VIT TOKEN:

OUR OWN CRYPTOCURRENCY

Project Report

for the course

CSE1011 – Cryptography Fundamentals

Submitted by:

Lakshit Mangla (18BCI0246)

Alka Rani (19BCI0004)

Soham Faldu (19BCI0024)

Utkarsh Shukla (19BCI0099)

Parul Tripathi (19BCI0147)

Professor: *Dr. Madhu Vishwanatham V*

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Date: 31 May, 2021

Contents

Abstract

We all have bank accounts and we do use them frequently especially during the current COVID-19 situation. But do you remember how much of stress you went through when you were opening a new Bank account or arguing with the higher authorities over the phone?

What if there was a way to still send and receive money but without any of the hassles? Yes, and the answer to this is Cryptocurrency, and that's exactly what we are trying to do. To relieve people from this headache of banks and a centralized authority over them, we are creating our own Cryptocurrency - VIT token.

In this project, we plan to develop our cryptocurrency using Solidity, an object-oriented programming language, for writing Smart Contracts.

Our currency will be complying with the ERC-20 Token Standard provided by Ethereum.

Once the Smart contract is in place, our Backend team will become proactive and start creating APIs for the transactions that will take place.

Side by Side, our Frontend web developers will be working on the UI/UX which will allow end-users to buy and interact with VIT token smoothly without any hassle. They'll be using a Technology Stack of HTML, CSS, JavaScript, and Bootstrap.

Once both Backend, as well as the Frontend, run individually smoothly, we will start integrating both of them.

Meanwhile, our Documentation team will be working on providing a transparent guide on how to interact efficiently with VIT token.

We plan to host our website on GitHub as of now but we are still looking for a possibility of purchasing a domain.

Since we want this to be as transparent as possible, we will be Open Sourcing our code completely so that people can have a look at it anytime and our fellow developers can help us make it better over time and be a part of this revolution.

By the end of our project, VIT token will be hosting its ICO (Initial Coin Offering) on our webpage.

Keywords:
Cryptocurrency, Blockchain, Ethereum, Smart Contracts, ERC-20, ICO.

Introduction

Cryptocurrency, in simple words, is a digital currency which instead of being controlled by a central authority (like a bank) is managed by peers or nodes in the network with no superior powers than you. Yes, somebody who joined just now has the same level of authority as somebody who has been there since the beginning.

Cryptocurrency basically eliminates the middle-men like central banks, it also eliminates the higher authorities which have control over your money or bank account, and to sum it up, it also provides anonymity to the user to a great extent.

Now, a Cryptocurrency runs on a Blockchain. Blockchain is a distributed immutable ledger. Data in the form of blocks are distributed over the nodes of a network rather than a single server of an IT company, immutable means that it cannot be changed or manipulated once written, and ledger is all the data stored in it. Once a block is full, another block is mined to the chain, and the new data is entered in the next block and so on. The chain thus continues and this is why it is called a blockchain.

Thus, we are planning to develop our cryptocurrency called VIT token. VIT token allows the users to securely send and receive money with maximum possible anonymity. We promote transparency thus our whole codebase will be open-sourced so that people can count on us when they make financial transactions.

A Smart Contract is used to create rules for the functioning of our currency without the involvement of any mediator or a third party. In simple words, it is like a lawyer in the physical world.

For coding the smart contracts, Solidity will be used as our main language as it is object-oriented and well accepted in the blockchain industry. The user will be able to send and receive VIT tokens using their cryptocurrency wallets. Initially, we will be providing support for the Metamask wallet. Our coin will comply with the EIP 20 token which allows us to host our ICO.

We will be using the Ethereum blockchain's test network called Rinkeby to deploy our Cryptocoin. We cannot use the main Ethereum networks since every byte stored or every line of code present in the code has a cost to be executed in the network in the form of Gas Ethers.

And to make our VIT token easily accessible, we will be deploying it on a webpage. A clean webpage will be built for easy and quick interactions, the backend will be coded using NodeJS and the Express library as it has a secure and quick response time.

At the end of this project, we plan to host an Initial Coin Offering (ICO) for our coin (like an IPO of a company in share market) which helps us understand the market value of our ICO and give investors an early chance to get on board. During this ICO, one will be able to get hold of VIT token before VIT token goes public.

