International Conference on Innovative Computing and Communication (ICICC-2023)

Decentralised Escrow Protocol that Facilitates Secure Transactions between Trustless Parties

Ahamed Ali S[1], Yukesh S[2], Shankar T[3], Thanigai Arul R[4]*

haiahamed@gmail.com [1], Associate Professor, Department of Computer Science and Engineering, Easwari Engineering College [Autonomous], Tamil Nadu, India
yukeshyukss@gmail.com, shankararun1912@gmail.com, thanigaiarulr@gmail.com, [2,3,4] ,Department of Computer Science and Engineering, Easwari Engineering College [Autonomous], Tamil Nadu, India

Abstract: A decentralized escrow protocol makes it easy for people who don't trust each other to make safe payments. The Escrow protocol is used. Before a transaction can be made, tokens are sent to an escrow, which is a third-party smart contract. Once the terms of payment have been met, the escrow will release the tokens. Each party to a transaction is responsible for delivering the agreed-upon good or service and making the corresponding payment. One party shouldn't be able to back out of a deal at the other party's expense. If the payment terms depend on outside information, like when a product is shipped, the oracle pattern can be used to give the escrow the information it needs. Once the code for the smart contract is recorded on the blockchain, it cannot be altered. This makes sure that the escrow functionality is safe. This gives everyone involved in the trade peace of mind that they won't be taken advantage.

Keywords: Escrow, Blockchain, Smart Contracts, Decentralized, Transparent, Accountable

1. Introduction

To facilitate transactions without an intermediary through machine consensus, a Blockchain system operates on top of the Internet, on a transaction network of computers that all execute the protocol and contain an identical duplicate of the ledger of transactions. 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 that 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. There is no longer a need for trusted third parties like banks, Marketplaces, or other types of clearing financial institutions to interact over the Internet when they do not know or trust each other, reside in different countries, are subject to different authorities, and have no legal contacts with each other. This could provide new opportunities for the new entrepreneur to create their e-commerce site and start their business with zero trust as the smart contract enables both the entrepreneur and the customers to pay and receive payments only after the product delivery is done. Since the 1980s, academics have addressed many concepts related to cryptographically secured P2P networks, largely in theoretical studies. 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 distributed, and public ledger of transactions that can be viewed by anyone but is controlled by no one. A blockchain is a decentralized database that stores a growing mechanism of transaction records that are encrypted to prevent alterations.

The ills troubling the supply chain process are alleviating, owing to B2P for procure-to-pay solutions. It improves availability of liquid assets and cash flow, makes the whole process efficient, computerized, reduces time duration, and helps to enable prompt payments. Blockchain provides prompt access to appropriate data, establishment of data, joining and mixing data with ERP, and advanced payment system. It helps companies deal with problems in unscheduled procurements and threats of unauthorized access to information. P2P, or peer-to-peer, refers to a type of decentralized network communications paradigm in which a collection of devices (nodes) store and distribute files collectively, with each node functioning as an independent peer. With no server or admin in charge, 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 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 blockchain technology that underpins Bitcoin and other cryptocurrencies are 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.

While funds are held in Escrow, waiting for payout, we allocate investment funds to stablecoin Yield-Farming Protocols. 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. Each computer, or node, can function as a file server and a client, 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.

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" set-up to share and store data. When it comes to transmitting information, this creates a major security risk. Data kept on a peer-to-peer transaction is 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, the 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 peer-to-peer network. Blockchain is a distributed ledger that stores payments and cash flows for many digital assets in distributed ledger systems. Decentralized peer-to-peer networks, in which all nodes are interconnected and keep their 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 significant advantage of the usage of blockchain technology in peer-to-peer transactions is the suspension of paperwork or at least reduces the documentation of the cash flows. Since the entire blockchain technology is based on storing the details of the intrigate transaction in the ledger, there is no need for filing the cash flow. Blockchain eliminates the need for paperwork in the consent and validation process in attainments. 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 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.

