Kalpa Publications in Computing
Volume 19, 2024, Pages 365–375
Proceedings of 6th International Conference on Smart Systems and Inventive Technology

A Decentralised Escrow Protocol for Enabling Secure Transactions between Trustless Parties

Sandadi Deepak Reddy[1], Kukkala Sathvik[2], R. Vignesh[3]

[1, 2]Student, Department. Of Computer Science Engineering (B.E.) Sathyabama Institute of Science and Technology Chennai, India
[3]Assistant professor, Department. Of Computer Science Engineering (B.E.) Sathyabama Institute of Science and Technology Chennai, India
[1]deepaksandadi@gmail.com, [2]Sathviknani1703@gmail.com,
[3]vignesh.cse@sathyabama.ac.in

Abstract

This study has proposed a new transaction method for people, who don't trust one another to send secure money by using a decentralized escrow technology. The proposed protocol takes an escrow, a third-party smart contract to receive tokens before a transaction get completed. The tokens will be released by the escrow upon fulfilment of the payment requirements. Delivering the agreed-upon commodity or service and paying the associated payment are the obligations of each party to perform a transaction. It should not be possible for one side to pull out a bargain at the cost of the other. The Escrow may be provided with the necessary information by using the oracle pattern if the conditions of payment are contingent on external data, such as the time of product shipment. Once a smart contract's code is recorded on the blockchain, it cannot be changed. This guarantees the safety of the escrow feature.

Keywords**:** Decentralized, accountable, transparent, blockchain, escrow, smart contracts

1. Introduction

In a proposal for Bitcoin published in October 2008, the idea of Blockchain was introduced to the public to establish a decentralized, peer-to-peer (P2P) currency, which would function independently of traditional financial institutions. Bitcoin presented a new way to solve the age-old issue of trust between people. Because of blockchain technology, we may place faith in the system's results even if we don't have faith in any of its participants. Proof-of-work serves as the consensus mechanism for the distributed ledger. Incentives in the market and secure communication are at the heart of this system. Blockchain is a that can be viewed by anyone but is controlled by no one.

P2P, or peer-to-peer, refers to a type of decentralized network communications paradigm in which a collection of independent with no server or admin in charge, where all the nodes in this network are equally important and do the same work when it comes to peer-to-peer communication. Structured, unstructured, and hybrid peer-to-peer networks are the three main types of P2P architecture, each of which is well suited to specific use cases. Nodes in an unstructured peer-to-peer network connect to one another at random, creating a network that is less efficient than a structured one. Each node in a well-organized peer-to-peer system may quickly and easily search the network for any information it needs. The overall performance of hybrid networks, which combine elements of P2P and client-server models, is typically higher than that of either purely P2P or purely unstructured P2P systems.

It is believed that 300 million people around the world utilize cryptocurrency. Bitcoin, the most widely used cryptocurrency, was designed to be used in private, direct, and anonymous value transfers between its users, bypassing traditional intermediaries like banks and brokers. The is based on this decentralized, peer-to-peer approach. Investors in start-ups now have more say over their money thanks to Escrow Protocol, a Blockchain-based Web3 platform. Milestones are achieved before funding is provided for a project. We protect investor money by using the tried-and-true method of placing it in escrow, from which distributions are made upon the completion of certain milestones in the project.

Global investment nowadays is leveraging day by day. It fragmented the way of sustaining the world. The massive growth in technology has played a key role in making the system easy and smooth. Business leaders and employees mostly get benefitted from this. The p2p payment gateway with escrow protocol has a huge potential for users. Specifically, businesses are on the verge of making it more effective and smarter. Peer-to-peer (P2P) systems are distributed, peer-to-node (P2N) networks that connect various computer systems. Therefore, there is no need for a centralized server. When a node takes on the role of client, it receives data from the network's servers; when it serves as a server, it can itself become a source of data downloads.

