A TRUSTLESS ESCROW MECHANISM THAT SUPPORTS SECURE PEER-TO-PEER TRANSACTIONS WITHOUT RELYING ON CENTRAL AUTHORITIES

Mrs. S. Jayasree
Assistant Professor, Department of Computer Science
SRM Arts and Science College, Kattankulathur
jayasreecat@srmasc.ac.in
https://doi.org/10.34293/9789361639715.shanlax.ch.035

Abstract

*A **decentralized escrow protocol** allows individuals who may not trust each other to carry out secure transactions. It relies on an **escrow smart contract**, which acts as an impartial third party. Before the actual exchange occurs, tokens are locked into the escrow. Once the agreed conditions are fulfilled, the contract automatically releases the tokens to the rightful recipient.Each party is accountable for providing the promised product or service and making the required payment. The system is designed to prevent either party from backing out in a way that harms the other. If the agreement relies on real-world events—such as the delivery of a product—an **oracle** can supply the necessary information to the escrow contract. Since smart contracts are unchangeable once deployed to the blockchain, the escrow process is secure and trustworthy. This ensures that everyone involved can engage in the transaction with confidence and without fear of being cheated.*
***Keywords**: Escrow, Blockchain, Smart Contracts, Decentralized, transparent and accountable*

Introduction

To support peer-to-peer (P2P) value transfers without relying on intermediaries, a blockchain system functions over the Internet through a decentralized network of computers. Each of these computers runs the same protocol and stores an identical copy of the transaction ledger.

The concept of blockchain was introduced to the public in **October 2008** through the proposal of **Bitcoin**, which aimed to create a decentralized digital currency that operates without the involvement of traditional banks or financial institutions. Bitcoin provided a novel way to address the long-standing problem of trust between parties. Blockchain technology allows users to trust the **outcome** of the system even if they don't trust the individual participants. It removes the need for centralized third parties—such as banks, online platforms, or clearinghouses—enabling individuals and organizations to conduct transactions across borders, legal systems, and jurisdictions, without the need for direct relationships or legally binding contracts. 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, distributed, and public ledger of transactions that can be viewed by anyone but is controlled by no one. A block chain is a decentralized database that stores a growing list 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 business liquidity, makes the whole procedure paperless, saves

time, reduces costs, and helps ensure timely payments. Blockchain offers real-time access to relevant information, verification of data, integration with ERP, and advanced payment matching. It helps companies deal with problems in unscheduled procurement, threats of unauthorized access to information, and compliance-related issues. 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 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 crypto currency. Bit coin, 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 Bitcoinand other cryptocurrencies 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.

While funds are temporarily held in escrow awaiting release, they are invested in **stablecoin-based yield farming protocols** to generate passive returns. The global investment landscape is expanding rapidly, transforming how financial sustainability is achieved. Technological innovation has played a major role in streamlining systems, benefiting both business leaders and employees.

The integration of **P2P payment gateways with escrow protocols** presents significant opportunities, especially for businesses aiming to enhance transaction efficiency and security. **Peer-to-peer (P2P) systems**, structured as **peer-to-node (P2N) networks**, link various computer systems in a decentralized manner. Each node in the network can act both as a client and as a server—downloading data when acting as a client and sharing data when functioning as a server—removing the need for a centralized authority.

Peers, also known as participating computer systems, can share and receive resources on the same network. Files, space, the ability to use a scanner or printer, and computing power are all examples of resources. Neither a single point of failure nor a governing body exists. 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

as both clients and serversto the other nodes in the network. As 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 peer-to-peer network node 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.

ForP2Ptowork,all it takesis 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 peer-to-peer network. Blockchain is a distributed ledger that records transactions for many digital assets in a distributed ledger system. Decentralized peer-to-peer 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.

An outcome of the implementation of blockchain technology in P2P is the elimination of paper work or, at the least, reducing paperwork to the minimum. When everything is recorded on a distributed ledger accessible to everyone on the network, it does away with the requirement of a paper trail. Blockchain eliminates the need for paperwork in the authorization and authentication process in procurements. The various advantages of P2P networks have led many programmers to adopt them, oratleast 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 tokeep running. Developers may nowsafely take advantage of the benefits ofapeer-to-peermobile 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 inthe 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 customerstoshopat majorbusinesses likeWhole Foods and Target for necessities like food, cleaning supplies, and furniture. Financial transactions are just the beginning of what maybe 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 appsthat are compatible with Apple devices.

Literature Survey

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

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, or credible. These systems are often centralized and rely on trusted third parties(TTPs) to facilitate delivery between vendors and customers. Costly, relying on a single point of failure, and vulnerable to hacking, privacy evasion, and compromise, TTPs are notal ways 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 audit ability, transparency, and accountability by leveraging the widely used permission less Ethereum blockchain. The system utilizes Ethereum smart contracts to verify delivery of a supplied item between a seller and a buyer, regardless of the number of intermediary transporters involved. We propose a solution in which all involved parties' benefit.

To be trust worthy and to rely on double-deposit security. One way to guarantee that everyonegets their fair portion of ether after a transaction has 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 code for Ethereumon GitHub.

