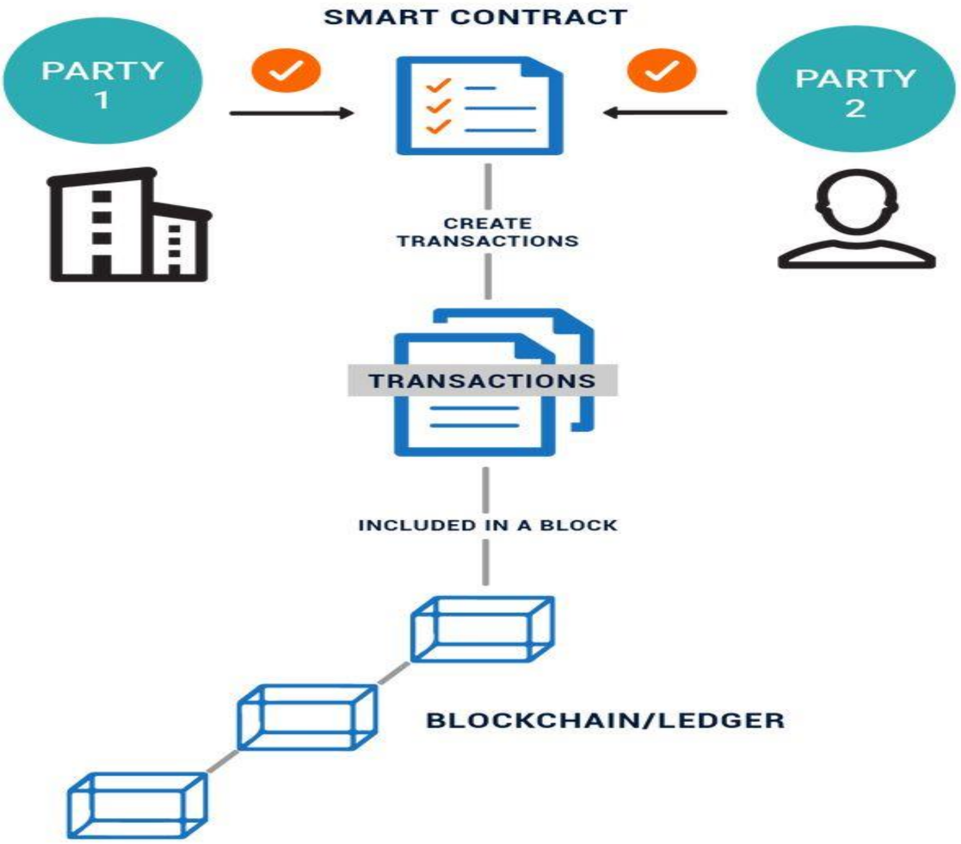


Fig 5.1 Architecture of Proposed System

IV. MODULES OF PROPOSED SYSTEM

A. *Token Smart Contract*:

Token formation events, token launches, security token offering (STO), and, most popularly, initial coin offering (ICO) are all terms used to describe the emerging phenomenon of trading crypto tokens here on the blockchain network. STOs indicate a far more established and regulated type of TS in which security tokens are issued, although ICOs have already been associated with the issuance of cryptocurrencies. We will use the phrase "token sale" in the following since it is not associated with any token type. The issuing entity in a TS creates cryptographic tokens that investors can purchase. The acquisition is stored on the blockchain, a decentralized and unchangeable global database. New assets of payments are only uploaded to the blockchain network once users have verified their validity through a general agreement method. Miners compete to answer a hashing algorithm (e.g., SHA-256) to accept transactions to the blockchain for which they have been compensated in a most common consensus procedure, known as concrete evidence. To enforce and execute a TS, smart contracts are required. A smart contract seems to be a piece of code recorded on the blockchain. It sets the guidelines for multiple parties to communicate. If the predefined circumstances are satisfied, the terms expressed in a smart contract are immediately performed. In the event of a TS, these restrictions apply to parameters like token price and sale length. Most of the Ethereum blockchain system has been used as a foundation for TSs (Buterin 2014). Ethereum, unlike the Bitcoin network, enables (quasi) Full accurate smart contracts. Financial institutions employ smart contracts to create (also called minting) and issue tokens that have a certain set of characteristics. When the Transaction is online, the smart contract becomes operational and can collect capital from depositors, most commonly in the form of cryptocurrencies like bitcoins or Ethereum. Smart contracts release a corresponding amount of coins to the buyer and send the money to the bank's wallet when this cash is received. These payments are processed by producers and stored on a blockchain. Holders can exchange the tokens on cryptocurrency platforms like Coinbase, Binance, Poloniex, or Kraken. [7]