The sharing, downloading, and transferring of data is facilitated by all connected nodes. P2P refers to the fact that a transaction is made directly between two peers rather than through a third party. Without going through a central server or administrator, data can be transferred directly between nodes in a network. As was previously mentioned, nodes act the in the network. opposed to the more conventional client/server architecture, P2P networks allow users to directly access the resources they need rather than going through an intermediary server.

P2P architecture is the backbone of blockchain technology and is responsible for handling all cryptocurrency transactions. Cryptocurrencies are decentralized digital currencies that operate on a blockchain to facilitate instantaneous transactions between users.

It's obvious that blockchain is a game-changing technology, but how can mobile developers take advantage of it? P2P mobile payment and security is an area where many new opportunities are opening. When compared to a centralized system based on a trusted server, peer-to-peer mobile payments (and other transactions or communications) are fundamentally less secure. Without the need for a central server, a network of computers and other devices can work together in a "peer-to-peer" setup to share and store data. When it comes to transmitting information, this creates a major security risk. Data kept on a also particularly vulnerable because such nodes typically lack the encryption capabilities and high-level security controls that would be in place on a centralized server.

For P2P to work, all it takes is a commitment to a single, fundamental principle: the idea of decentralization. Blockchain's decentralized, peer-to-peer design facilitates global, instantaneous transactions for all cryptocurrencies without a trusted third party or centralized server. Anyone who wants to help validate Bitcoin blocks as they are added to the blockchain can do so by installing a node on the decentralized. Blockchain ledger records transactions for many digital assets in a system. networks, in which all nodes are interconnected and keep their own copies of the ledger and check against one another to make sure the data is correct, are what we mean when we talk about peer-to-peer networks. This is not like a bank, where your transactions are safely hidden away and only the bank has access to them.

The various advantages of P2P networks have led many programmers to adopt them, or at least consider using them, when building mobile applications. It's highly improbable that hundreds or thousands of nodes in a peer-to-peer network would all fail at once, making these networks speedier and more stable. P2P networks are easy to set up and require little in the way of resources to keep running. Developers may now safely take advantage of the benefits of a peer-to-peer mobile network thanks to blockchain technology. Moreover, consumers' faith in the app is bolstered by this extra layer of protection.

In the past several months, we've seen a rise in the number of mobile apps that use blockchain. The Glyph is an online marketplace where users may purchase and sell goods with the use of blockchain-based transaction verification and security. Another major company, The Fold, is implementing blockchain technology to enable customers to shop at major businesses like Whole Foods and Target for necessities like food, cleaning supplies, and furniture. Financial transactions are just the beginning of what may be done with blockchain technology. Thanks to a collaboration with Circle, blockchain-based payments are now available on Apple devices running iOS 10. This allows for the creation of brand-new peer-to-peer mobile payment apps that are compatible with Apple devices.

2. Literature Review

[1] Haya R. Shahib and Khaled Saleh, "Coin-based tangible proof delivery system," Khalifa University's electronics department conference, 2018.

To identify a decent solution, the survey was a really excellent approach. It is advisable to review every notion associated with it. A dependable way to ensure the prompt delivery of ordered items is more crucial than ever in this era of ubiquitous internet shopping. Regretfully, there is currently no transparent, traceable, or reliable pod delivery proof of delivery technology. These systems, which are often centralized, depend on trusted third parties (TTPs) to enable delivery between suppliers and clients. Though expensive, dependent on a single point of failure, and susceptible to hacking, privacy evasion, and compromise, TTPs aren't always the ideal choice. Because the blockchain is a decentralized, trustworthy ledger with records and events, it facilitates transparency, traceability, and tracking. Using the widely-used permissionless Ethereum blockchain, we provide in this article an example and a high-level framework for creating a reliable, distributed Pod system with integrated auditability, transparency, and accountability. The system verifies the delivery of a given item between a seller and a buyer using Ethereum smart contracts, irrespective of the number of intermediate carriers involved. We suggest a course of action that is advantageous to all parties.

[2] Yawling Jahan, Ixia Yang, and Shining Wang presented "Auditable Protocols for Fair Payment and Physical Asset Delivery Based on Smart Contracts" at the 2019 Xi'an University of Technology Conference in Science.