Literature Survey

1. *Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Manubot.*
   In this paper, the need and working of a purely peer-to-peer version of electronic cash system is discussed. It would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.

2. *Buterin V. (2015). Ethereum. Retrieved February, 18, 2020.*
   In this paper, Buterin, the founder of Ethereum, discusses the logic and scripting of cryptocurrency. From here we can derive the implementation of smart contracts for the logical part of transactions. For any block transaction list Tx with n transactions, there must be a valid state transition from what was the canonical state before the transaction was executed to some new state. If any transaction has a higher total denomination in its inputs than in its outputs, the difference also goes to the miner as a "Transaction fee". The problem with this line of reasoning is that transaction processing is not a market; although it is intuitively attractive to construe transaction processing as a service that the miner is offering to the sender, in reality every transaction that a miner includes will need to be processed by every node in the network, so the vast majority of the cost of transaction processing is borne by third parties and not the miner that is making the decision of whether or not to include it.

3. *Bonneau, J., Clark, J., & Goldfeder, S. (2015). On Bitcoin as a public randomness source. IACR Cryptol. ePrint Arch., 2015, 1015.*
   In this paper they have pointed out the need for more randomness. As a side-effect of Bitcoin's proof-of-work-based consensus system, random values are broadcasted every time new blocks are mined. They have made a Beacon function which will decrease the min-entropy. Bitcoin has a remarkable number of interesting security protocols such as timestamping and multiparty computation. The authors added a public randomness beacon for which Bitcoin provides an unprecedented opportunity to build a highly available beacon which has a convincing cryptographyic argument of security with no trusted third parties. The beacon has a vast number of application. It will promote transparency and accountability for number of processes.

4. *Vogelsteller, F., & Buterin, V. (2015). Eip 20: Erc-20 token standard. Retrieved February, 18, 2020.*
   This paper gives a standard interface for tokens. Making an interface for the tokens will make is flexible to be used by other applications: from wallets to decentralized exchanges. The author has also define the functions which will allow tokens to be approved so that they can be spent by another on-chain third party. Multiple implementations are provided. Making a standard interface for ERC-20 makes it available for the world to make use of it and make third party transactions and wallets.

5. *Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015, May). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In 2015 IEEE symposium on security and privacy (pp. 104-121). IEEE.*
   This paper talks about providing the first systematic exposition Bitcoin and the many related cryptocurrencies or altcoins.' Drawing from a scattered body of knowledge, we identify three key components of Bitcoin's design that can be decoupled. This enables a more insightful analysis of Bitcoin's properties and future stability. Also surveying the anonymity issues in Bitcoin and provide an evaluation framework for analysing a variety of privacy-enhancing proposals. Finally, it provides new insights on what we term disintermediation protocols, which absolve the need for trusted intermediaries in an interesting set of applications.

6. *Baqer, K., Huang, D. Y., McCoy, D., & Weaver, N. (2016, February). Stressing out: Bitcoin "stress testing". In International Conference on Financial Cryptography and Data Security (pp. 3-18). Springer, Berlin, Heidelberg.*
   In this paper, we present an empirical study of a recent spam campaign (a "stress test") that resulted in a DoS attack on Bitcoin. The basic goal of our investigation being to understand the methods spammers used and impact on Bitcoin users. We show the impact of increasing non-spam transaction fees from 45 to 68 byte on average, and increasing delays in processing non-spam transactions from 0.33 to 2.67 h on average, as well as estimate the cost of this spam attack at 201 BTC (or $49,000 USD). We then concluded out by pointing out changes that could be made to Bitcoin transaction fees that would mitigate some of the spam techniques used to effectively DoS Bitcoin.

7. *Peck, M., Tonti, W. R., Stavrou, A., Rupe, J. W., Rong, C., & Kostyk, T. (2017). Reinforcing the links of the Blockchain. IEEE Future Directions Blockchain Initiative White Paper, 1-16.*
   This paper talks about Blockchain, as an industry, that has entered its Cambrian phase. A glut of investor interest has led to an explosion in the technical diversity of projects now underway. Blockchain technology is poised to change nearly every facet of our digital lives, from the way we send money to the way we heat our homes. By obviating third parties, blockchains promise to make our systems more efficient. By circumventing censorship, they promise to make our systems more equitable. And if properly implemented, they could make our systems more reliable and secure. All these changes will arrive more quickly, and their effects will be compounded, if the parties who are now building them work together. Today, that is not the case. Alliances have been announced. But, thus far, what they have added to the industry is more blockchains, more designs, more choices, and more competition.

