BLOCKEXCHANGE: CRYPTOCURRENCY EXCHANGE THROUGH BLOCK CHAIN

Shahanas M S, Shejina N M, Dr G.Kiruthiga

[1] *Student, Dept. of Computer science and Engineering, IES College of Engineering, Kerala, India*
[2] *Assistant professer, Dept. of Computer science Engineering, IES College of Engineering, Kerala, India*
[3] *Associate professer, Dept. of Computer science Engineering, IES College of Engineering, Kerala, India*

ABSTRACT

In recent years, the rapid rise of Blockchain technology and cryptocurrencies has shifted the financial industry, resulting in the birth of a new crypto-economy. The bitcoin blockchain is a fundamental component of a number of crypto-currencies. Blockchain technology provides the foundation for a variety of businesses, including cryptocurrency exchange, laundering of anti-money tracking systems, healthcare, real estate, supply chain, and logistics monitoring. The findings revealed that blockchain is a relatively new technology, and that nodes in the network share data without putting their trust in other nodes. Cryptocurrency is a peer-to-peer digital exchange system in which cryptography is used to generate and distribute currency units. People used cryptocurrencies for a variety of purposes, including trading, necessitating the establishment of a cryptocurrency exchange. Cryptocurrency exchange users profit from the fact that they can exchange money without having to rely on a centralized authority. Users in the crypto world purchase, sell, and exchange crypto coins in the blockchain network, which is one of the most important features of using this technology. A user can use an Ethereum smart contract to buy or sell ERC20 tokens in the decentralized distributed network with the swap. This paper will help people in the blockchain network in using swapping as a reliable and efficient method of trading crypto coins or tokens in the blockchain network. Smart contracts, which are computer protocols that automate the negotiation and enforcement of agreements between numerous untrustworthy parties, have enabled decentralized applications without the use of a trusted third-party. We also look at the creation of a block chain-based application that ensures that no one may change the code of the program.

Keyword : *blockchain, cryptocurrency, exchange, Ethereum, smart contract*

1. INTRODUCTION

Blockchain is the underlying technology of a number of digital cryptocurrencies. Blockchain facilitates peer-to-peer digital asset transfers without the use of intermediaries. Blockchain was first developed to support the well-known cryptocurrency Bitcoin. Bitcoin was proposed by Satoshi Nakamoto in 2008 and realized in 2009[1]. A sort of digital currency is referred to as cryptocurrency. It functions similarly to ordinary currency in terms of purchase, sale, borrowing, and lending. Nothing can be touched or sensed by us.

Intermediaries have played a critical role in financial transactions throughout the last decade. Through this Blockchain, Satoshi Nakamoto eliminates the necessity for intermediaries. The features of blockchain, including decentralization, immutability, transparency, and Auditability, make transactions more secure and tamper-proof. All other coins are referred to as altcoins instead of bitcoin. One of the examples is Ethereum. Smart contracts were designed for Ethereum to allow Turing-complete languages and automatic transactions, and they are frequently utilized in decentralized applications such as cryptocurrency exchange, supplychain, etc.

A cryptocurrency exchanger is a fully decentralized exchanger that can exchange quantities without the use of intermediaries and provides security because of the blockchain's safe transactions. The key benefits of this decentralized exchange are that it overcomes liquidity, transparency, and security issues. First, describe how the system functions generally. The remainder of the paper covers several fundamental concepts related to blockchain, cryptocurrencies, and system implementation.

1.1 Basics of Blockchain and Cryptocurrencies

A blockchain is a type of storage system that uses blocks to store information that is then linked together into chains and entered into a public ledger. Each block in the chain, including the genesis block, has a sequence number, a timestamp, the cryptographic hash of the block before it, some metadata, a nonce, and a number of successful transactions[Fig 1]. The hash function of the preceding block is saved in the new block whenever a new block is added. Every transaction from the transaction pool that is added to the blockchain is verified by miners[2]. Once this transaction is included to the block and verified by these miners, it becomes immutable. All transactions occur in a decentralized manner that eliminates the requirement for any intermediaries to validate and verify the transaction.