It is advisable to run the poll prior to receiving the final figures in order to get a better outcome. Because of the rapid development of electronic information technology, the emphasis has shifted from conventional market transactions to online payment and asset delivery. But since the third-party payment system is still in its early stages and there are a lot of charge Trojans out there, it is easy to cause a confidence issue. There is sometimes imbalance in the information flow between the two sides as a result of the existing centralized organization. Therefore, designing a distribution system that allows for auditable assets and equitable payments is a challenging issue. The blockchain technology that is currently being developed provides a novel approach because to its openness, transparency, and verifiability. Although asset- or payment-centric models make up the majority of the research now in publication, neither one offers customers a full buying model. In this work, we propose to use smart contracts to build a transparent physical asset delivery and equitable payment system. Three different types of smart contracts have been established to guarantee fair and consistent payment between merchants, consumers, and logistics companies. The auditability and traceability of blockchain technology make it a useful instrument for verifying the authenticity of assets and data shared across the transportation sector. The practice of "pre-verification" has been put in place due to the prevalence of product swapping. Because clients give the pickup codes in our system, there is less chance of fraud and thieves cannot use fake codes to deceive people into doing illegal acts or losing their property. Our approach also establishes a thorough return procedure for the first time, enhancing customer productivity and their overall service experience. Eventually, all the contracts required for the scheme's operation are deployed to the Ethereum test network. Our method boosted security and availability while reducing expenses, according to the examination and analysis of our security measures.

[3] W. Z. Wang, Cai, J. B. Ernst, Hong, Z., C. Feng, and V. C. M. Leung, "Decentralized Applications: The Blockchain-Empowered Software System," IEEE Access, 2018

Blockchain technology is attracting a lot of attention from the academic community and the financial industry. But the hysterical rumours about the hundreds of cryptocurrencies that are available and the frequency of initial coin offering frauds have also sparked controversial debates about this emerging technology. This article explores the development of blockchain technology from its beginning to its present, highlighting the significance of decentralized applications (daps) and the possible future value of blockchain. The present status of daps is examined in this study, along with potential ways to enhance blockchain technology to better serve daps' requirements. Get an overview of dap research and learn about the most recent developments in blockchain technology.

[4] Not N. Aitzaz, Z. and D. "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain, and Anonymous Messaging Streams," by Voinovich, published in IEEE Transactions on Dependable and Secure Computing (2017)

Smart grids with bidirectional communication flow are expected to provide advanced use monitoring and electricity trading. Regarding the security and privacy of customer and corporate data, there are, still, a lot of challenges to be solved. We address in this study how to guarantee transaction security in distributed energy trading over a smart grid without relying on centralized authority. Our proof-of-concept for a decentralized energy trading system is built on multi-signature, anonymous encrypted chat streams, and blockchain technology. Its goal is to enable peers to negotiate energy price and carry out trade transactions in an anonymous and safe manner. We performed case studies to analyze security and assess performance in light of the produced security and privacy demands.

[5] Nasheed Khan, Faiza lousily, Peer-to-peer networking applications, 2021, "Blockchain smart contracts: Applications, challenges, and future trends."

Due to the recent explosive expansion of digital currency and blockchain technology, new fields of crypto economics have developed. This has made it possible to create next-generation decentralized applications that don't depend on a third party, thanks to the introduction of smart contracts, which are computer protocols that automate the negotiation, verification, and enforcement of an agreement among several unreliable parties. Smart contracts are beneficial, however due to security concerns, flaws, and legal issues, they have not yet gained widespread use. In this article, we provide a thorough introduction to blockchain-enabled smart contracts, including the theory and real-world uses of this nascent area.

We do this by offering a taxonomy of current blockchain-enabled smart contract systems, categorizing the research papers that are included, and discussing the studies that have previously been carried out using smart contracts. We have identified some challenges and unresolved issues with this survey data that will need further research. In the end, we predict future trends.

[6] In the Computer Networks and Technology Conference in 2021, Enes Erden, Momin Kibbe, and Kernel Akala presented "A Bitcoin payment network with reduced transaction fees and confirmation times."