Smart contracts provide the following advantages:

- There is no need for an intermediary.
- Accuracy is extremely high,
- reducing execution risk.
- It supports business and operational modes; and
- The cost is very cheap.[8]

B. *Sending Erc-20 Tokens*

The first thing you should know is that all Ethereum wallet addresses are ERC-20 token compliant. While this is a given, it is your wallet provider's responsibility to grant you access to your ERC-20 token balance. In other words, while certain wallet providers accept Ethereum addresses, you may not be able to see ERC-20 tokens linked with the address.

It is as simple as typing or copying the recipient's Ethereum wallet address to send ERC-20 tokens. You may transmit your ERC-20 tokens from two sources: a wallet from your centralized exchange (Binance, Coinbase, etc.) and a software wallet, commonly known as a hot wallet (Metamask, Trust Wallet, etc). Gas costs are an important factor to consider while transmitting ERC-20 tokens. These are transaction fees paid by users to miners for their transactions to be included in the blockchain. Gas prices will rise during peak hours when numerous users are transacting on the Ethereum network. Users may look up suggested gas prices on websites such as Eth Gas Station.

C. *Receive An Erc-20 Token*

It is best to check the compatibility of wallets ahead of time. Make sure your wallet not only supports ERC-20 tokens but also specifies the precise token you expect to receive, especially if you intend to receive airdrops. Airdropped tokens are often obscure digital assets that have yet to be listed on exchanges. If this is true, such coins are unlikely to be supported by exchange wallet addresses.

MyEtherWallet (MEW) and MetaMask are the preferred wallets for ERC-20 tokens. Whatever the ERC-20 token is, you may be confident that it is available through these two wallets.

Before you establish an account with any of these two ETH wallets, keep in mind that they are self-custody wallets. As a result, they will keep your private keys on your devices and require you to write down and save your seed phrase. When you lose access to your wallet or forget your password, you must input a seed phrase, which is a set of 12 random phrases.

D. Buying Erc-20 Token

To start with, the token smart contract keeps a record of a few basic token attributes. It maintains a record of the term "My Token," the sign used on a cryptocurrency exchange, and the overall sum of tokens, for example. Also, it keeps a record of who holds "My Token," as well as how much people paid for it. ERC-20 tokens may be moved from one bank to another as transactions, just like every other cryptocurrency. They can also be acquired through a crowd sale, such as an initial coin offering (ICO), which we shall discuss in the following section. A cryptocurrency exchange may also be used to buy and sell them. Tokens based on the ERC-20 standard can be delivered in several ways. Holding a crowd sale, also known as an initial coin offering, is a common strategy (ICO). Public sales are a way for a company to raise funding by issuing an ERC-20 token that traders can buy using Ether. When a crowd sale occurs, the company earns liquid funds in the form of Ether from the buyers, as well as an allocated number of the ERC-20 tokens acquired in the crowd sale. An investor must first create an account on the Ethereum Blockchain to participate in the public sale. This payment contains a bitcoin address for storing Ether and ERC-20 tokens purchased during the public sale. The investor must go to a website that connects to a smart contract to participate in the public sale. The smart contract governs all the rules that regulate how the public auction operates. When an investor purchases tokens on the public sale site, they transmit Ether from their account to a smart contract, which instantly transfers the tokens to their account.