8. *Victor, F., & Lüders, B. K. (2019, February). Measuring ethereum-based erc20 token networks. In International Conference on Financial Cryptography and Data Security (pp. 113-129). Springer, Cham.*
   This paper focuses on the trade of tokens rather than traditional analysis of content and communication graphs on different blockchain. The authors provide theoretical background, current research results and related work on cryptocurrencies, blockchain and smart contracts. Ethereum is an open-source, public, distributed, blockchain based platform with a Proof of Work-based consensus algorithm coupled with rewards, which involves the need for trusted intermediaries. Ethereum's most significant feature is the Ethereum Virtual Machine (EVM) - a stack-based runtime environment that can execute programs known as smart contracts. They can

be developed in high level languages such as Solidity and deployed on the blockchain as bytecode by any participant of the network.

9. *Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. Financial Innovation, 5(1), 1-14.*
   The research paper conducts a systematic and objective review that is based on data statistics and analysis. It describes different disciplines in blockchain and also its future applications in business. The application of blockchain has extended from digital currency and finance and it has gradually extended into health care, supply chain management, market monitoring, smart energy and also copyright protection. The paper also deals with promising research directions and practical applications of blockchain.

10. *Ansari, K. H., & Kulkarni, U. (2020). Implementation of Ethereum Request for Comment (ERC20) Token. Available at SSRN 3561395.*
    In this paper we have learnt the essential aspects of Blockchain technology. The proposed system will create its cryptocurrency. The paper deals by explaining the proposed model, different functions of ERC20 standard, the different tasks performed by each function and implementing various functionalities of ERC20 Token in Solidity. The system developed has two smart contracts one each for ERC20 Token and Crowd sale and developed the smart contract for token portion of our system. Here we have described various functions used in creating our tokens and different event and task performed by each of them. Successfully conducted test against our token smart contract which checks various aspects of tokens and depicted various pictures of our implementation.

Design and Architecture

Methodology adapted

Developing an ERC-20 Token using Smart Contracts and hosting an ICO.

ERC-20 (Ethereum Request for Comment and 20 is the proposal identifier) tokens differ from other cryptocurrencies such that they are based on Ethereum blockchain instead of having their own Blockchain. These exist to propose improvements to the Ethereum network. Therefore, we don't need to create our blockchain which requires a lot of resources and nodes in the network with high computing powers.

ICO or Initial Coin Offering refers to the process of launching the cryptocurrency to the interested investors (pretty much like Initial Public Offering (IPO) in share market).

So for our project, we have used the Rinkeby Test Network, which is a version of the Ethereum network, mainly used for test purposes. Therefore, all the Ethers (tokens) exchanged on our network are not of any real value on the actual network.

Our project is a web-app that lets you interact with our cryptocurrency. This was developed using HTML, CSS, Bootstrap, and JavaScript. Our coin is based on the EIP protocol provided by Ethereum for setting up the Smart Contracts on Solidity.

We have developed 2 Smart Contracts for our project:

- One for the coin (according to ERC-20 standard)
- Other one for the token sale (ICO).

We have used Solidity as a language for our smart contacts. To implement Blockchain locally we used Ganache and Truffle framework using NodeJS. Lastly to connect to the Blockchain network the user needs to have the MetaMask extension on their web browser. Metamask also provides users with Ethers from their wallet which they can send and receive to test our currency as well as our network.

Timeline of our project

We have successfully completed our project on time. From the coding the Smart Contracts in Solidity to integrating it with a Web Interface.

- Collection of resources and learning Solidity along with basic Web Application Development.
- Researching various papers and finding out the difficulties faced while using a cryptocurrency and how to make it safe from any attacks which could devalue our token.
- Now, we designed a Wireframe for our project and the development began.
- First we designed the VIT token that is our cryptocurrencies' properties, data sizes, etc using Solidity and tested it against various attacks to certify ourselves that it is not prone to any such attacks.
- Then we designed our frontend of the web app whose screenshots you will find below, we all spent a lot of time figuring out the perfect balance between how a Cryptocurrency ICO website should look to a developer to how it looks a person just entering in the world on Cryptocurrencies and Blockchain.
- Side by Side, we started implementing the Backend to create a Robust API that could facilitate the transactions on the go.
- Finally, we connected all the parts and our VIT token is now complete.