For many applications, Bitcoin's long confirmation waits and high transaction costs make it unfeasible, particularly for smaller payments that need immediate clearing. Although other cryptocurrencies have subsequently been introduced to address these issues, the Bitcoin network continues to enjoy the highest level of popularity. Innovative solutions are needed to address the high transaction fees and drawn-out verification procedures that now plague the bitcoin business if it is to capitalize on its user base. One such proposed payment network, the Lightning Network (LN), uses off-chain, two-way channels for value exchange. Transaction costs and verification times might be significantly reduced by using off-chain connections, which can be configured to perform batch transactions on a regular basis without adding new data to the blockchain. The fundamental purpose of decentralization is undermined by LN's continued usage of fee-charging relay nodes, which monopolize certain nodes as it expands. Nevertheless, despite the general consensus that LN would provide both high decentralization and a "scale-free network mechanism," the process of creating such a network involving several parties has never been studied. Therefore, in order to boost Bitcoin's ability to handle a large amount of transactions, we suggest using the LN in this article to construct a fully decentralized payment network. It is suggested that off-chain links, or payment channels, which are created dynamically according to market demands, be used to connect Bitcoin-accepting retailers, or nodes. Following our first network optimization model modelling of the problem, we proceed to a heuristic solution in which connections are pruned to induce evenly distributed payment flows while minimizing the total expenditures required to build initial off-chain linkages. The assessments demonstrate the extent to which the network may grow as well as the advantages and disadvantages of various strategies for allocating flows and configuring the network's initial flow capacity.

[7] Reza Trapdoor and Peja Ghazi, "Block by block: A peer-to-peer business transaction for international trade using blockchain technology," at the 2022 Technological Forecast and Social Change Conferences

Prior to starting to discover a solution, doing the survey is a smart idea since it guarantees a high-quality solution. The involvement of third parties in business transactions raises many concerns, such as heightened complexity and expense, as well as an elevated risk of information leakage. This study proposes a novel cross-border commerce method to address the disadvantages of depending on third parties in commercial transactions. A more thorough explanation of the mechanism's functioning is offered by business process modelling, which is also supplied and applied to a business transaction scenario in accordance with the standards and principles of Business Process Model and Notation (BPMN) 2.0. This paper examines and defines the roles and capabilities of blockchain technology, proposing a blockchain technology-based letter of credit (BTLC) as a means of producing letters of credit (LCs) that use smart contracts and blockchain.

[8] In the 2017 International Conference on Financial Cryptography and Data Security, Steven Goldfaden, Joseph Bonneau, Rosario Gennaro, and Arvind Narayanan presented their paper "Escrow Protocols for Cryptocurrencies: How to Buy Physical Goods Using Bitcoin."