E. End Sale

The token's price is determined by the smart contract, which also governs how the public auction is conducted. Crowd sales come in a variety of sizes and forms. Pre-ICO, ICO, and ICO Bonus are examples of different phases or stages. Almost all these levels might appear at any time and behave in a variety of ways. They can also use whitelists to limit which investors are allowed to buy tokens. They can however reserve a specific number of tokens for the public auction that will never be sold. These funds are usually reserved for members of the company's management team, namely the owners and consultants. These reserves might be in the form of a set number of tokens or a percentage of the total quantity of tokens. When a crowd sale ends, an administrator can close it down. All allocated tokens will now be handed to the appropriate accounts at that point, and the public sale will now be declared complete.

VI. SOFTWARE USED:

1. NODE PACKAGE MANAGER:

Node.js is now a free and open-source cross-platform software implementation for developing server-side and core capabilities. Node.js applications are developed using JavaScript and execute on the Node.js environment on Operating System, Microsoft Windows, and Ubuntu. Node.js also includes a wide collection of JavaScript libraries, which makes developing web-based applications with it much easier. It may also be used with Node Package Manager to install additional packages (NPM).

INSTALLATION: You may either download it straight from the NodeJS website or use PowerShell to install it. [8]

2. **TRUFFLE FRAMEWORK**:

The second prerequisite is the Truffle Framework, which enables us to build decentralized applications on the Ethereum platform. It includes a suite of devices that enable everyone to develop smart contacts by using a Solidity programming language. Also, it enables everyone to use blockchain to evaluate and implement smart contracts. Also, it provides a location for us to work on our client-side application**.**

3. GANACHE:

Ganache, a localized in-memory blockchain, will be the next dependent. Ganache may be downloaded from the Truffle Framework portal and installed. It can provide us with 10 exchange rates with Ethereum credentials on our local blockchain. Each user comes with 100 bogus ethers.

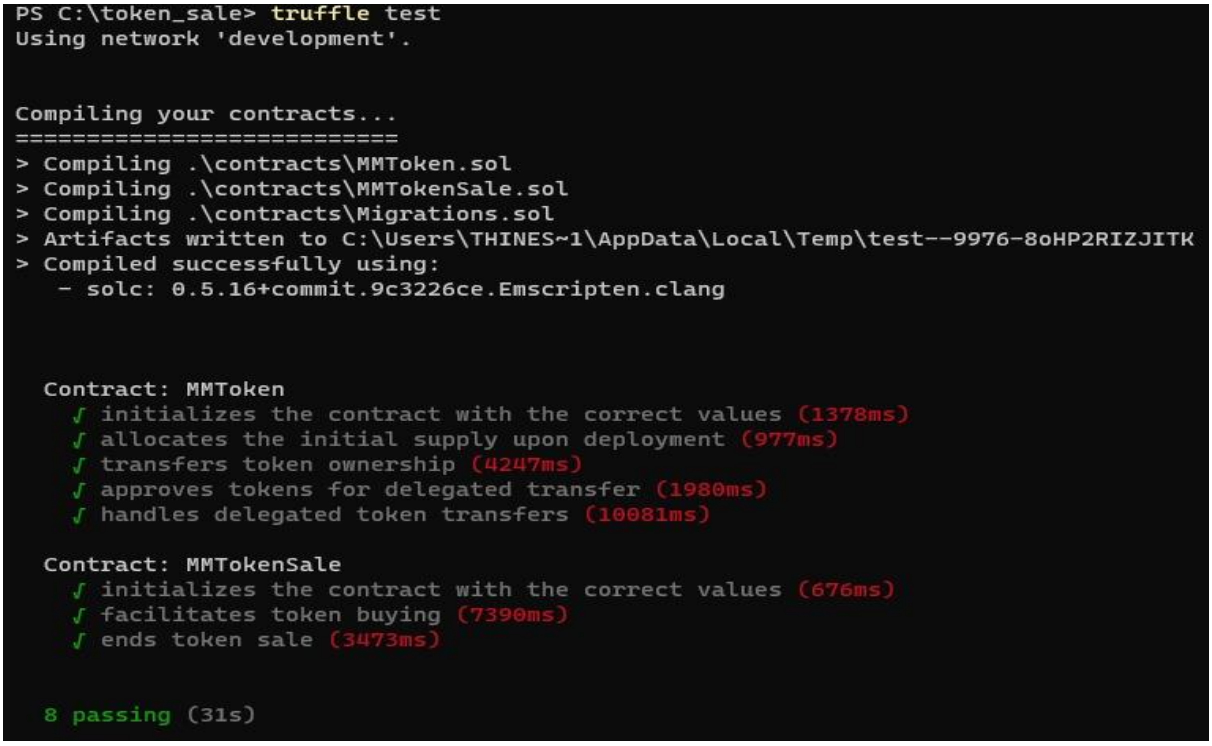
4. **METAMASK**:

The Metamask extension for Google Chrome is the next need. Users must link to the blockchain to use it. By using the Ethereum smart contracts, we'll need to download a specific browser extension. Metamask comes to the rescue in this situation. With our membership, we'll be able to link to our localized Ethereum blockchain and communicate with our smart contract.

Because we'll be utilizing the Metamask Chrome extension, you'll now have to download and install the Google Chrome Web browser if you don't know it exists. To set up Metamask, go to the Google Chrome online store and look for the Metamask Chrome extension. Make sure it's enabled in your selection of extensions after you've launched it. When it's enabled, the fox icon will appear in the upper right-hand corner of your Chrome Web browser.

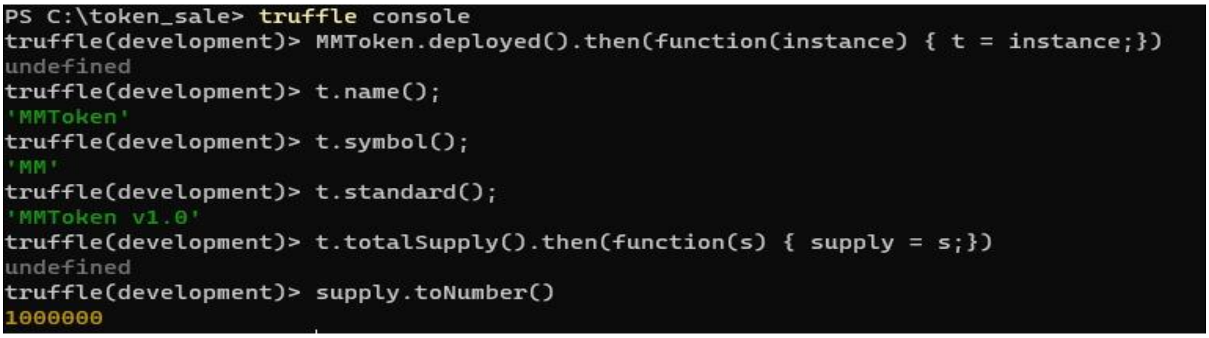
INSTALLATION: To set up a metamask, go on to the chrome browser store and look for the metamask plug-in, then install it. Once you have installed metamask, go to your chrome extension and confirm that metamask is activated.[9]