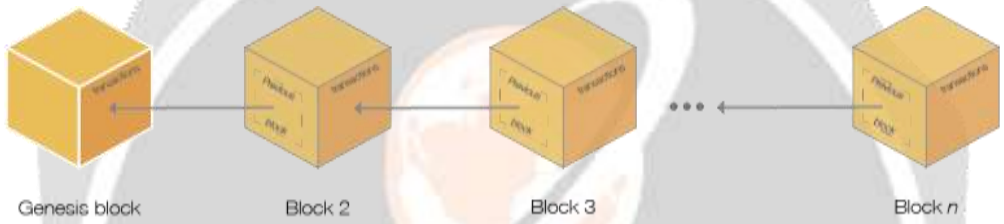

Fig 1: Block chain

Blockchain networks employ cryptocurrency as a digital medium of exchange. It is a peer-to-peer digital exchange system where currency units are created and distributed using cryptography. Cryptocurrencies have emerged as important financial software platforms. Mining is a crucial component of such systems, which rely on a safe distributed ledger data. Because they were created as peer-to-peer systems, cryptocurrencies do not have a central authority to mediate transactions.

Bitcoin is the first fully functional decentralized cryptocurrency. Peer-to-peer currency systems have been discussed in published articles in the past, but none have been put into practice. Following the popularity of Bitcoin, numerous new cryptocurrencies, including Ethereum and ripple Litecoin[6], were created. The way that cryptocurrencies operate is as follows: A created address is in the user's wallet. As a public key, this address is used. A generated private key that is used to sign transactions and demonstrate ownership is also stored in the wallet. While signing the document with their private key, the payer pays money to the payee's address. Mining is used to verify each of these transactions. Various consensus algorithms are used for mining cryptocurrency.

2. RELATED WORKS

An Ethereum Blockchain was utilized in this decentralized cryptocurrency exchange. In 2014, Ethereum[3] was funded by the public. Although it also uses Proof of Work, Ethereum does not employ a pre-existing hash algorithm. The designers created EtHash[4], a custom hashing algorithm. The main goal of creating a new Proof of Work function rather than using an existing one was to alleviate the issue of mining centralization, in which a few hardware companies or mining operations might amass an excessive amount of power to influence or control the network. Externally Owned Accounts (EOA) and Contract Accounts(CA) are the two types of accounts available for Ethereum. While CA symbolizes a smart contract(SC), EOA is required to participate in the Ethereum network and interacts with the blockchain using transactions.

In essence, a smart contract is an Ethereum client with the same permissions and capabilities. But it is run by a random piece of code created for the Turing complete Ethereum Virtual Machine(EVM), not by a person. The combination of the Ethereum account and the program running on it is what we refer to as a Smart Contract. Every contract's Ethereum address can be used to identify it, just like a regular Ethereum user can. Typically, smart contracts are written in the higher level programming language called Solidity [5] rather than directly in the EVM assembly code. Smart contracts operate in the open on Ethereum's blockchain, unlike traditional programs. A smart contract may be created by anyone, and once it is written and deployed, it cannot be changed. In Ethereum, gas or fuel is needed for every operation. For convenience of calculating, gas is used as payment instead of ether. The key justification for this is that gas is a coin with a value independent of transaction and computation fees.

2.1 Existing system

In transitional or emerging nations, two currencies are regularly in use as a medium of exchange. Currency exchange is nevertheless done in spite of this. By imposing currency limitations and setting transaction procedures that favor the local currency, governments can encourage private agents to engage in currency exchange in order to recover their home currency. Converting one currency into another is known as a currency exchange. Several fiat currencies, including the dollar, rupee, dinar, and others, are currently exchanged. The criteria for exchanging are determined by the exchange rate. The exchange rate is the value of one currency in relation to another.

Fig 2: Existing currency exchange system

Intermediaries are used in every currency trade currently taking place. The price of the transaction is heavily influenced by middlemen. A centralized authority oversees every transaction. Every step of the transaction can be managed by them. the Ethereum blockchain will be used to solve this issue. As a result, we can exchange the amount with the press of a button and bypass middlemen. All of these transactions happen without the need for a centralized authority. Furthermore, it prevents problems with security, transparency, and liquidity.