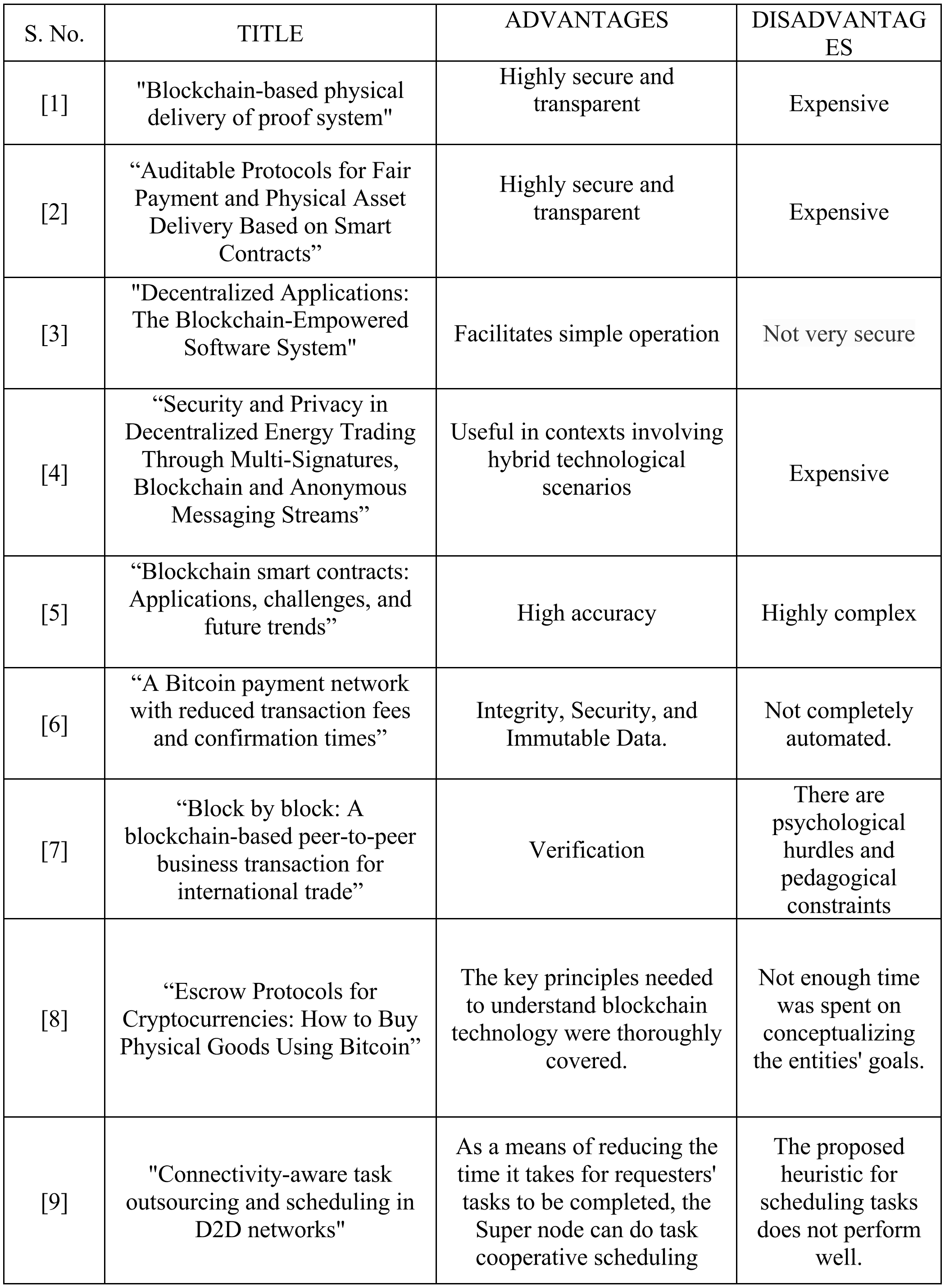
Given its strong influence on the final product, the survey ought to be carried out. We talk about the challenges that come up when attempting to pay with cryptocurrencies for conventional things. A cyclical dependence exists because both the buyer and the seller must make decisions on whether to send the products before getting payment and whether to trust the seller to pay for them before receiving them. This dilemma is usually resolved in real business transactions by using an escrow service offered by a third party. But as our study shows, basic escrow methods are fundamentally unsafe and violate users' right to privacy. We provide an enhanced security and privacy attributes set of techniques and define the escrow issue. Our protocols work with cryptocurrencies built on blockchains like Bitcoin.

[9] Zin Z. "Connectivity-aware task outsourcing and scheduling in D2D networks," by Hong, Z. Wang, W. Cai, and V. C. M. Leung, Proc. 26th Intern. Conv. Do the math. Ordinary. Fresht. 2017 (ICCCN),

