INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 07 ISSUE: 03 | MARCH - 2023 IMPACT FACTOR: 7.185 ISSN: 2582-3930

Transaction System Based on Blockchain Technology using Smart Contract

Ashish Kumar Jha, Shivani Dubey, Harshit Kumar
Department of Information Technology
Greater Noida Institute of Technology, Greater Noida, India

Abstract: Blockchain is a peer-to-peer distributed ledger technology, nowadays widely used and a hot topic in the industries. A Smart Contract is a virtual contract based on Blockchain technology which executes and operates between two parties (especially a buyer and a dealer) when a certain condition of the contract is met. The objective of this research is to present a decentralized transaction system based on Blockchain technology implemented using Smart Contract. Blockchain based cryptocurrencies are an evidence for a secure implementation of any currency-based centralized systems put forth in use in a decentralized way. Current transaction systems and payment gateways are centralized systems that need monitoring and verification from a central agency like a bank or a third party organization which are not completely automated as some of the processes are human controlled. Also deposition and withdrawal of money sometimes take a long procedural time. Still these systems are neither completely error free nor secure and time to time certain issues may arise. Even nowadays some payment methods charges transaction fee which is like paying for the money you are paying for. In this research paper we are proposing an automated Ethereum blockchain technology based transactionsystem which will eliminate the bank and third party verification.Each block of the Ethereum blockchain in the system will store the transaction details also linked with all the previous transaction details in the form of a chain. A Smart Contract is used to define the terms and conditions of the transaction which include account creation, ether deposition and withdrawal. This system enables users to carry out transaction without any fraud and losses from anywhere around the globe within split seconds.

Keywords: Transaction system ,Blockchain, Smart Contract, decentralized,crypto-currency

I. INTRODUCTION

A Blockchain is a peer-to-peer distributed ledger technology in which computers are connected in a network which stores the record of transactions made using any crypto currency in form of blocks.A block stores the record of a particular transaction and has a unique hash value. Each block in a Blockchain also stores the hash of the previous block which links all the blocks in a network. Transactions are safe and secure in a Blockchain as previous transaction records cannot be altered as this will change the hash of several blocks and all the systems/peers connect on that network does allow any modification. There are many crypto currency-based systems built using the Blockchain Technology and Ethereum is one such very popular system that allows us to create decentralized, immutable, transparent and encrypted applications. “Ether” is the currency of Ethereum. A crypto currency is a digital or virtual currency that is secured by cryptography and is immutable. Crypto currencies are peer-to-peerde centralized electronic currencies based on Blockchain technology. They are like traditional money but the only difference is that they do not have any physical form. Cryptography is a technique of encryption and decryption and is used in crypto currencies to make them more secure as no other can steal any information in between the transmission of data. Most essential feature of crypto currencies is that they are present in a limited unit which needs to be mined. Mining is the process of extracting crypto currency units and it consumes a certain amount of energy and processing power of the system.

Among all crypto currency-based systems Ethereum is one of the best as it is open-sourced and has almost minimal scarceness. It is preferred by developers for developing Blockchain based systems all over the world. Hence we can use Ethereum network to build a virtual transaction system in which the transaction records cannot be altered and modified. Also each and every step of the transaction can be automated i.e. between deposition and withdrawal of currency from the virtual wallet.There would be wide scope for this type of transaction system which is free from aberration as neither the transaction history can be altered nor can the currency in the wallet be incremented or decremented. With the completion of each transaction a block is created in the Blockchain which stores the hash, transaction data and the hash of the previous block, also the space for next block in the chain is created. As and when the hash of the block is established and if any data inside the block changes, the hash will change as well. Hence that will no longer remain the same block and all the blocks linked in the network will become unstable and all the previous block becomes in validas each block also stores the hash of previous block. It is because of this technique that the Blockchain is so transparent and secure. When a new block is created, the whole network becomes aware of it and each and every node checks and verifies whether the block is tampered with or not. Accordingly each node agrees upon whether to add that block on the network or not. This creates a consensus mechanism and the overall network decides according to it. To tamper with the whole network, one will have to tamper majority of the blocks in the network which is practically impossible as one would need to fool more than half of the network node which are in millions of number. A smart contract is a self-executing contract with terms of agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist

across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible. A Smart Contract holds all of the receiver's money until a certain condition is fulfilled.In our transaction system we will integrate a Smart Contract which will verify and monitor the condition for the deposit, withdrawal and for the registration purpose. The contact will automatically execute and will transfer the amount to the receiver when he delivers the proper work with all the conditions being fulfilled.