Softwares and Languages

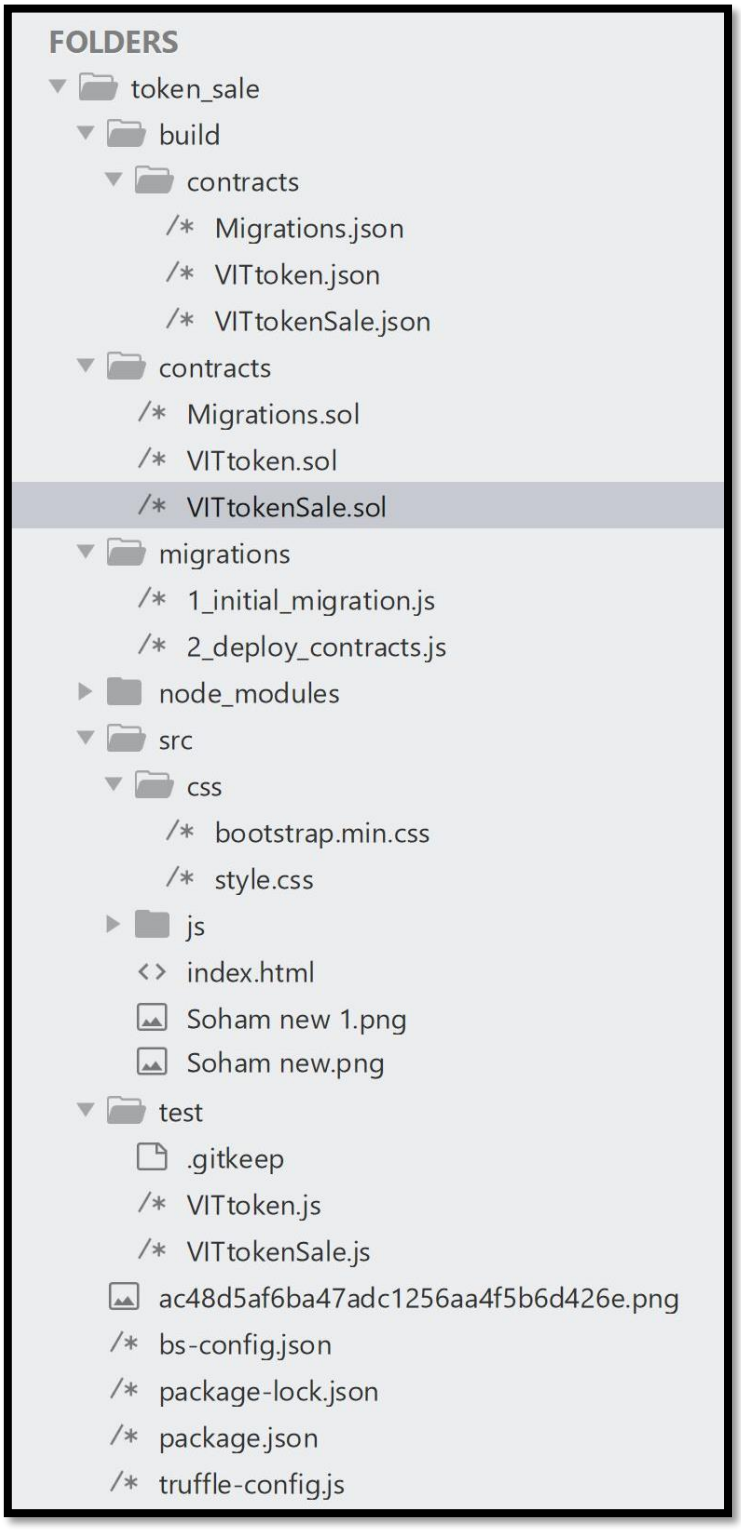
- Solidity Compiler
- Metamask
- Truffle
- Ganache
- HTML
- CSS
- JavaScript
- NodeJS

Tools

- **Rinkeby:** Ethereum is the most popular Blockchain used for deploying Smart Contracts. However, we will be using their test network known by the name of Rinkeby. Rinkeby is also a peer-to-peer decentralized blockchain that is used for testing various decentralized apps. Rinkeby is free-of-cost to use and handles requests well.
- **Ganache:** Ganache provides us a simulation of chains of block worth of data to test our model, execute different commands, test our API, and lets us inspect each state before we go into production.
- **Truffle:** Truffle provides a set of tools, scripts, and boilerplate code which gets us underway and also provides developers with Ethereum Virtual Machine (EVM) like features and accessibility.
- **Metamask:** It is an Ethereum wallet and a gateway to a million of applications that require a crypto-wallet. It is secure and can be accessed from multiple devices. It can store more than 200 cryptocurrencies at once. Our end-users will be purchasing VIT token using Ethereum through their Metamask wallet.

