IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DECENTRALIZED BLOCK CHAIN MONEY TRANSACTION SYSTEM

Dr.M.Kalaiarasu, Rithika S, Shamini V, Subha V

Assistant Professor, UG Scholar, UG Scholar, UG Scholar
Information Technology,
Sri Ramakrishna Engineering College, Coimbatore,Tamil Nadu

Abstract: As information technology advances and is used more widely, blockchain technology (BT) is emerging as a key tool for advancing the integration of the physical and digital economies. BT has advanced to a point where it can be used for finance, traceability, and asset transactions. But there isn't a practical application framework or trading method for using BT in decentralized transactions offered by current technology. This article proposed a blockchain-based decentralized transaction method, which we simulated using Python(flask) programming language. This is achieved by implementing a decentralized system that eliminates the need for intermediaries, reducing delays and transaction costs. This system provides an intuitive user experience accessible to a wide range of users, including those unfamiliar with complex financial systems or technology. Through the use of blockchain technology, this project aims to redefine the way decentralized transactions are conducted, offering a secure, efficient, and user-friendly alternative to traditional methods.

Index Terms - Decentralized System, Python(flask), Block chain Technology

I. INTRODUCTION

In today's digital age, global economy entered the stage dominated by the information industry.The rapid growth and implementation of information technology, including blockchain technology, artificial intelligence (AI), and the Internet of Things (IoT), has resulted in a deepening and transformation of the global economy and industry structure.
It is imperative that industry development undergo a digital, networked, and intelligent transition.To create a new industrial system pillar and move up the global value chain, it is important to support the integration and growth of the real economy and the digital economy.

The field of mobile electronic commerce (M-commerce) has grown rapidly in the last few years, and electronic commerce (E-commerce) has also become much more influential.Globally, e-commerce is a significant driver of economic growth. One significant driver of global economic growth is e-commerce. In e-commerce, the coordination and efficient handling of many transactional elements, such as participants, finances, and materials.

A modern market economy is primarily a type of credit economy.Credit is the basis for the proper operation of the market economy and the presumption of commodity exchange. Furthermore, decentralization is necessary in the digital economy in addition to a reliable value delivery mechanism. Currently, manufacturing, distribution, and maintenance of electronic payment methods are left to a third party (banks, e-commerce platforms, etc.). Although the centralized architecture makes management and regulation easier, system security is impacted.

BT is characterized by its decentralized architecture and tamper-proof method. It can be used for smart contracts, e-commerce, and other things. To guarantee data confidentiality and transparency, a blockchain-based Peer-to-Peer (P2P) transaction contract can be created. Smart contracts are usually used to exchange digital assets Haibo Tian et al.11 of Sun Yat-sen University proposed a blockchain-based method for signing a fair contract. Transaction information cannot be disputed, and BT is used to verify the security of the conditions of the agreement between the two parties.

BT is often at a specific stage of development when it comes to financing, traceability, and asset transactions. However, there is currently no suitable trading mechanism or application framework for the application of BT to P2P transactions. Thus, this paper intends to apply to smart contracts and electronic transactions in light of the existing issues, and build a P2P transaction method based on blockchain.

Overall, this paper presents a comprehensive framework for the block chain based peer to peer transaction. This project involves creating a user interface and integrating it with blockchain. The user interface is created with basic and simple web technologies such as HTML, CSS, JavaScript and Angular JS.

II. RELATED WORKS

Smart Contracts: security patterns in the Ethereum ecosystem and solidity

Blockchain-based smart contracts are gaining a lot of interest from the scientific community and new business applications because they remove the need for a trusted third party by enabling untrusted parties to manifest contract terms in program code. Writing secure and functional contracts in Ethereum, the most popular smart contract platform available today, is a challenging undertaking. Science and industry have only recently begun to conduct research on this subject. We have developed numerous typical security patterns based on an analysis of gathered data using Grounded Theory methodologies, which we explain in detail using Solidity, the primary Ethereum programming language. The patterns that are provided provide solutions to common security problems and are applicable.

Ethereum is a major blockchain-based ecosystem that provides an environment to code and run smart contracts. Writing smart contracts in Solidity is so far a challenging undertaking. It involves the application of unconventional programming paradigms, due to the inherent characteristics of blockchain based program execution. Furthermore, bugs in deployed contracts can have serious consequences, because of the immediate coupling of contract code and financial values. Therefore, it is beneficial to have a solid foundation of established and proven design and code patterns that ease the process of writing functional and error free code.

