Journal of Advanced Research in Technology and Management Sciences (JARTMS)
Volume: 03 Issue: 04 ISSN: 2582-3078 July 2021
Available online at: http:// www.jartms.org

An Invulnerable Money Transfer using Block chain

B.S.Vara Prasad, G.Mahathi, P.Sree Sai Deeksha, G.Keerthi Reddy, G.Vamsi Krishna

Abstract: In the current time of drastic and revolutionary changes, it is imperative to radically rethink business models and archetypes in general. Traditional financial services providers, banks in particular, are lagging behind the pace of technology development. According to one report from Accenture, most large banks use systems from the 1970s or even the 1960s, and newer computing technologies are simply laid on top of this foundation to support providing banking services online or via mobile devices. Currently, the global financial system is enormous, but it is very cumbersome to transfer money. Financial middlemen are required to transfer any sum of money, each of which takes a service charge. During the transfer of money, the frauds may occur and there will be a huge loss in the economy. Blockchain reduces the number of middlemen while increasing the security, both of which will reduce costs.

Keywords: Blockchain, distributed systems, money transfer, security

* Correspondence Author
Mr.B.S.Vara Prasad, *Department of CSE,*
Usha Rama College of Engineering and Technology,
India.
Email:mail2vara@gmail.com
G.Mahathi, *Department of CSE,*
Usha Rama College of Engineering and Technology,
India,
Email:mahathigunti1999@gmail.com
P.Sree Sai Deeksha, *Department of CSE,*
Usha Rama College of Engineering and Technology,
India,
Email:deekshapanchumarthi@gmail.com
G.Keerthi Reddy, *Department of CSE,*
Usha Rama College of Engineering and Technology,
India,
Email:keerthireddy1962@gmail.com
G. Vamsi Krishna, *Department of CSE,*
Usha Rama College of Engineering and Technology,
India,
Email:vamsighanta999@gmail.com

1. INTRODUCTION

The objective of this project to create a de-centralized blockchain based e-wallet to access currency. The project entails creating a generalized blockchain API which can later be used for further development in the blockchain field of applications. This blockchain API will be used to construct a cryptocurrency from scratch. Implement a new hashing function for the blockchain which will take data and create a fixed length output. Implementing a highly secure and personal e-wallet system to access and control the said cryptocurrency. This e-wallet system will let the user control and transact the currency efficiently. It provides the user with full authority over the token currencies. The aim is also to make the currency secure, easy to access, fast and as cheap to avail as possible. Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved. Business runs on information. The faster it's received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members. A blockchain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities. If you have been following banking, investing, or cryptocurrency over the last ten years, you may have heard the term "blockchain," the record-keeping technology behind the Bitcoin network. Blockchain is a specific type of database. It differs from a typical database in the way it stores information. Blockchains store data in blocks that are then chained together. As new data comes in it is entered into a fresh block. Once the block is filled with data it is chained onto the previous block, which makes the data chained together in chronological order. Different types of information can be stored on a blockchain but the most common use so far has been as a ledger for transactions. In Bitcoin's case, blockchain is used in a decentralized way so that no single person or group has control rather, all users collectively retain control. Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone. Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. If you take a look at Bitcoin's blockchain, you'll see that each block has a position on the chain, called a "height." As of November 2020, the block's height had reached 656,197 blocks so far. After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block unless the majority reached a consensus to do so. That's because each block contains its own hash, along with the hash of the block before it, as well as the previously mentioned time stamp. Hash codes are created by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well. Here's why that's important to security. Let's say a hacker wants to alter the blockchain and steal Bitcoin from everyone else. If they were to alter their own single copy, it would no longer align with everyone else's copy. When everyone else cross-references their copies against each other, they would see this one copy stand out and that hacker's version of the chain would be cast away as illegitimate. Succeeding with such hack would require that the hacker simultaneously control and alter 51% of the copies of the blockchain so that their new copy becomes the majority copy and thus, the agreed upon chain. Such an attack would also require an immense amount of money and resources as they would need to redo all of the blocks because they would now have different timestamps and hash codes. Due to the size of Bitcoin's network and how fast it is growing, the cost to pull off such a feat would probably be insurmountable. Not only would this be extremely expensive, but it would also likely be fruitless. Doing such a thing would not go unnoticed, as network members would see such drastic alterations to the blockchain. The network members would then fork off to a new version of the chain that has not been affected. This would cause the attacked version of Bitcoin to plummet in value, making the attack ultimately pointless as the bad actor has control of a worthless asset. The same would occur if the bad actor were to attack the new fork of Bitcoin. It is built this way so that taking part in the network is far more economically incentivized than attacking it.

2. DESIGN

The proposed framework consists of a DApp wallet in which users can make the money transactions through Cryptocurrency using Blockchain.