Researchers and entrepreneurs alike are becoming more interested in the possibilities of mobile cloud computing due to the widespread use of powerful mobile devices like smartphones and tablets. When compared to the traditional approach of running large computational processes on potent desktop computers and the cloud, mobile cloud computing stands out for its affordability, flexibility, and availability. But because of this characteristic, it is challenging to design a good mobile computing system. Firstly, mobile devices cannot be trusted to do several computation-intensive activities by themselves since they lack the processing power of desktop computers. The additional financial costs (such those for computer services or wireless transmission) that come with moving computational tasks to the cloud could also be too much for certain clients to bear. Here, we introduce a new connectivity-aware task scheduling paradigm that leverages the "fog"—an aggregation of computing resources in the ad-hoc—to assist mobile device users in completing computation-intensive tasks cooperatively in the D2D network. Cooperative tasks are scheduled by a super node at the base station to satisfy users' different mobility demands. We provide a simple heuristic method for work scheduling that ensures quick cooperative job completion in order to further enhance users' quality of experience (Quek). In our simulations, we find that our cooperative paradigm greatly reduces the average time it takes for mobile device users to accomplish a task in a D2D network.

[10] Ma. Wuhrer and U. Zdun, (2018) "Smart contracts: Security patterns in the Ethereum ecosystem and solidity" , Proceedings Inside. Workshop: Soft Focused on Blockchain. ENG. 2018 (IWBOSE).

The survey is a critical component in defining a superior outcome in the end, and its needs should make it distinct. Smart contracts that are based on blockchain technology are gaining a lot of interest in new business applications and the scientific community as they remove the need for a trusted third party by allowing untrustworthy organizations to show contract conditions in program code. Although Ethereum is the most widely used smart contract platform at the moment, using it to develop secure and functional contracts is not simple. The scientific community and industry have just lately started to investigate this issue. By using Grounded Theory techniques to collected data, we have created a number of common security patterns and given a thorough explanation of them in Solidity, the most widely used Ethereum programming language. By simulating typical dangers, developers using Solidity may safeguard their applications from common attack.



S. No.	TITLE	ADVANTAGES	DISADVANTAGES
[1]	"Blockchain-based physical delivery of proof system"	Highly secure and transparent	Expensive
[2]	“Auditable Protocols for Fair Payment and Physical Asset Delivery Based on Smart Contracts”	Highly secure and transparent	Expensive
[3]	"Decentralized Applications: The Blockchain-Empowered Software System"	Facilitates simple operation	Not very secure
[4]	“Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams”	Useful in contexts involving hybrid technological scenarios	Expensive
[5]	“Blockchain smart contracts: Applications, challenges, and future trends”	High accuracy	Highly complex
[6]	“A Bitcoin payment network with reduced transaction fees and confirmation times”	Integrity, Security, and Immutable Data.	Not completely automated.
[7]	“Block by block: A blockchain-based peer-to-peer business transaction for international trade”	Verification	There are psychological hurdles and pedagogical constraints
[8]	“Escrow Protocols for Cryptocurrencies: How to Buy Physical Goods Using Bitcoin”	The key principles needed to understand blockchain technology were thoroughly covered.	Not enough time was spent on conceptualizing the entities' goals.
[9]	"Connectivity-aware task outsourcing and scheduling in D2D networks"	As a means of reducing the time it takes for requesters' tasks to be completed, the Super node can do task cooperative scheduling	The proposed heuristic for scheduling tasks does not perform well.

[10]	"Smart contracts: Security patterns in the Ethereum ecosystem and solidity"	Facilitates the autonomous running of blockchain-based applications	There is no Solidity-specific design pattern language that is both structured and informative.

Hence, in the existing system, the size of the proof stored in the blockchain for each transaction is extremely large. The existing system is not trustable and reliable. The existing system requires the use of a third party and charges extra fees than necessary.
The existing Escrow protocols are neither transparent nor secure.

3. Proposed Methodology

Creating a decentralized peer-to-peer (P2P) retail trading network requires coordinated efforts between multiple stakeholders and sophisticated software development. Choosing the appropriate process model or methodology is essential to the project's success. These are two chosen approaches that can be modified to create a decentralized peer-to-peer retail exchange.

Agile development processes are ideal for developing new and dynamic applications such as decentralized P2P retail exchanges. Agile emphasizes adaptability, teamwork, and iteratively producing value. This is how Agile can be used. Scrum or Kanban are certain Agile frameworks that give the development process organization. Development work is separated into time-bound iterations called sprints in Scrum, which typically run two to four weeks. Tasks are managed on a visual board and progress through phases of development in a more continuous manner with Kanban.