We are proposing a transaction system based on Blockchain Technology which can be used and integrated in many sectors like payments app, online payment system, banking systems, e-commerce website and apps etc. more securely and safely with very less effective waiting time unlike traditional payments system. Current systems are not free from ambiguity and data can be tampered with because of the involvement of third parties and humans for the validation and verification purpose which also consumes processing time. Our system is quick and automated whichcannot be tampered hence is safe and secure. Also the users would not have to stand in queues for the purpose of withdrawal and deposition of funds. We have used Blockchain Technology and Ethereum cryptocurrency in our system which will change the means of transaction system as compared to the current one.

Our system can perform the following functions:

- **Account creation**
- **Deposition of funds**
- **Withdrawal of funds**

Other features could also be included in the system easily but we will be demonstrating our system with the three basic functions required for the transaction.

II. LITERATURE REVIEW

A. *Blockchain Application in Banking System*

The authors of [2] this paper have explained the principal benefits of Blockchain in the banking sector. The benefits of the Blockchain are effectiveness, cost decrease, straightforwardness and removal of the outsiders in the current banking system. Because of the Blockchain records can be kept digitally and accessed in no time much quicker than the manual labour. The authors also explain how Blockchain can save exchange and activity costs. They also explain how current banking system are not completely safe and fraudsters can steal large amount of data and money.The major purpose of this research is to analysethe Blockchain system and find its use cases in the banking system.

B. *Online Payment Using Blockchain*

In [3] this paper the authors explain how the current payment gateways include various third party systems, which is time consuming process as transaction has to go through multiple third parties for verification which is major risk for transaction getting failed. They also put light on security factor and how the current system can be tampered by the hackers and can cause money loss and also the faith of the customers is lost. Then there come the transaction charges which is a concern for the customers which can be highly reduced using the Blockchain. Here the authors presented an online payments system based on Blockchain Technology.

C. *Ecommerce payment model using blockchain*

In research [4] the authors present the issues relating to current scenario of e-commerce payments gateway. Nowadays the use of e-commerce sites for the purpose of shopping is widely used because of the convenience of not going anywhere with which the online payment gateways are frequently used even for small amount of transactions. Most customers use credit cards and debit cards for the payment purpose and the payment gateways ensure integrityand nonrepudiation of card payments. This inevitably generates transaction fees as intermediary entities such as PG or value added network companies intervene in the payment process which is amajor issue when customers purchase an item of low price frequently and still they have to pay for the transaction fees. High volume of small payments are rapidly generating problems for the e-commerce market which leads to the issue of fees related to online transaction for the small businesses and customers. The authors presented the following main implications of their study:

- Decentralized authentication can be executed using the Blockchain system that contains agreements andtransactions between participating nodes through the Blockchain cryptocurrency system.
- A Blockchain payment technology is developed that ensures transaction integrity and nonrepudiation of transactions between participating nodes.

III. SYSTEM OVERVIEW

A. *Register an account*

Firstly the users needs to create an account for the purpose of using automated transaction system for the deposition and withdrawal of ethers. An identity is required just for the purpose of registration which the smart control will read and create a new account for the user. This account will let the user to add and withdraw ethers form the Ethereum wallet.

B. *Ether deposition*

After the creation of the user's Ethereum wallet account one can deposit ether to someone other's Ethereum wallet. The ethers deposited will go through the smart contract which will calculate the amount sent and will add to the receivers account.

C. *Ether withdrawal*

Upon the user's request for the required amount of ether from the smart contract, the smart contract will fetch the ethers from the Ethereum wallet and will send to the authorized personnel who will calculate the corresponding money and will hand over to the user.