USER LAYER A user of a system is defined as an individual who makes effective use of the system and its resources. A user has various roles and features on the system, making him identifiable on the system. The main task of these users would be to interact with the system and perform basic tasks such as send, receive and request money. The users using this system would be accessing the system's functionality by a browser which in technical terms we refer as DApp browser, as it is containing the GUI (Graphical User Interface) of the DApp, i.e., our proposed system framework. The GUI contains all the functions that could be accessed by a particular user. The user according to the assigned role could use this GUI for interacting with the other layer of the system, i.e., blockchain layer.

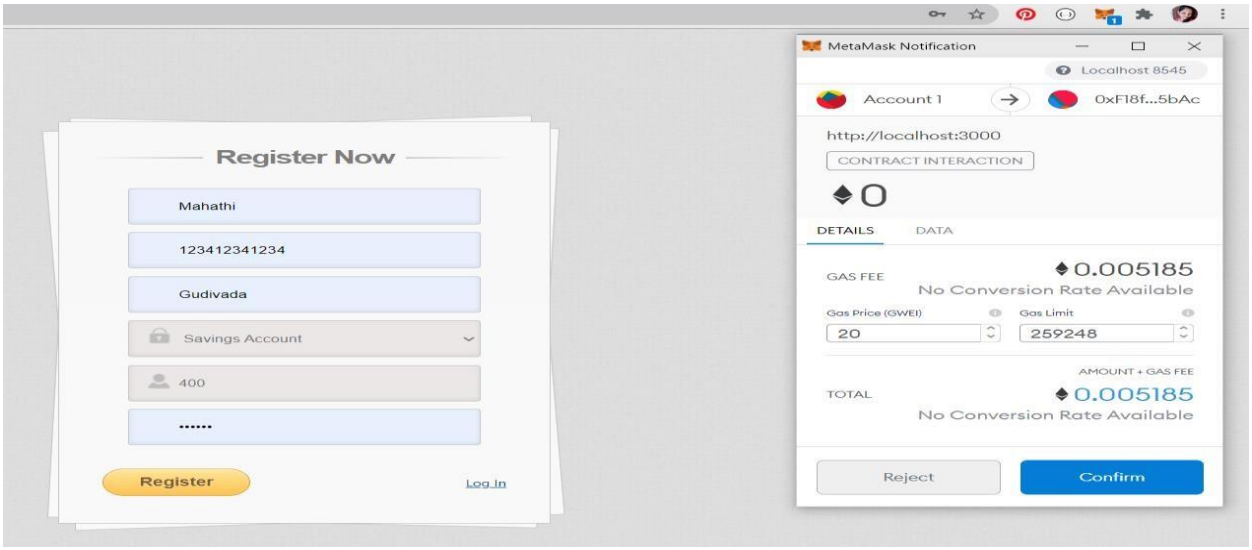
Modules used in this system are

Registration: Here the user can Register into the Wallet by providing the required credentials. In this the user has to select a unique User ID which is used to login to the account. If the user selects the user id which is already existed, he can't be able to register and an alert message appears that the account is already existed. By using this User Id and password user may login to his account whenever he wants and can access the wallet and make the transactions.

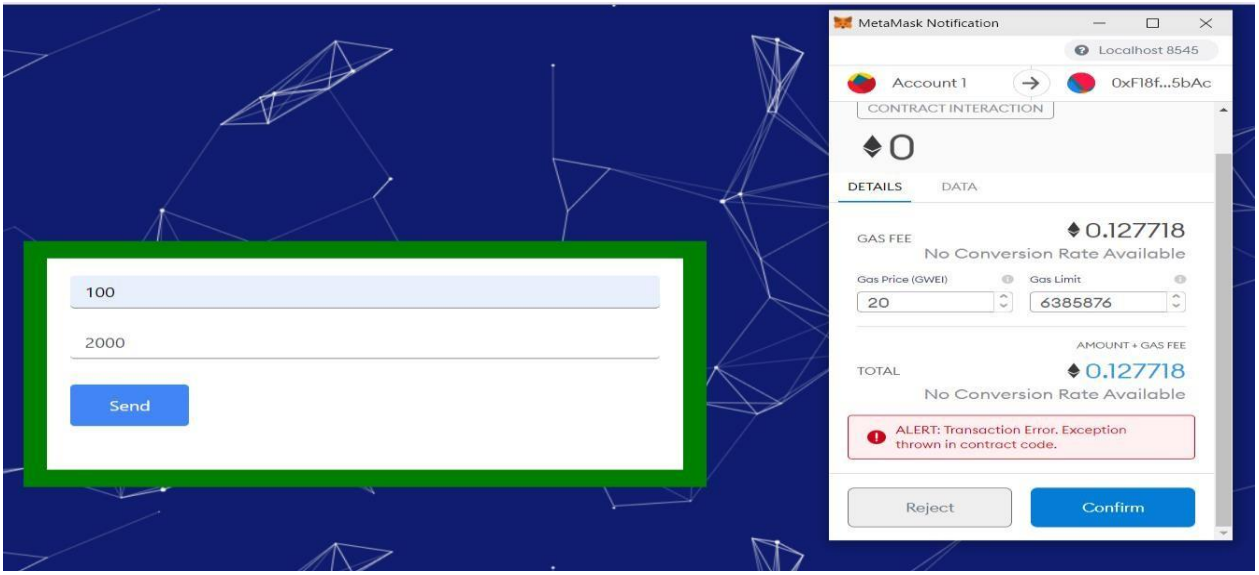
Journal of Advanced Research in Technology and Management Sciences (JARTMS)
Volume: 03 Issue: 04 ISSN: 2582-3078 July 2021
Available online at: http:// www.jartms.org