Codebase

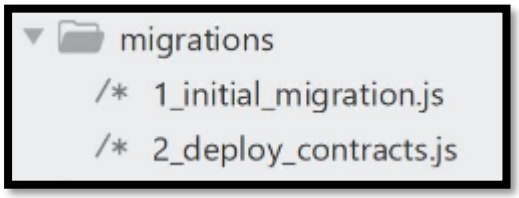
Directory Structure



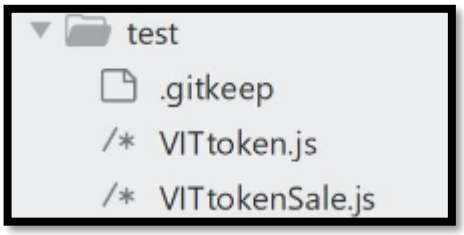
Build

Contracts

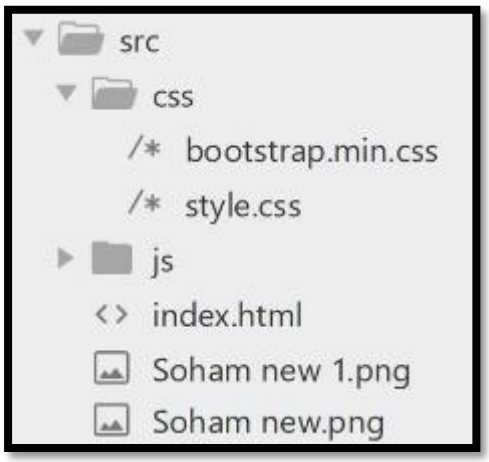
Migrations



Test

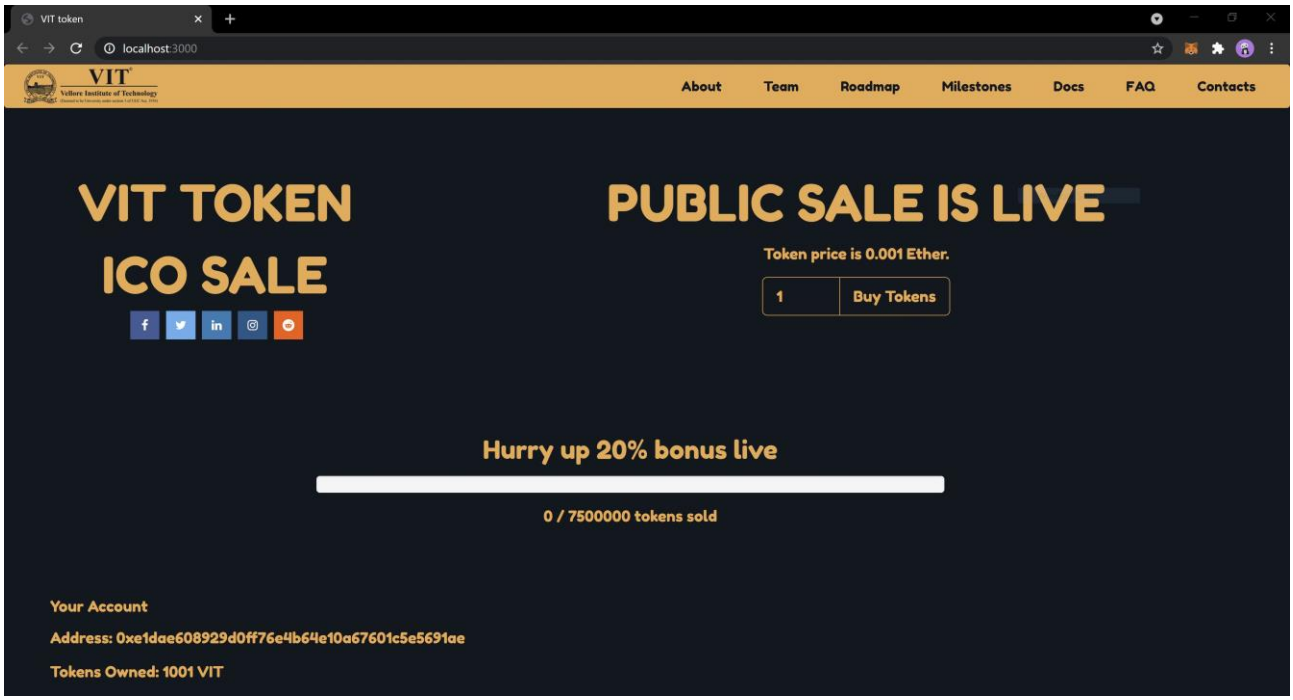


Src

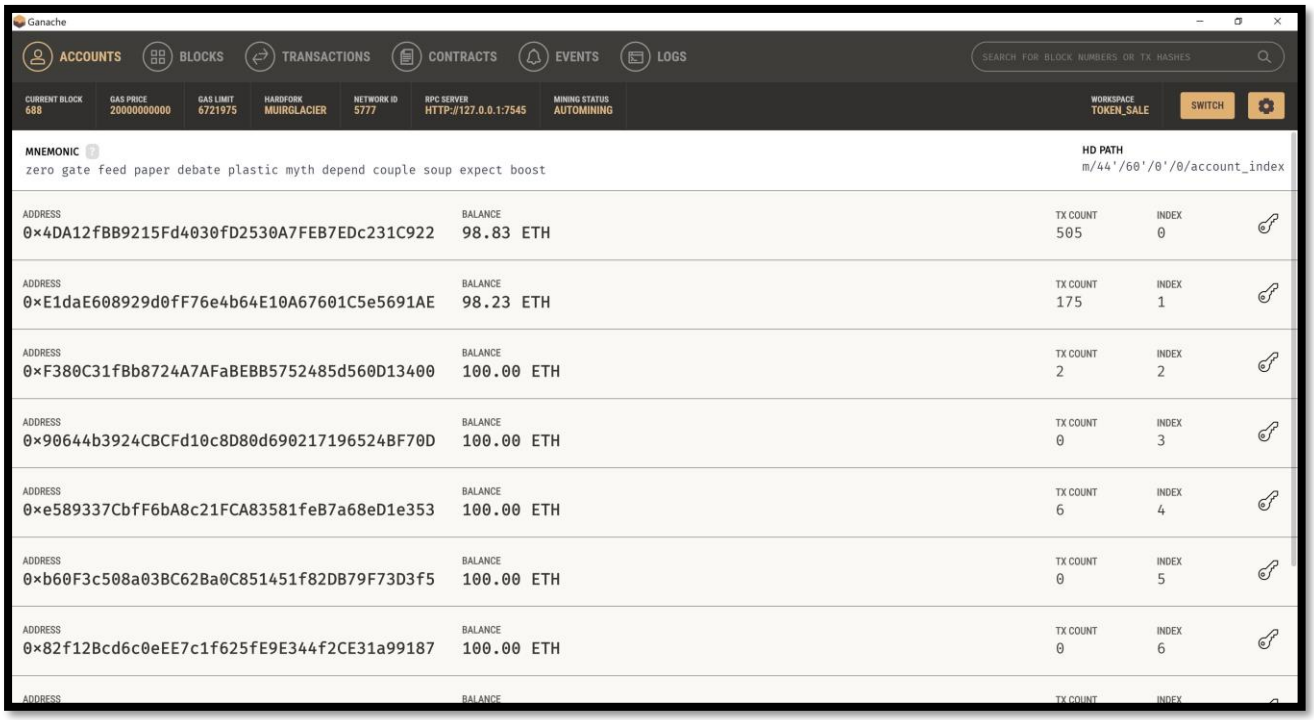


Implementation

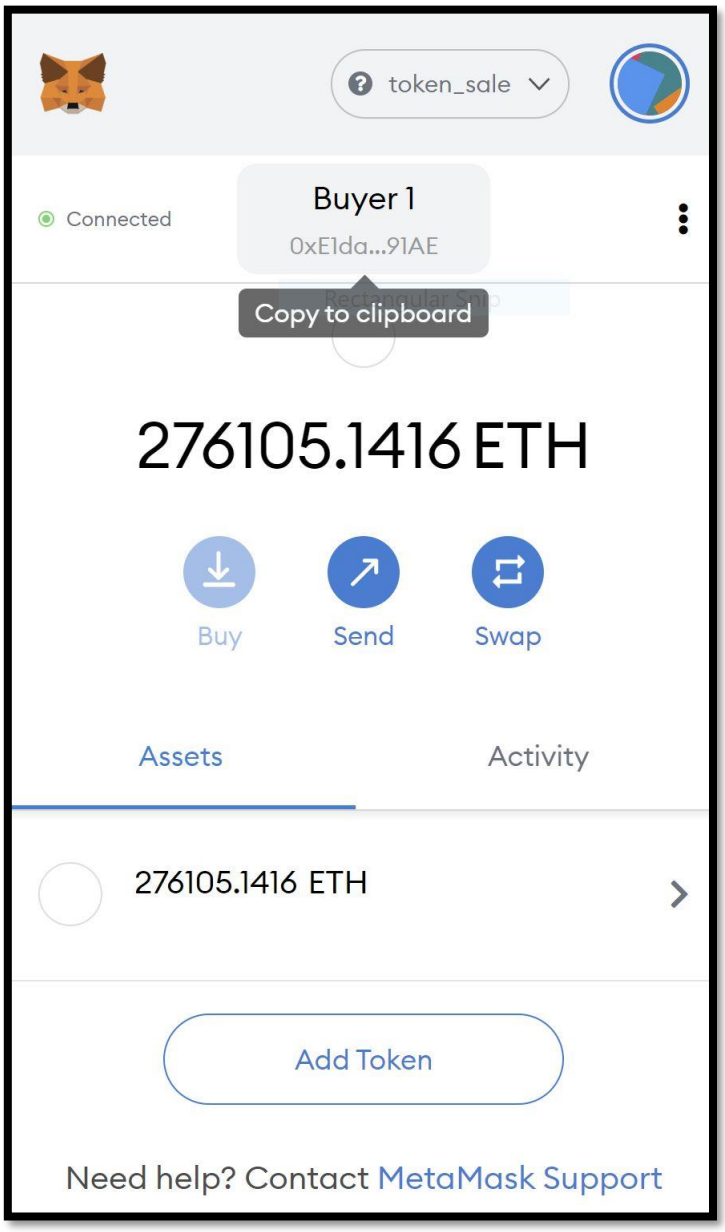
Website



Ganache workspace



Metamask Browser Extension



Conclusion

A fully functioning Cryptocurrency has been implemented with a web interface to facilitate transactions stored in the Rinkeby blockchain network.

As of now, we can only host this on our local network. To publish this, we would require monetary support as deploying every line of code or storing even a single int costs money on the Ethereum Blockchain.