1.1 Motivation

Smart contracts ensure the funds are rightfully distributed and carefully secured using escrow protocol, as it has become the primary choice. Many developers opt for this transaction method as it cuts down on human interference and works as developed by the engineers. It can utilize features like democratic voting to stop sponsoring projects or share out the capital to newly added breakthroughs to provide interactions with contracts. It provides feasible options for start-ups where investment in infrastructure will not be needed. Rather than receiving the entire collected funds, it is released in pre-arranged sums. It promises quality in delivery for start-up and allows investors to remain in control of the situation.

2. Existing System

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. The existing payment system are might take too long to process and transfer the amount. The new user can’t use the existing system for doing transactions in new businesses or companies as they couldn’t be sure of their company, the policies and their trust levels might be low.

3. Proposed system

The parties must make sure that the goods or service is provided, and the money is paid. New businesses can chose the new system to implement payment in their websites for payments as the smart contracts takes responsibilities of both the customer and the seller in the transaction. The new user/organisation can safely do transaction in the trust-less parties as the money can only be paid after the delivery of services by the company.

The system provides smart contract between the user and the trusted third party. The Meta mask acts as the digital wallet for holding crypto currencies in the transactions as shown in the fig. 1. Neither party should be forced to bear the consequences of the other’s default on the deal.

- Trust and safety - An escrow smart contract mitigates the possibility of fraud by serving as a third party and verifying the correct execution of escrow logic.

- Transparency - The system's operations are open and transparent to all participants in the blockchain, as all relevant transactions are available to all users.

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

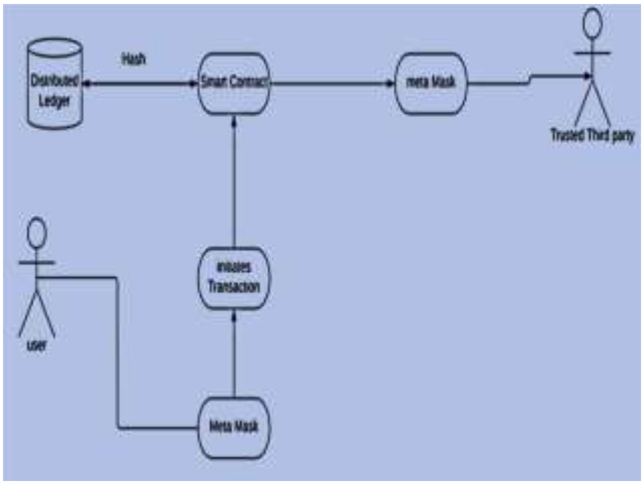

Fig. 1 – Architecture diagram of the proposed system

4. Literature survey

[1] The survey was a very good process to find out a good solution. Reviewing all the concepts related to it is a good practice. In this age of pervasive online shopping, a reliable means of guaranteeing the timely delivery of purchased goods is more important than ever. Unfortunately, the current pod delivery proof of delivery technologies is neither transparent, traceable, nor credible. These systems are often clustered and rely on trusted third parties (TTP) to facilitate dispatch between vendors and customers. Costly, relying on a single point of failure, and vulnerable to hacking, confidentiality bypassing, and incriminating, TTP is not always the best option. Transparency, traceability, and tracking are all facilitated by the blockchain because it is a decentralized, trusted ledger containing logs and events.

In this paper, we introduce an exception and a high-level framework for developing a trustworthy, distributed Pod system with built-in auditability, transparency, and accountability by leveraging the widely used permissionless Ethereum blockchain. The system utilizes Ethereum self-executing contracts to verify the distribution of a supplied item between a seller and a buyer, regardless of the number of intermediary conveyers involved. We propose a solution in which all involved parties benefit.

To be trustworthy and to rely on double-deposit security. One way to guarantee that everyone gets their fair portion of ether after a transaction has been completed successfully is through automated payment in ether delivery. If a disagreement should emerge while the transport operation. In this article, we detail the steps we used to build and test our Pod solution's capabilities. In addition to our security research, we also offer ether gas cost projections. We have released all the smart contract codes for Ethereum on GitHub.