Bitcoin:A peer- to- peer Electronic cash system

Online payments might be transmitted straight between parties without passing through a banking institution if electronic cash was only available peer-to-peer. Digital signatures help, but if a reliable third party is still needed to stop double-spending, the primary advantages are negated. We provide a peer-to-peer network-based solution to the double-spending issue. By hashing transactions into a continuous chain of hash-based proof-of-work, the network creates a timestamp that cannot be altered without repeating the proof-of-work. The longest chain is evidence of the order in which the events were seen as well as the source of the greatest amount of processing power.Online payments could be made using an electronic cash that is solely peer-to-peer.

Blockchain -Based Smart contracts:A systematic mapping study

Smart contracts are a compelling aspect of blockchain technology. Executable code that operates on top of the blockchain and allows an agreement between untrusted parties to be facilitated, carried out, and enforced without the need for a trusted third party's intervention is known as a smart contract. In this work, we gather all the technical research related to smart contracts through a thorough mapping analysis. By doing this, we hope to determine the hot subjects and unresolved issues in smart contract research going forward. 24 publications are extracted from various scientific databases. The findings indicate that identifying and resolving smart contract issues constitutes almost two thirds of the articles. It is determined that there are four main concerns: privacy, security, codification, and performance.

The remaining papers concentrate on applications of smart contracts or other subjects connected to smart contracts. Here are several research gaps that need to be filled in further investigations.

In most existing systems, parties perform transactions in a centralized manner that necessitates the engagement of a reliable third party, such as a bank. On the other hand, this might lead to expensive transaction costs and security problems (like a single point of failure). In order to address these problems, untrusted actors can now engage with one another in a distributed manner without the assistance of a reliable third party thanks to blockchain technology. Blockchain is a distributed database that keeps track of every network transaction ever made. Blockchain was first presented in connection with the peer-to-peer digital payment system known as Bitcoin, but it later developed into a framework for creating a variety of decentralized applications. Smart contracts are a compelling application that can be implemented on top of blockchain technology.

Executable code that operates on the blockchain to enable, carry out, and uphold the conditions of an agreement between untrusted parties is known as a smart contract. It can be compared to a system that, upon fulfillment of certain regulations, transfers digital assets to all or some of the parties involved.Smart contracts have lower transaction costs than regular contracts since they don't depend on a reliable third party to function. While there are several blockchain systems available for creating smart contracts, Ethereum is the most widely used. This is due to Ethereum's programming language's support for the Turing-completeness feature, which enables the creation of more complex and customized contracts.

In the literature, smart contracts have been defined in a variety of ways. The definitions in were categorized by the author into two groups: smart contract code and smart legal contract. "Code that is stored, verified, and executed on a blockchain" is what smart contract code is. The blockchain's capabilities and the programming language used to write the contract determine this smart contract's functionality. Code that completes or replaces legal contracts is referred to as a smart legal contract. The ability of this smart contract is contingent upon the legal, political, and business establishments rather than technology.

III. RESEARCH METHODOLOGY

Our study aims to develop a decentralized transaction model with an immutable cryptographic signature called an hash. A decentralized network is a network configuration where there are multiple authorities serving as a centralized hub for participants. In the computing world, a decentralized network architecture distributes workloads among several machines instead of relying on a single central server.This section speaks about the decentralized system.