Regular iterations and releases provide swift development and flexibility in response to evolving needs. Throughout the development process, feedback from stakeholders—including end users—allows for modifications.

The Cross-functional teams collaborate closely to make sure that the development is in line with corporate objectives. Further, the adaptability to shifting consumer demands and market situation, feedback and collaboration from stakeholders' result in a platform is becoming more user-focused. Also, it is essential to work closely with blockchain and smart contract developers.

The process can be incorporated with DevOps principles and CI/CD pipelines to guarantee the seamless and effective deployment of updates in a decentralized P2P retail exchange. This approach involves the following:

In the proposed approach, the parties must make sure that the goods or service is provided, and the money is paid. Neither party should be forced to bear the consequences of the other's default on the deal.

By acting as a third party and confirming that the escrow logic is being executed correctly, an escrow smart contract reduces the risk of fraud.
The system's operations are open and transparent to all participants in the blockchain, as all relevant transactions are available to all users.

Reduced transaction costs and improved service efficiency are two direct results of Blockchain's elimination of the need for intermediaries.

Figure 1: depicts the workflow of the proposed system.

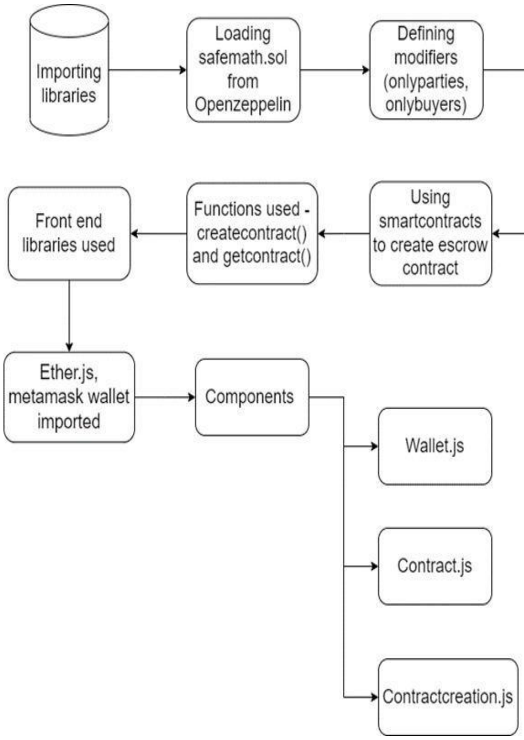
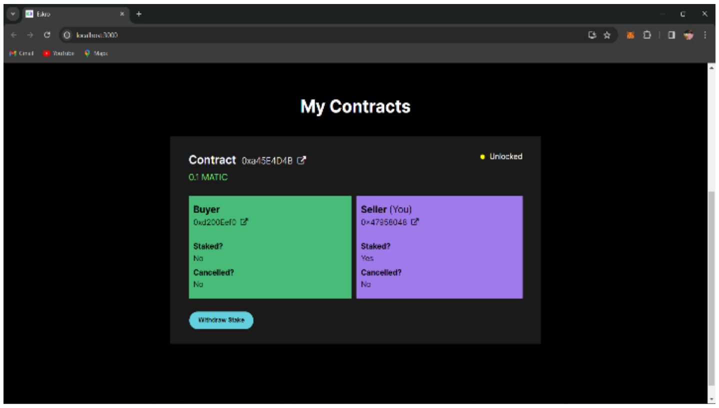

Importing libraries
Loading safemath.sol from Openzeppelin
Defining modifiers (onlyparties, onlybuyers)
Using stake() function
revokestate(), cancel(), and confirm() function used
Using smartcontracts to create escrow contract
Functions used - createcontract() and getcontract()
Front end libraries used
Ether.js, metamask wallet imported
Components
Wallet.js
Contract.js
Contractcreation.js

Figure 1: Proposed System

4. Results & Discussion

Validated outcomes are shown in Fig 2 and Fig 3.