[2] To get a better result, it's a good idea to conduct the poll before you have the final numbers. There has been a shift in focus from traditional market transactions to online payment and delivery of assets due to the rapid growth of electronic information technology. However, it is simple to provoke a trust crisis due to the unfinished nature of the third-party payment mechanism and the intrusion danger posed by numerous charging Trojans. Because of the current centralized structure, there is the frequent asymmetry in the flow of information between the two sides. So, it's a tricky task to figure out how to make a distribution system where payments are fair, and assets can be audited. Because of its openness, transparency, and verifiability, blockchain technology now in development offers a new approach. Most of the existing literature is either payment- or asset-centric, but neither of these approaches provides a comprehensive purchasing model for consumers. In this paper, we suggest using smart contracts to create a transparent system for delivering physical assets and making fair payments. In the end, the Ethereum test network is used to deploy all the contracts necessary for the scheme to run. The evaluation and analysis of our security measures revealed that our strategy not only reduced costs but also increased security and availability.

[3] The academic community and the financial sector are showing a lot of interest in blockchain technology. However, infamous arguments on this developing technology have also been prompted by the overwhelming speculations on the hundreds of accessible cryptocurrencies and the prevalence of initial coin offering scams. To show why decentralized applications (daps) are so crucial, and how much blockchain could potentially be worth in the future, this article follows the history of blockchain. Here in this paper, we look at the current state of daps and examine how blockchain technology might be improved to meet the needs of daps. Learn about the latest advancements in blockchain technology and receive an outline of dap research.

[4] Advanced usage monitoring and power trading are anticipated from smart grids with bidirectional communication flow. However, there are significant obstacles to overcome regarding the safety and confidentiality of consumer and business data. In this paper, we discuss how to ensure the safety of transactions in the distributed trading of energy across a smart grid without the use of centralized authorities. To allow associates to agree upon energy pricing and conduct trade transactions anonymously and securely, we have created a proof-of-concept for a decentralized energy trading system based on blockchain technology, multi-signatures, and anonymous encrypted chat streams. To analyse security and evaluate performance in the context of the safety and confidentiality needs that were generated, we conducted case studies.

[5] New crypto economics has emerged as a result of the swift growth of blockchain technology and digital currency in recent years. The emergence of smart contracts—computer conventions designed to automate the facilitation, verification, and enforcement of compromise and discussion among multiple unprincipled parties—has allowed for the development of next-generation decentralized applications that do not rely on a dependable third party. Despite their benefits, smart contracts have not yet been widely adopted because of security fears, weaknesses, and legal complications. In this paper, we provide a detailed overview of blockchain-enabled smart contracts, covering both the technology and practical applications of this emerging field. We achieve this by providing a grading of existing blockchain-enabled smart contract systems, classifying the embraced conference papers, and talking about the studies that have already been conducted using smart contracts. With this survey data in hand, we've uncovered several obstacles and unanswered questions that will require further investigation. Ultimately, we forecast future tendencies.

[6] Bitcoin is impractical for many uses because of its high transaction fees and lengthy confirmation delays, especially for smaller payments that need quick clearance. Several alternative cryptocurrencies have since been launched to help solve these problems, but the Bitcoin network is still the most popular one. To reap the benefits of its user base, innovative solutions are required to combat the high transaction fees and lengthy verification processes now plaguing the cryptocurrency industry. The Lightning Network (LN) is one such proposed payment network that takes advantage of off-chain, two-way channels for exchanging value. Since off-chain linkages may be set up to execute batch transactions at regular intervals without adding new data to the blockchain, this has the potential to drastically cut down on both transaction fees and verification times. However, how to build such a network across several parties has never been researched, despite the widespread belief that LN will come up with a "scale-free network technique" in addition to strong decentralization. As a result, in this article, we propose to utilize the LN to create a completely decentralized payment network that will increase Bitcoin's capacity to process a high volume of transactions.