3. DECENTRALIZED CRYPTOCURRENCY EXCHANGE

We can exchange cryptocurrencies without the help of middlemen because of the fully decentralized method we have presented. Instant, secure, and irreversible payment services are provided by Ethereum. Merchants can considerably reduce their costs and increase their profitability because of its low transaction fees. Here, Ether is being exchanged for an ERC-20-based coin. A form of cryptocurrency known as a token operates on a distinct blockchain network. The network reaches "consensus" that your transaction is valid whenever you transmit cryptocurrency, and your balance is correctly updated on the public ledger. The front end website of the application is connected with the aid of HTML, CSS, and JS. Instead of using a back-end server, this website communicates directly with the blockchain. The application's whole code base, data, and code reside here. Solidity is the programming language used throughout the entire smart contract. These smart contracts cannot be altered. The public ledger, which is likewise immutable, contains all of the data. It will always be possible for the public to verify any new data that we post to the blockchain.

3.1 Tool used

1) Metamask: The Metamask addon for Google Chrome is the requirement. It serves as a connection between a browser and an Ethereum blockchain. To use the Ethereum block chain, users will need to install a special browser extension. Metamask comes to the rescue in this situation. With users personal account, user's will be able to connect to local Ethereum blockchain and communicate with smart contract. To install Metamask, visting the Google Chrome online store and look for the Metamask Chrome plugin. When it's installed, a fox icon will be visible in the upper right corner of Chrome browser. For connecting of metamask to ganache as a first step, a custom RPC was added to establish the connection. As a result, the RPC server address received from ganache and a network id provided by ganache are used. With 100 ethers available, the ganache account can be imported to metamask.

Metamask also provides a software platform for serving Ether or other ERC-20 assets. At the same time, it also helps you interact with Ethereum decentralized apps. The browser-based functionality delivers a potential boost to ease of use for Metamask. This application link with Metamask for selling and buying ERC20 token and ETH. Users can also use Metamask for saving keys for ETH & ERC20 tokens. Metamask has the capability of interacting with various Ethereum test networks, thereby making it a suitable wallet for blockchain developers. After the installation of the app in the browser, users can have an in-built Ethereum wallet at their disposal.

2) Ganache: As a blockchain tool from the Truffle Suite. Ganache enables blockchain developers to create their own private Ethereum blockchain for testing dapps, inspecting state, and executing commands with providing full control of the operation of the chain. It will provide us with 10 external accounts with Ethereum addresses on the local blockchain. Each account comes with 100 ethers. Each project will be divided into six sections. Accounts, blocks, transaction, contract, events and logs are all types of data. The most important characteristic of Ganache is that it enables users to perform all the actions that could be performed on the main chain, without making any payment for the same. Ganache is a very popular Blockchain tool among developers as it provides a number of options such as built-in block explorer and advanced mining controls. Blockchain developers use Ganache for testing their smart contracts during the process of development.

3) Truffle: One of the notable competitors among the top blockchain tools refers to Truffle[10]. It is an Ethereum blockchain framework tailored for establishing a development environment to facilitate the development of Ethereum-based solutions. Truffle also includes a massive library of custom deployments that support writing new smart contracts and resolve challenges in blockchain development. In addition, Truffle is also ideal for the development of complex Ethereum decentralized apps. Another prominent functionality of Truffle as a blockchain tool is automated contract testing. Truffle can leverage Mocha and Chai for automated contract testing. Furthermore, Truffle can also help in enabling the development of smart contracts followed by linking them and their compilation and deployment. Most important of all, Truffle also facilitates a configurable build pipeline to ensure the execution of custom build procedures.

3.2 Implementation

Ten accounts are automatically assigned to each project in Ganache. Each account has a distinct index and an equally distinct address that may be used to identify it. For each transaction completed on a certain account, the number of transactions will increase from zero to one, allowing the total number of transactions to be determined. Ether will be depleted in accordance with the transaction. Here, we are converting ETH into ERC-20 tokens[8], hence two smart contracts are required. one for the token exchange and one for the Ethereum exchange.

One of the most well-liked tokens that may be purchased, sold, and even traded is the ERC-20 token. It resembles other cryptocurrencies like Bitcoin, Ether, etc. You must realize that Ether and ERC-20 are not the same thing, though. ERC-20 is a standard for a particular kind of token, whereas Ether is the actual native currency of the Ethereum network. As a result, other developers can utilize this standard to produce new ERC20 tokens, each of which will have a unique token name. we can simply create token with its mandatory rules. Any smart contract that wants to use the ERC-20 token must adhere to certain guidelines or ERC standards. In other situations, it won't be appropriate to refer to it as an ERC-20 token if you break the regulations.