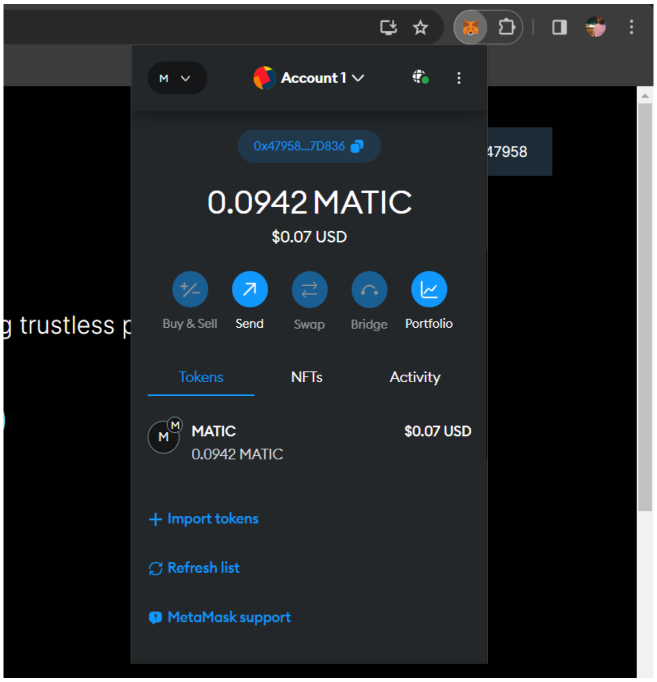
My Contracts

Contract 0xa45E4D4B
0.1 MATIC
Unlocked

Buyer
0xd200Eef0
Staked?
No
Cancelled?
No

Seller (You)
0x47958048
Staked?
Yes
Cancelled?
No

Figure 2: Homepage



Account 1
0x47958...7D836
0.0942 MATIC
$0.07 USD

MATIC
0.0942 MATIC
$0.07 USD

Figure 3: Transaction Screenshot

5. Conclusion

The proposed Escrow methods are absolutely unrelated to how files are actually transferred between peers. Both the escrow service and the content verification can be handled by the peer-to-peer platform itself, or by a third-party organization. As such, this research will inspire others to overcome the challenges in the blockchain.

References

[1] Haya r sahib, Khaled Saleh, "Blockchain-based physical delivery of proof system", Khalifa university conference and electronics department,2018

[2] shingling wang, ixia yang, yawling Jahan, "Auditable Protocols for Fair Payment and Physical Asset Delivery Based on Smart Contracts", Xi'an university of a technology conference in science,2019

[3] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized Applications: The Blockchain-Empowered Software System," in IEEE Access,2018

[4] N. Z. Aitzaz and D. Voinovich, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," in IEEE Transactions on Dependable and Secure Computing, 2018

[5] Nasheed khan, Faiza lousily, "Blockchain smart contracts: Applications, challenges, and future trends", Peer-to-peer networking applications, 2021

[6] Enes Erden, Momin kibbe, kernel Akala, "A Bitcoin payment network with reduced transaction fees and confirmation times", Computer networks and technology conference,2021

[7] Reza Trapdoor, Peja ghazi, “Block by block: A blockchain-based peer-to-peer business transaction for international trade”, Technological forecast and social change conferences, 2022

[8] Steven Goldfaden, Joseph Bonneau, Rosario Gennaro & Arvind Narayanan, "Escrow Protocols for Cryptocurrencies: How to Buy Physical Goods Using Bitcoin", International Conference on Financial Cryptography and Data Security, 2017

[9] Z. Hong, Z. Wang, W. Cai, and V. C. M. Leung, "Connectivity-aware task outsourcing and scheduling in D2D networks", Proc. 26th Int. Conf. Compute. Common. Newt. (ICCCN), 2017

[10] M. Wuhrer and U. Zdun, "Smart contracts: Security patterns in the Ethereum ecosystem and solidity", Proc. Int. Workshop Blockchain Oriented Soft. Eng. (IWBOSE), 2018.