[7] The survey is good practice before going into finding the solution, it ensures a good output for the problem. Third-party engagement in commercial transactions presents several issues, including increased complexity and cost, as well as the increased danger of information leakage. Business process modelling, according to the norms and principles of Business Process Model and Notation (BPMN) 2.0, is also provided and applied to a business transaction scenario to give a more in-depth understanding of the mechanism's operation. This research suggests a blockchain technology-based letter of credit (BTLC) as a mechanism for issuing letters of credit (LCs) that take advantage of crypto payments and smart contracts by studying and defining blockchain's responsibilities and capabilities.

[8] The survey should be conducted because it has a very positive impact on the final output. We discuss the difficulties that arise when trying to purchase traditional goods with cryptocurrency. There is an inherent circular reliance: the buyer must decide whether to believe the seller to pay for the goods before receiving them, and the seller must decide whether to ship the products before procuring the payment. In actual business, this conundrum is typically solved by employing the use of an escrow service provided by a third party. However, our research demonstrates that simple escrow protocols are inherently insecure and violate users' right to privacy. We describe the escrow problem and give out a set of strategies with enhanced privacy assets. Our protocols are consistent with Bitcoin and other blockchain-based cryptocurrencies.

[9] The proliferation of high-powered mobile gadgets (such as smartphones and tablets) has piqued the interest of researchers and businesspeople alike in the potential of mobile cloud computing. Mobile cloud computing stands out because of its low cost, adaptability, and availability in comparison to the conventional method of conducting massive computational operations on high-performance desktop computers and cloud platforms. A successful mobile computer system, however, is difficult to construct due in part to this property. To begin with, mobile devices do not have the same level of computational capacity as desktop computers, therefore they cannot be relied upon to undertake many comprehensive tasks on their own. Additionally, customers may find the added monetary expenditures (such as wireless transmission cost or computing service cost) associated with shifting computational work to the cloud to be prohibitive. To help mobile device users complete computation-intensive activities collaboratively in the D2D network, we present an innovative connectivity-aware solution scheduling criterion that makes advantage of the "fog" - a collection of analytical powers in the ad-hoc. To accommodate users' varying mobility needs, a super node located at the base station schedules cooperative tasks.

[10] The survey is a very important dynamic to specify a better result in the last and it should be unique as to the requirements. Since they allow untrustworthy entities to exhibit contract conditions in program code and therefore eliminate the requirement for a trusted third party, smart contracts that build on blockchain technology are attracting a lot of recognition in new corporate industries for blockchain payment and the scientific circle in the world. Ethereum is the most preferred cryptocurrency platform currently available, but it is not an easy operation to create well-performing and safe contracts with it. Only recently have industry and science begun researching this problem. Using Grounded Theory methods on acquired data, we've crafted numerous typical security patterns and provided a detailed description of them in Solidity, the most popular programming language for Ethereum. Developers working with Solidity can protect their projects from common threats by emulating the patterns outline.

Table 1 – Comparison analysis of different papers

Title	Pros	Cons
"Blockchain-based physical delivery of proof system"	Highly secure and transparent	Subject to manipulation
“Auditable Protocols for Fair Payment and Physical Asset Delivery Based on Smart Contracts”	Highly secure and transparent	Expensive compared to other solutions
"Decentralized Applications: The Blockchain-Empowered Software System"	Facilitates simple operation	Not very secure
“Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams”	Useful in contexts involving hybrid technological scenarios	Compromised network entities
“Blockchain smart contracts: Applications, challenges, and future trends”	High accuracy	Highly complex
“A Bitcoin payment network with reduced transaction fees and confirmation times”	Integrity, Security, and Immutable Data.	Not completely automated.
“Block by block: A blockchain-based peer-to-peer business transaction for international trade”	Verification of documents and terms in real time	There are psychological hurdles and pedagogical constraints
“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.
"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 Supernode can do task cooperative	The proposed heuristic for scheduling tasks does not perform well.
"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.

5. Conclusion

Our proposed escrow methods are unrelated to how files are 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. This payment system might create new opportunities for the entrepreneurs and new business owners. As such, we're hoping our research will inspire others to dive into this pressing issue on 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.