VII. RESULTS



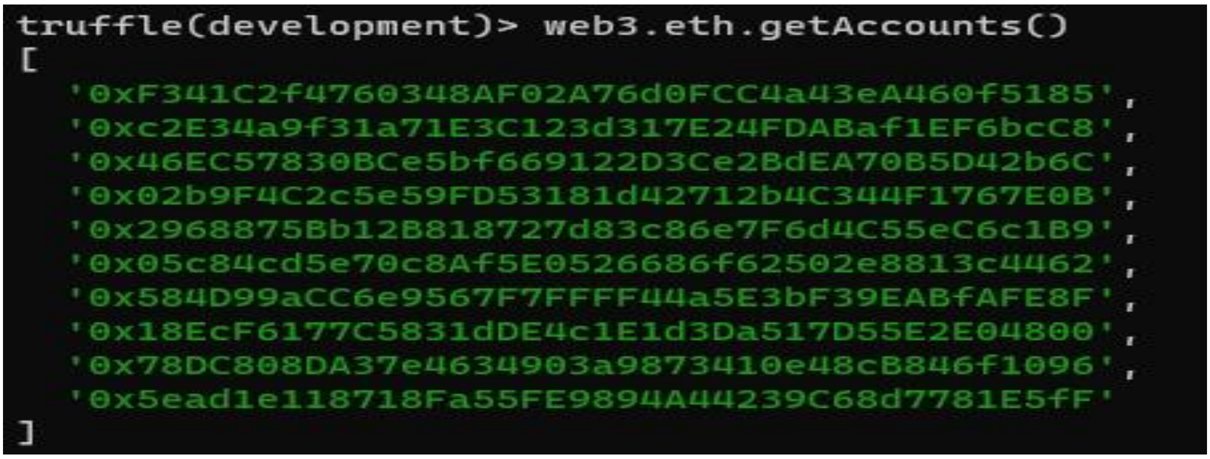
```
PS C:\token_sale> truffle test
Using network 'development'.


Compiling your contracts...
===========================
> Compiling .\contracts\MMToken.sol
> Compiling .\contracts\MMTokenSale.sol
> Compiling .\contracts\Migrations.sol
> Artifacts written to C:\Users\THINES~1\AppData\Local\Temp\test--9976-8oHP2RIZJITK
> Compiled successfully using:
   - solc: 0.5.16+commit.9c3226ce.Emscripten.clang



  Contract: MMToken
    √ initializes the contract with the correct values (1378ms)
    √ allocates the initial supply upon deployment (977ms)
    √ transfers token ownership (4247ms)
    √ approves tokens for delegated transfer (1980ms)
    √ handles delegated token transfers (10081ms)

  Contract: MMTokenSale
    √ initializes the contract with the correct values (676ms)
    √ facilitates token buying (7390ms)
    √ ends token sale (3473ms)


  8 passing (31s)
```

Fig 7.1 Output Screenshot-1



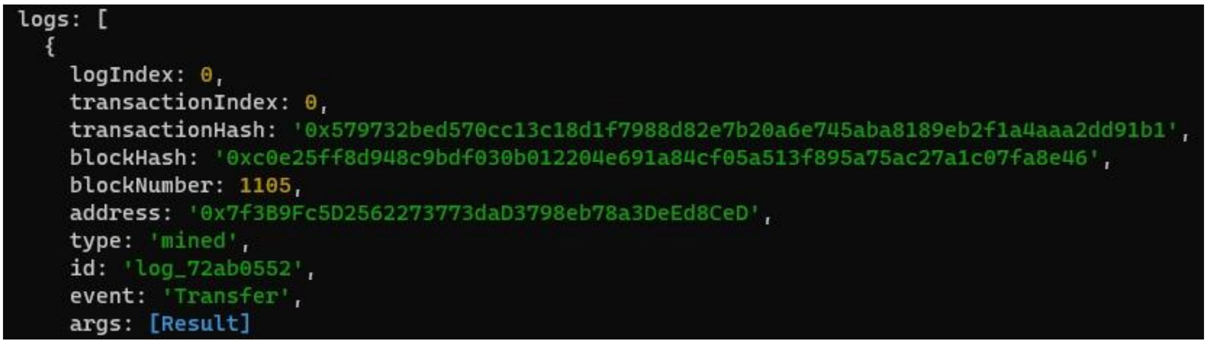
```
PS C:\token_sale> truffle console
truffle(development)> MMToken.deployed().then(function(instance) { t = instance;})
undefined
truffle(development)> t.name();
'MMToken'
truffle(development)> t.symbol();
'MM'
truffle(development)> t.standard();
'MMToken v1.0'
truffle(development)> t.totalSupply().then(function(s) { supply = s;})
undefined
truffle(development)> supply.toNumber()
1000000
```