Once we have our VIT token on the Blockchain, we plan to conduct our first ICO wherein users can buy our VIT token with real money and deal accordingly.

References

Literature Papers

https://bitcoin.org/bitcoin.pdf

https://ethereum.org/en/whitepaper/

https://eips.ethereum.org/EIPS/eip-20

https://pdfs.semanticscholar.org/ebae/9c7d91ea8b6a987642040a2142cc5ea67f7d.pdf

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163021

https://link.springer.com/chapter/10.1007/978-3-662-53357-4_1

https://blockchain.ieee.org/images/files/pdf/ieee-future-directions-blockchain-white-paper.pdf

https://link.springer.com/chapter/10.1007/978-3-030-32101-7_8

https://link.springer.com/article/10.1186/s40854-019-0147-z

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561395

Other Sources

https://www.exodus.io/blog/how-to-create-a-cryptocurrency/#head1

https://mlsdev.com/

https://www.dappuniversity.com/articles/how-to-build-a-blockchain-app

https://www.investopedia.com/terms/b/blockchain.asp

https://blockgeeks.com/guides/smart-contracts/

https://www.ledger.com/academy/crypto/what-are-erc20-tokens/

https://www.dappuniversity.com/articles/code-your-own-cryptocurrency-on-ethereum

https://youtu.be/XdKv5uwEk5A

https://support.blockchain.com/hc/en-us/articles/360027491872-What-is-an-ERC20-token-