The final smart contract that is required for automatic test operation is this one, in which we describe the value of each currency and how sell and buy work. We should launch Ganache before deploying these smart contracts. Otherwise, it will not function. If this contract is implemented on our blockchain, the account's gas cap will be reduced. The front end of the application must then be connected to the blockchain. The Metamask additional web extension for this. Reactjs is used to build every client-side website, which communicates directly with two Ethereum contracts stored on the blockchain. We must import one account private key from the Ganache account to Metamask in order to connect the blockchain with the latter. thereafter, we can view the balance of that account in metamask. Run this program, then use the ETH associated with those accounts to purchase tokens to later sell for ETH.

3.3 Advantage of the system

- Without any additional intermediaries, this is a fully decentralized system. Both transaction costs are decreased, and liquidity is maintained.

- Blockchain offers strong security since blocks are linked to one another, thus if a hacker tries to change any block, the block's hash function will change.
- There is no need for a centralized authority because all transactions are recorded in a public ledger.With just one click, we can transfer any amount. It results in improved performance and reduced process.

4. CONCLUSIONS

Blockchain technology can change the paradigm for decentralized business models by lowering transaction costs, broadening the scope of transactions, and enabling peer-to-peer transactions. Decentralized finance, which uses blockchain technology to establish an alternative financial system that can be more decentralized, inventive, interoperable, borderless, and transparent, has emerged as a result of this new paradigm. Smart contracts' decentralization, auto-enforcing capacity, and verifiability enable the execution of their encoded business rules in a peer-to-peer network where each node is "equal" and none has any particular authority without the need for a central server or trusted authority. Thus, it is anticipated that smart contracts would alter a number of established sectors, including finance, healthcare, energy, and others. Additionally, in order to improve speed, cryptocurrencies are experimenting with their mining protocols and algorithms, and some are looking for mining-alternatives. They might push scientists to develop fresh hypotheses to account for the potential advantages and disadvantages of decentralization. The fundamentals of blockchain technology and its structure were covered in this paper. The usage of smart contracts makes the Ethereum blockchain powerful. Due to the immutability of smart contracts, they are highly useful in decentralized applications. This smart contract makes it incredibly easy and safe to exchange two coins. This study addressed the overall software dependencies and implementation of this decentralized exchange. We may purchase and sell cryptocurrencies directly with this application without using middlemen.

5. REFERENCE

[1] S.Nakamoto *et al.*, *Bitcoin: A Peer-to-Peer Electronic Cash System*.Citeseer, 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[2] A. Kroll, I. C. Davey, and E. W. Felten, ``The economics of bitcoin mining,or bitcoin in the presence of adversaries," in *Proc. WEIS*, Jun. 2013,p. 11.

[3] Gavin Wood. Ethereum: A secure decentralised generalized transaction ledger. Ethereum Project Yellow Paper,2014.

[4] Anonymous. Ethash. https://github.com/ethereum/wiki/wiki/Ethash, 2014.Reference 4

[5] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. “A Survey of Attacks on Ethereum Smart Contracts (SoK)”. In: International Conference on Principles of Security and Trust. Springer. 2017, pp. 164–186

[6] C Lee. Litecoin, 2011.

[7] Blockchain smart contract:Applications, challenges, and future trends S N Khan, F Loukil, C Ghedira-Guegan, peer- to –peer Networking,2021-spinger

[8] ERC20 Token Standard, available at: https://theethereum.wiki/w/index.php/ERC20_Token_Standard

[9] Blockchain technology, bitcoin, and ethereum: A brief overview D Vujicic, D Jagodic, S Randic -2018 – ieeexplore.ieee.org

[10]Truffle, [Online]. Available: https://www.trufflesuite.com/docs, 2019.

[11]Visual Studio Code, [Online]. Available: https://code.visualstudio.com/, 2019.

[12] Solidity, [Online]. Available: https://solidity.readthedocs.io/en/v0.5.11/, 2019

[13]A survey of blockchain from the perspectives of applications, challenges, and opportunities AA Monrat, O Schelén, K Andersson - IEEE Access, 2019 – ieeexplore.ieee.org

[14]Blockchain disruption and decentralized finance: The rise of decentralized business models Y Chen, C Bellavitis - Journal of Business Venturing Insights, 2020 – Elsevier