Fig 7.2 Output Screenshot-2



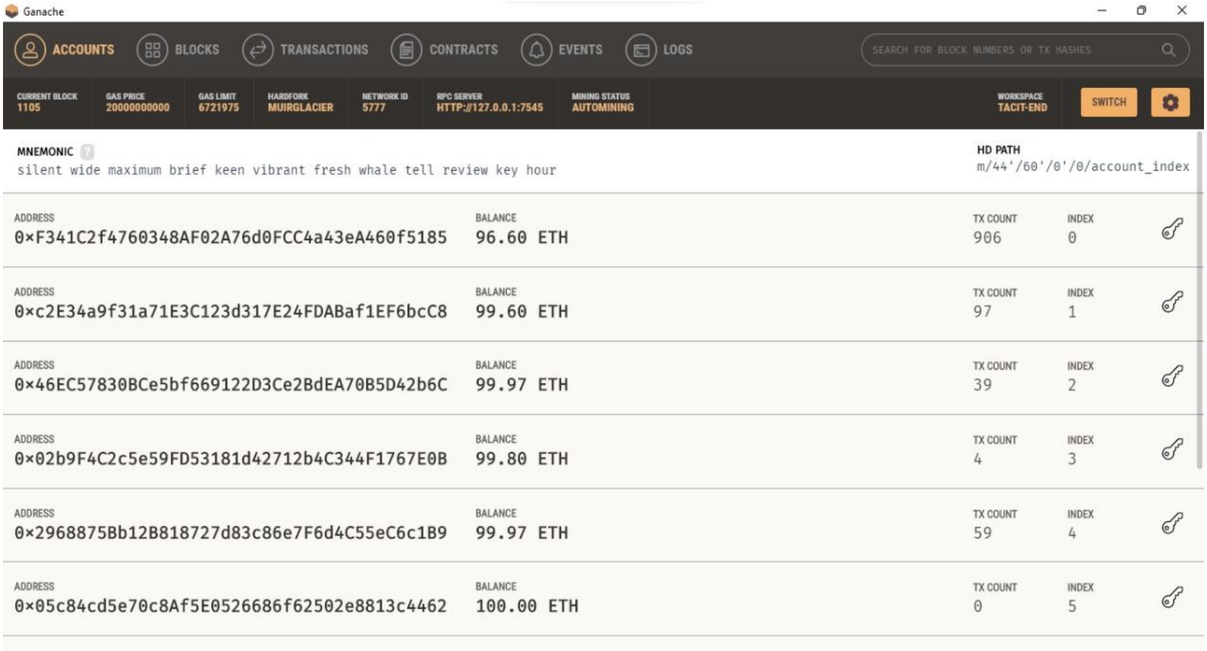
```
truffle(development)> web3.eth.getAccounts()
[
  '0xF341C2f4760348AF02A76d0FCC4a43eA460f5185',
  '0xc2E34a9f31a71E3C123d317E24FDABaf1EF6bcC8',
  '0x46EC57830BCe5bf669122D3Ce2BdEA70B5D42b6C',
  '0x02b9F4C2c5e59FD53181d42712b4C344F1767E0B',
  '0x2968875Bb12B818727d83c86e7F6d4C55eC6c1B9',
  '0x05c84cd5e70c8Af5E0526686f62502e8813c4462',
  '0x584D99aCC6e9567F7FFFF44a5E3bF39EABfAFE8F',
  '0x18EcF6177C5831dDE4c1E1d3Da517D55E2E04800',
  '0x78DC808DA37e4634903a9873410e48cB846f1096',
  '0x5ead1e118718Fa55FE9894A44239C68d7781E5fF'
]
```