IV. METHODOLOGY

A. *Implementation Tools*

The following technologies and tools were used in the implementation of the transaction system:-

- **Solidity**- for designing smart contracts.
- **Javascript** -for communicating with the smart contract in the backend.
- **Ganache library** - for establishing the local test network.
- **React.js** -in the design of the front end.
- **Node.js** - for runtime environment.
- **MetaMask** -for accessing Ethereum enabled apps.
- **Mocha** -a JavaScript framework for testing.
- **Rinkeby** - for test network.

B. *IMPLEMENTATION DETAILS*

A Smart Contract is created using solidity programming language. React has been used for creating the frontend which interfaces with the Smart Contract using it's contract address and bytecode. The Solc compiler is used for compiling the Smart Contract and JSON files are created corresponding to the Smart Contract. Smart Contract's function property is tested using the Mocha testing framework. Using infura.com which provides a Rinkeby test network URL. The JSON file contains the bytecode and ABIs for the Smart Contract. Truffle-HD-Wallet is used for the deployment of JSON file to the URL on the Rinkeby test network. Web3 acts as link between the front-end and Rinkeby test network. MetaMask is used for accessing the implemented Ethereum enabled DApp and manages all the transactions.

C. *Solidity for Smart Contract*

We have used Solidity programming language for creating Smart Contract which contains almost all the code and conditions required for the registration, deposition and withdrawal of ether. It uses the fileextension .sol.

D. *Solc Compiler*

It is the compiler used for the solidity language. It created the bytecode and an ABI when a Smart Contract is created. This bytecode and ABI is uploaded to the Rinkeby test network so that they can communicate with the Smart Contract.

E. *Front-end using React.js*

React is a JavaScript framework which is used for creating dynamic front-end web apps easily. Our system user interface has the capability for creating an account, deposition and withdrawal of funds.

F. *MetaMask*

MetaMask is a decentralized payment gateway and wallet used for running Ethereum DApps in our browser. It allows the users to access their Ethereum wallet with a user interface.

G. *Mocha*

Before deploying the Smart Contract to the Ethereum network it must be thoroughly checked and tested for various test cases for knowing it's proper functioning which will not result in any financial loss or system loss to the user. For this purpose Mocha a Node.js based JavaScript test framework is used.

H. *Rinke by test network*

Infura.com allows us to use the Rinkeby test network and allows us test our contact before deploying on the main network. Users need to register on Infura.com and after that they can access the test network and find the vulnerabilities in their DApps.

I. *Smart Contract for transaction procedures*

Smart Contract is a major and very important part of our system as it contains the terms and conditions for the process of registering, deposition and withdrawal. To register for an Ethereum based account one needs a minimum of 25 ether coins in their ether wallet.Funds will be deposited from users wallet to his bank wallet whenever the deposition function is called. The withdrawal function will check the required funds will perform the task of withdrawal. Whenever these functions are executed a transaction is initiated.

V. RESULT AND DISCUSSION

Here is the demonstration of our proposed transaction system which we have implemented which is free from data breach, financial loss, transaction delays and almost free from cyber attacks and hacking.Figure 1 shows the transaction process. Consider a user wanting to send funds to some other user, firstly he'll need to register for an account and for that the condition is that he must have a minimum of 25 ethers in his Ethereum wallet. If he has the required amount of ether than his account is created and now he can send money. He can enter the amount to send and than can proceed, the Smart Contract will process the transaction conditions and will automatically add the funds to the receiver's Ethereum wallet. Similarly if the first user wants to receive funds than he can request the other user and that user will send the requested funds from his wallet to the first user. Also the corresponding amount of money can be withdrawn from the bank after sending the withdrawal request for that amount to the bank and the required ethers will be deducted from the Ethereum wallet of the user.The interaction of the user and bank via the proposed transaction system is shown in below figure.