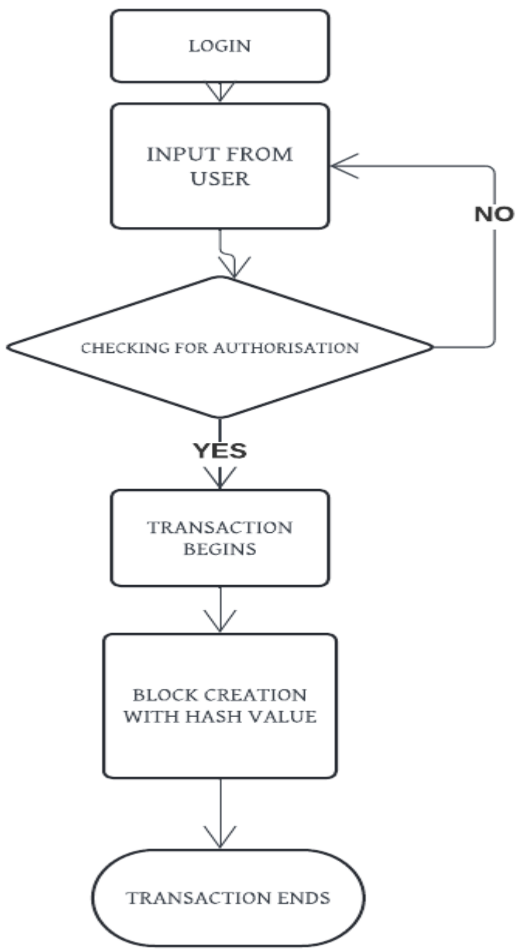

Fig. 1. Work flow diagram

A. *Decentralized system*

Decentralized systems in blockchain operate based on the principles of distributed ledger technology (DLT), where transactions are recorded across a network of nodes without the need for a central authority. Transactions are recorded on a distributed ledger, which is a decentralized database shared among all nodes in the network.Each node maintains a copy of the ledger and independently verifies the integrity of transactions using cryptographic algorithms.

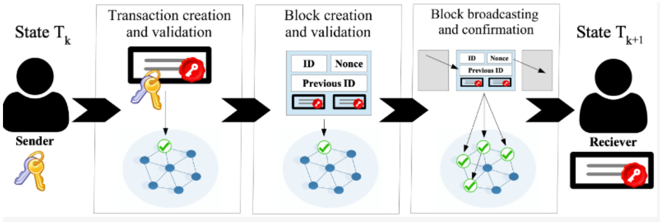

Fig. 2.Decentralized system architecture for blockchain transaction

B. *Blockchain implementation*

The following section gives the brief explanation of the block of code:

```
class Blockchain:
    diff = 10
    maxNonce = 2**32
    target = 2**(256-diff)

    block = Block("Genesis text", "Genesis")
    dummy = head = block

    def add(self, block):
        block.previous_hash = self.block.hash()
        self.block.next = block
        self.block = self.block.next

    def mine(self, block):
        for n in range(self.maxNonce):
            if int(block.hash(), 16) <= self.target:
                self.add(block)
                print(block)
                return block.blockName,block.data
            else:
                block.nonce += 1
```

Fig. 3. Class definition

The class blockchain defines diff, maxNonce, and target: These are class attributes that define the difficulty level of mining, maximum nonce value, and the target hash value required for mining a block.block, dummy, and head: These are instance attributes representing the first block (genesis block) of the blockchain. dummy and head are used as pointers to the first block.add(self, block): This method adds a new block to the blockchain. It sets the previous hash of the new block to the hash of the current block, links the current block to the new block, and then updates the current block pointer to the new block.mine(self, block): This method simulates the process of mining a block. It iterates through nonce values until it finds a hash value that meets the target criteria. If such a hash is found, the block is added to the blockchain using the add method. Otherwise, the nonce value is incremented and the process continues.

```
app = Flask(__name__)
blockchain = Blockchain()
my_dict = []

@app.route('/')
def my_form():
    return render_template('index.html',content = "")

@app.route('/',methods=['POST', 'GET'])
def my_form_post():
    PayeeName = request.form['PayeeName']
    AmountTransfer = request.form['AmountTransfer']

    nm, tx = blockchain.mine(Block(AmountTransfer, PayeeName))
    my_dict.append([nm,tx])
    return render_template('index.html', name_list = my_dict)

if __name__=="__main__":
    app.run(debug=True)
```

Fig. 4. Setting up Flask application

The Flask framework is imported to create the web application. An instance of the Flask app is created. An instance of the Blockchain class is created, assuming it's defined elsewhere. An empty list my_dict is created to store transaction data.Two routes are defined: The '/' route renders the index.html template when the application is accessed via a web browser. It displays a form for user input. The same '/' route handles form submissions via POST method. It retrieves PayeeName and AmountTransfer from the submitted form, mines a new block using the blockchain, appends the transaction data to my_dict, and renders the index.html template with the updated name_list. The app.run(debug=True) statement runs the Flask application in debug mode. Make sure you have a template file named index.html in the templates directory (templates/index.html). This template should contain

HTML code for rendering the form and displaying transaction data. Additionally, ensure that the Blockchain and Block classes are defined properly in a separate Python file named blockchain.py (assuming they are not defined within the same file).