Fig 7.3 Output Screenshot-3



```
logs: [
  {
    logIndex: 0,
    transactionIndex: 0,
    transactionHash: '0x579732bed570cc13c18d1f7988d82e7b20a6e745aba8189eb2f1a4aaa2dd91b1',
    blockHash: '0xc0e25ff8d948c9bdf030b012204e691a84cf05a513f895a75ac27a1c07fa8e46',
    blockNumber: 1105,
    address: '0x7f3B9Fc5D2562273773daD3798eb78a3DeEd8CeD',
    type: 'mined',
    id: 'log_72ab0552',
    event: 'Transfer',
    args: [Result]
```

Fig 7.4 Output Screenshot-4



CURRENT BLOCK 1105 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE TACIT-END

MNEMONIC
silent wide maximum brief keen vibrant fresh whale tell review key hour

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×F341C2f4760348AF02A76d0FCC4a43eA460f5185	96.60 ETH	906	0
0×c2E34a9f31a71E3C123d317E24FDABaf1EF6bcC8	99.60 ETH	97	1
0×46EC57830BCe5bf669122D3Ce2BdEA70B5D42b6C	99.97 ETH	39	2
0×02b9F4C2c5e59FD53181d42712b4C344F1767E0B	99.80 ETH	4	3
0×2968875Bb12B818727d83c86e7F6d4C55eC6c1B9	99.97 ETH	59	4
0×05c84cd5e70c8Af5E0526686f62502e8813c4462	100.00 ETH	0	5

Fig 7.5 Output Screenshot-5

VIII. CONCLUSION:

We looked at how to create an Ethereum-based payment application. It was also deployed and tested. We next dived into the Solidity language syntax, which is not only large but also diverse. JavaScript codes were also investigated. Furthermore, we discovered how to create our own coin ERC20 tokens, and then send and test them. Finally, it demonstrates that the performance of the presented models is influenced by security, as a considerable improvement is brought about by blockchain's innovative characteristics.

REFERENCES

[1] Chen, L., Cong, L. W., & Xiao, Y. (2021). A brief introduction to blockchain economics. In Information for Efficient Decision Making: Big Data, Blockchain, and Relevance (pp. 1-40).

[2] Liu, Y., Tsyvinski, A., & Wu, X. (2019). Common risk factors in cryptocurrency (No. w25882). National Bureau of Economic Research.

[3] Mani, Thirunavukkarasu & Kota, Harsha & Reddy, Kommireddy. (2021). Creating Payment Application and Cryptocurrency on the Ethereum Blockchain. International Journal of Computer Science and Mobile Computing. 10. 28-34. 10.47760/ijcsmc. 2021.v10i04.005.

[4] Halevi, T., Benhamouda, F., De Caro, A., Halevi, S., Jutla, C., Manevich, Y., & Zhang, Q. (2019, July). Initial public offering (IPO) on permissioned blockchain using secure multiparty computation. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 91-98). IEEE.

[5] Xi, Z. (2020, January). The comparison of the decentralized and centralized structure of network communication in different application fields. In Advances in Economics, Business and Management Research, International Conference on Management Science, and Industrial Economy (Vol. 118).

[6] Barsan, I. M. (2017). Legal challenges of initial coin offerings (ICO). Revue Trimestrielle de Droit Financier (RTDF), (3), 54-65.

[7] Kranz, J., Nagel, E., & Yoo, Y. (2019). Blockchain token sale. Business & Information Systems Engineering, 61(6), 745-753.

[8] Aswini, R., & Kiruba, K. (2019, March). College fees transaction using hash functions of the blockchain model. In 2019 IEEE International Conference on System, Computation, Automation, and Networking (ICSCAN) (pp. 1-6). IEEE.

[9] Ansari, K. H., & Kulkarni, U. (2020, April). Implementation of Ethereum Request for Comment (ERC20) Token. In Proceedings of the 3rd International Conference on Advances in Science & Technology (ICAST).