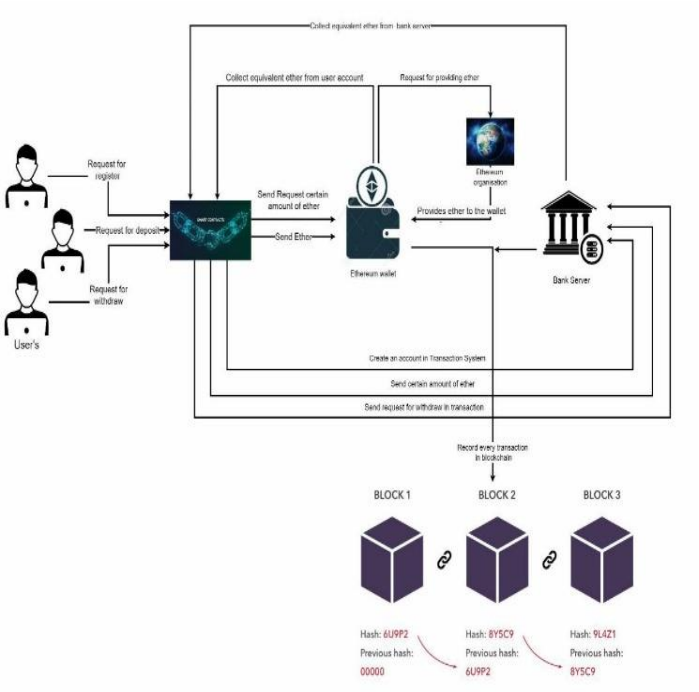

Figure 1: Interaction between bank and user via proposed transaction system

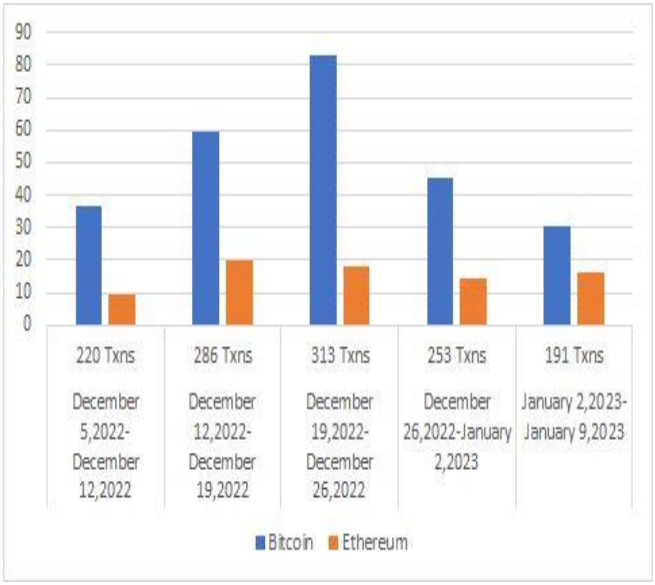

Figure.2: Complexity comparison using data

During the testing period we recorded the percentage price change of the Ether and Bitcoin which is represented by the line chart in figure 8. From the chart we can observe that the between two end points the percentage price change of ether is increasing and is positive while that of bitcoin is increasing but percentage change is less.

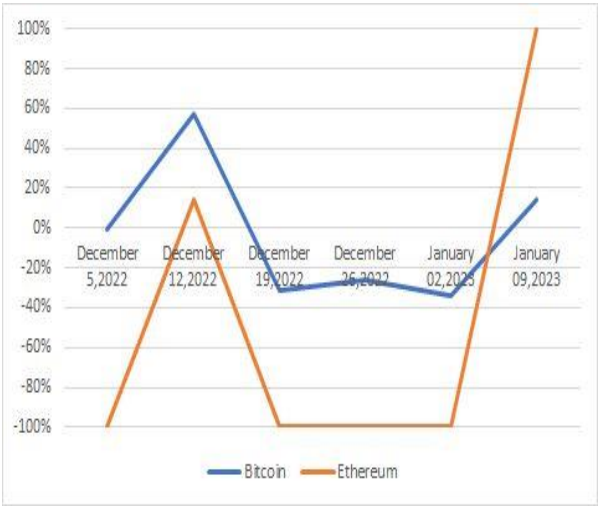

Figure.3: Percentage change in price of Ethereum and Bitcoin

With our proposed system we tried solving basic problems faced like confidentiality, fast and reliable transaction and data security while using conventional transaction systems. Our system is transparent as in case of transaction failure the funds automatically gets returned to the users wallet. The transactions take very less time and is gives a smooth experience. Moreover this system can be integrated with various platforms like payment gateways, e-commerce sites and banks for fast and secure transaction processes.