C. *Incorporation of blockchain with web application*

Incorporating a blockchain with a web application can be a powerful way to leverage the decentralized and secure nature of blockchain technology in various use cases. Below, I'll outline steps on how to integrate a basic blockchain into a Flask web application: Define the Blockchain: Create a Python file and define the Blockchain class along with the Block class. Implement methods for adding blocks to the blockchain, mining blocks, and verifying the integrity of the blockchain.

Setting Up the Flask Application :Create a Flask application (e.g., app.py) to serve as the web interface for interacting with the blockchain.Define routes for rendering HTML templates and handling form submissions.

Create HTML Templates:Design HTML templates to display forms for user input and to visualize blockchain data. Use Jinja2 templating engine to dynamically render blockchain data within HTML templates. Interact with the Blockchain: Implement Flask route handlers to process form submissions, mine new blocks, and display blockchain data. Use Flask's request object to retrieve data submitted through HTML forms.

As we can see, the decentralized blockchain is integrated with the web application money transaction system .

IV. RESULTS AND DISCUSSION

In conclusion,the use of blockchain technology in peer-to-peer transactions offers significant benefits such as increased security, transparency, and efficiency. By leveraging blockchain, transactions can be conducted securely and transparently without the need for intermediaries, reducing costs and processing times. The project demonstrates how blockchain can be used to create a decentralized platform for peer-to-peer transactions, ensuring that transactions are secure and transparent. By breaking down the project into modules, we were able to focus on each aspect of the project individually, making it easier to develop and manage. In the future, blockchain-based peer-to-peer transaction systems could be integrated with other blockchain applications, such as supply chain management or digital identity verification, to create a comprehensive decentralized ecosystem. Additionally, the system could be further developed as a mobile application, making it more accessible and convenient for users to conduct peer-to-peer transactions securely and efficiently.

REFERENCES

[1] A. Hari and T. V. Lakshman, "The internet blockchain: A distributed, tamper-resistant transaction framework for the internet," Proc. 15th ACM Workshop on Hot Topics Netw., Nov. 2016, pp. 204–210.

[2] Woher,M.,$Zdun, U.(2018).Smart contracts:security patterns in the Ethereum eco system and solidity.2018 International Worshop on Blockchain Oriented Software Engineering (IWBOSE).doi10.1109/iwbose.20188327565

[3] J. Li, J. Wu, and L. Chen, "Block-secure: Blockchain based scheme for secure P2P cloud storage," Inf. Sci., vol. 465, pp. 219–231, 2018

[4] C. Lu, P. Huan, Y. Zhang, and Y. Huang, "Blockchainbased secure trading method and system," CHN Patent 106845960A, Jun. 13, 2017

[5] H. Tian, J. He, and L. Fu, "A privacy preserving fair contract signing protocol based on block chains," J. Cryptologic Res., vol. 4, no. 2, pp. 187–198, 2017

[6] P. Gomis-Porqueras and D. Sanches, "Optimal monetary policy in a model of money and credit," J. Money, Credit Banking, vol. 45, no. 4, pp. 701–730, 2013.

[7] . J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," IEEE Commun. Surv. Tut., vol. 17, no. 3, pp. 1294–1312, Jul./Sep. 2015

[8] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Comput. Netw., vol. 76, pp. 146–164, 2015.

[9] A. Alsaad, R. Mohamad, and N. A. Ismail, "The moderating role of trust in business to business electronic commerce (B2B EC) adoption," Comput. Human Behav., vol. 68, pp. 157–169, 2017.

[10] L. E. Gillies. Electronic Commerce and International Private Law: A Study of Electronic Consumer Contracts. Evanston, IL, USA: Routledge, 2016.

[11] B. Yoo and M. Jang, "A bibliographic survey of business models, service relationships, and technology in electronic commerce," Electron. Commerce Res. Appl., vol. 33, 2019, Art. no. 100818

[12] N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by blockchain: Safeguarding internet of things devices," IEEE Consum. Electron. Mag., vol. 8, no. 3, pp. 28–34, May 2019.