Account Balance: In this application, the Balance of the wallet is given 1000 rupees by default. These money can be transferred to the other account. After the transaction is done the Balance is updated accordingly. Whenever we click on check Balance, your account balance will be appeared for 3 seconds.
Making Transactions: In this application, we can make transactions by using Send/Receive. Whenever we make a transaction the Metamask notification raises for the confirmation whether to complete the transaction or not. If we Accept, then the alert message appears that the transaction completed successfully else the transaction will not be processed.
Transaction History: If we Send or Receive the money, those transactions will be updated in the transaction History. All the transactions done till now will be recorded in a queue. When we click on Recent Transactions, then the icon show transactions will be displayed which displays the transactions on click.
Chatbot: This Chatbot is used to solve the queries regarding the application. Whenever we are unable to understand about how to create an account or how to make transactions or regarding the cryptocurrency etc., we can solve those type of queries using this chatbot.

Figure



Registration Page



Sending Money

3. ANALYSIS

The user will have access to the wallet to make a money transaction i.e., send/receive money. In this, Ganache acts as a Backend which is nothing but Blockchain in which the transactions will be stored as the Blocks. The Ganache consists of Auto mining and all the backend process will be done automatically without any miner. The Metamask is used as an interface between the DApp and the Ganache which allows the user to make the transactions through the Blockchain using Ethereum cryptocurrency. The main motto of DApp wallet is to provide better security during money transactions

4. RESULTS

We have got the favorable results in all the aspects like showing the user that the transaction was successful in case of a successful transaction or else giving the required warnings regarding low wallet balance or wrong wallet information. The authentication of the user after registering is successful as an alert message will be shown if the credentials does not match with the credentials in the database. It is also taken care about the smooth and efficient interface for the users.

5.CONCLUSIONS

The paper presents a simple and pragmatic blockchain-based architecture for secure money transactions. Further, a DApp is developed and its performance is analyzed in terms of costs and execution time. In future, we intent to extend the work by including privacy along with security. Blockchain technology is given prominence in many applications where security and transparency are very important. As explained in this application, if we include blockchain in the Money transactions we can make our transactions secured and can overcome the server issues. By using cryptocurrency, we can encrypt the transaction as it uses Blockchain. If this application can be implemented in the real-time it will bring a huge growth in our economy

REFERENCES

[1] H. Kuzuno and C. Karam, "Blockchain explorer: An analytical process and investigation environment for Ethereum," APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ, Published on 2017, pp. 9-16.
[2] Tian, Feng. "An agri-food supply chain traceability system for China based on RFID & blockchain technology." Service Systems and Service Management (ICSSSM), International Conference on. IEEE, Published on 2016.
[3] Ali, Muneeb, et al. "Blockstack: A Global Naming and Storage System Secured by Blockchains." USENIX Annual Technical Conference, Published on 2016.
[4] Larimer, D., N. Scott, V. Zavgorodnev, B. Johnson, J. Calfee, and M. Vandeberg "Steem: An incentivized blockchain based social media platform,". Published on 2016
[5] Buba, Zirra Peter,and Gregory Maksha Wajiga. "Cryptographic algorithms for secure data communication." International Journal of Computer Science and Security (IJCSS), Published on 2011, pp .227- 243.
[6] Stapleton, Jeff, and Ralph Spencer Poore. "Tokenization and other methods of security for cardholder data." Information Security Journal: A Global Perspective 20.2, Published on 2011, pp 91-99.
[7] Swan, Melanie, "Blockchain: Blueprint for a new economy," O'Reilly Media, Inc.", Published on 2015.
[8] Szydlo, Michael. "Merkle tree traversal in log space and time," International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg", Published on 2004.
[9] Grinberg, Reuben. "Ethereum: An innovative alternative digital currency."Published on 2011.
[10] Gilbert, Henri, and Helena Handschuh. "Security analysis of SHA-256 and sisters", Selected areas in cryptography. Springer Berlin/Heidelberg, Published on 2004.