VI. CONCLUSION AND FUTURE SCOPE

This project is presenting a smart contract-based transaction system for Blockchain based transaction processes. This ensures that our system makes sure of the users funds and will never produce any financial loss at any cost. It is an improvement over the old manually managed transaction applications, e-commerce transactions and bank transactions. Ethereum based transaction system can make transactions fast, secure, immutable, decentralized, fraud free and transparent in various sectors. Banking sector can completely rely on this system for future as it can fulfill the needs of the cashless economy coming ahead. E-commerce sites and apps will experience more traffic as buyers will be able to buy even a small thing like a pencil online will very less transaction fee. Future real estate purchases can be done between the buyer and seller through tokenization. Finance companies will adopt the decentralized finance with which the investors will not have to deposit their funds with the central authority.

REFERENCES

[1] Nakamoto, Satoshi. *"Bitcoin: A peer-to-peer electronic cash system."* (2008).
https://bitcoin.org/bitcoin.pdf

[2] Chowdhury, M.U.,Suchana, K., Alam, S.M.E. and Khan, M.M.(2021) *Blockchain Application in Banking System.* Journal of Software Engineering And Applications, 14, 298-311.
https://doi.org/10.4236/jsea.2021.147018

[3] Thanapal, Karthikeya & Mehta, Dhiraj & Mudaliar, Karthik & Shaikh, Bushra. (2020). *Online Payment Using Blockchain*. ITM Web of Conferences. 32. 03007. 10.1051/itmconf/20203203007.
https://doi.org/10.1051/itmconf/20203203007

[4] Kim, SI., Kim, SH. *E-commerce payment model using blockchain. J Ambient Intell Human Comput* **13**, 1673–1685 (2022).
https://doi.org/10.1007/s12652-020-02519-5

[5] S. Sakho, Z. Jianbiao, F. Essaf and K. Badiss, "Improving Banking Transactions Using Blockchain Technology," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1258-1263, doi: 10.1109/ICCC47050.2019.9064344
https://api.semanticscholar.org/CorpusID:215799948

[6] Huaqunn Guo, Xingjie Yu,A survey on blockchain technology and its security,Blockchain: Research and Applications,Volume 3, Issue 2,2022,100067,ISSN 2096-7209,
https://doi.org/10.1016/j.bcra.2022.100067

[7] Wood, G., et al. (2014) Ethereum: A Secure Decentralized Generalised Transaction Ledger. Ethereum Project Yellow Paper, 151, 1-32.
https://ethereum.github.io/yellowpaper/paper.pdf

[8] Mohammed Shuaib, Noor Hafizah Hassan, Sahnius Usman, Shadab Alam, Surbhi Bhatia, Arwa Mashat, Adarsh Kumar, Manoj Kumar, "Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison", Mobile Information Systems, vol. 2022, Article ID 8930472, 17 pages, 2022.
https://doi.org/10.1155/2022/8930472

[9] V. Naik, R. Pejawar, R. Singh, A. Aher and S. Kanchan, "Expeditious banking using Blockchain Technology," 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), Keonjhar, India, 2020, pp. 1-6, doi: 10.1109/CISPSSE49931.2020.9212253.

[10] M. Wohrer and U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity," 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Campobasso, Italy, 2018, pp. 2-8, doi: 10.1109/IWBOSE.2018.8327565.

[11] Park S, Kwon A, Fuchsbauer G, Ga˘zi P,Alwen J, Pietrzak K (2015) SpaceMint:A Cryptocurrency Based on Proofs of Space
https://eprint.iacr.org/2015/528

[12] Gupta, Suyash & Sadoghi, Mohammad. (2021). Blockchain Transaction Processing.
https://www.researchgate.net/publication/353479319_Blockchain_Transaction_Processing