[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**

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 frequently 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. To ensure consistent and equitable payment between retailers, customers, and logistics firms, three distinct forms of smart contracts have been developed. Blockchain's auditability and traceability make it a practical tool for checking the integrity of assets and data exchanged across the transportation industry as a whole. Because of the common occurrence of product swapping, the practice of "pre-verification" has been implemented. In our system, the pickup codes are issued by the customers themselves, which reduces the likelihood of fraud and stops criminals from using phony codes to trick others into engaging inillicit activities or losing their property. For the first time, our strategy also creates a comprehensive return process, which will improve the service experience and increase productivity for customers. 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] **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**

The academic community and the financial sector are showing a lot of interest in blockchain technology. However, infamous arguments onthis developing technology have also been prompted by the overwhelming speculations on the hundreds of accessible crypto currencies and the prevalence of initial coin offering scams. In order 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 technology. 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] **N.Z.Aitzazand D. Voinovich, "Security and Privacy in Decentralized Energy TradingThrough Multi-Signatures, Blockchain and Anonymous Messaging Streams," in IEEE Transactions on Dependable and Secure Computing, 2018**

Advanced usage monitoring and power trading are anticipated from smart grids withbidirectional communication flow. However, there are significant obstacles to overcome in r egard to the security and privacy 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. For the purpose of allowing peers to negotiate 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. In order to analyse security and evaluate performance in the context of the security and privacy needs that were generated, we conducted case studies.

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

New crypto economics have emerged as a result of the rapid growth of blockchain technology and digital currency in recent years. The emergence of smart contracts—computer protocols designed to automate the facilitation, verification, and enforcement of a negotiation and agreement among multiple untrustworthy parties—has allowed for the development of next-generation decentralized applications that do not rely on a trusted 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 adetailed overview of blockchain-enabled smart contracts, covering both the technology and practicalapplicationsofthisemergingfield. We achieve this by providing a taxonomy of existing blockchain-enabled smart contract systems, classifying the included research papers, and talking about the studies that have already been conducted using smart contracts. With this survey data in hand, we've uncovered a number of obstacles and unanswered questions that will require further investigation. Ultimately, we forecast future tendencies.

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

Bitcoin is impractical for many uses because ofits 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. In order 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. Despite this, LN continues to use fee-charging relay nodes, and as it grows, some nodes become monopolies, defeating the very point of decentralization. However, how to build such a network across several parties has never been researched, despite the widespread belief that LN will provide a "scale-free network mechanism" 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. It's proposed that Bitcoin-accepting stores (i.e., nodes) be linked together via off- chain linkages (i.e., payment channels) that are dynamically established based on the

requirements of the marketplace. After initially modeling the issue as a network optimization, we go on to a heuristic solution where links are pruned to induce equally distributed payment flows while limiting the overall investments made to construct initial off-chain links. The evaluations show how far the network can scale, and the costs and benefits of several approaches to distributing flows and setting up the network's initial flow capacity.

[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**

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 a number of issues, including increased complexity and cost, as well as increased danger of information leakage. To remedy the drawbacks of relying on third parties in business transactions, thisresearch suggests a revolutionary mechanism for cross-border commerce. Business process modeling, 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 in order to providea more in-depth understanding of themechanism's operation. This study suggests a blockchain technology-based letter of credit (BTLC) as a mechanism for issuing letters of credit (LCs) that take advantage of blockchainand smart contracts by studying and defining blockchain's responsibilities and capabilities.

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

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 dependency: the buyer must decide whether to trust the seller to pay for the goods before receiving them, and the seller must decide whether to ship the goods before receiving 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 formalize the escrow problem and present a set of schemes with improved security and privacy properties. Our protocols are compatible with Bitcoin and other blockchain-based cryptocurrencies.

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

The proliferation of high-powered mobile gadgets (such smart phones and tablets) has piqued the interest of researchers and businesspeople alike in the potential of mobile cloud computing. Mobile cloud computing stands out because to its low cost, adaptability, and

availability in comparison to the conventional method of conducting massive computational operations on powerful desktop computers and the cloud. A successful mobile computer system, however, is difficult to construct due in part tothis property. To begin with, mobile devices do not have the same levelof computational capacity as desktop computers, therefore they cannot be relied upon to undertake many computation- intensive 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 a novel connectivity-aware task scheduling paradigm that makes advantage of the "fog" - an aggregate of computational powers in the ad-hoc. In order to accommodate users' varying mobility needs, a super node located at the base station schedules cooperative tasks. To further improve users' quality of experience (Quek), we present a light weight heuristic technique for scheduling tasks to guarantee fast cooperative task completion. The average time it takes for users of mobile devices to complete a job in a D2D network is decreased significantly in our simulations, demonstrating the efficacy of our cooperative paradigm.

[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.**

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 thirdparty, smart contracts that build on blockchain technology are attracting a lot of attention in new corporate applications and the scientific community. Ethereum is the most popular smart contract platform currently available, but it is not an easy operation to create well-performing and safe contracts with it. Only recently has industry and science begun conducting research on 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 outlined here.

Table of Comparison

S.No	TITLE	PROS	CONS
[1]	"Blockchain-basedphysicaldelivery 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	Notvery 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 of documents and terms in real time	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 timewas spent on conceptualizing the entities' goals.
[9]	"Connectivity-aware task out sourcing 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]	"Smartcontracts:Security patterns in the Ethereum ecosystem and solidity"	Facilitates the autonomous running of blockchain-based applications	There is no Solidity-specific design pattern language both structured and informative.

Existing System

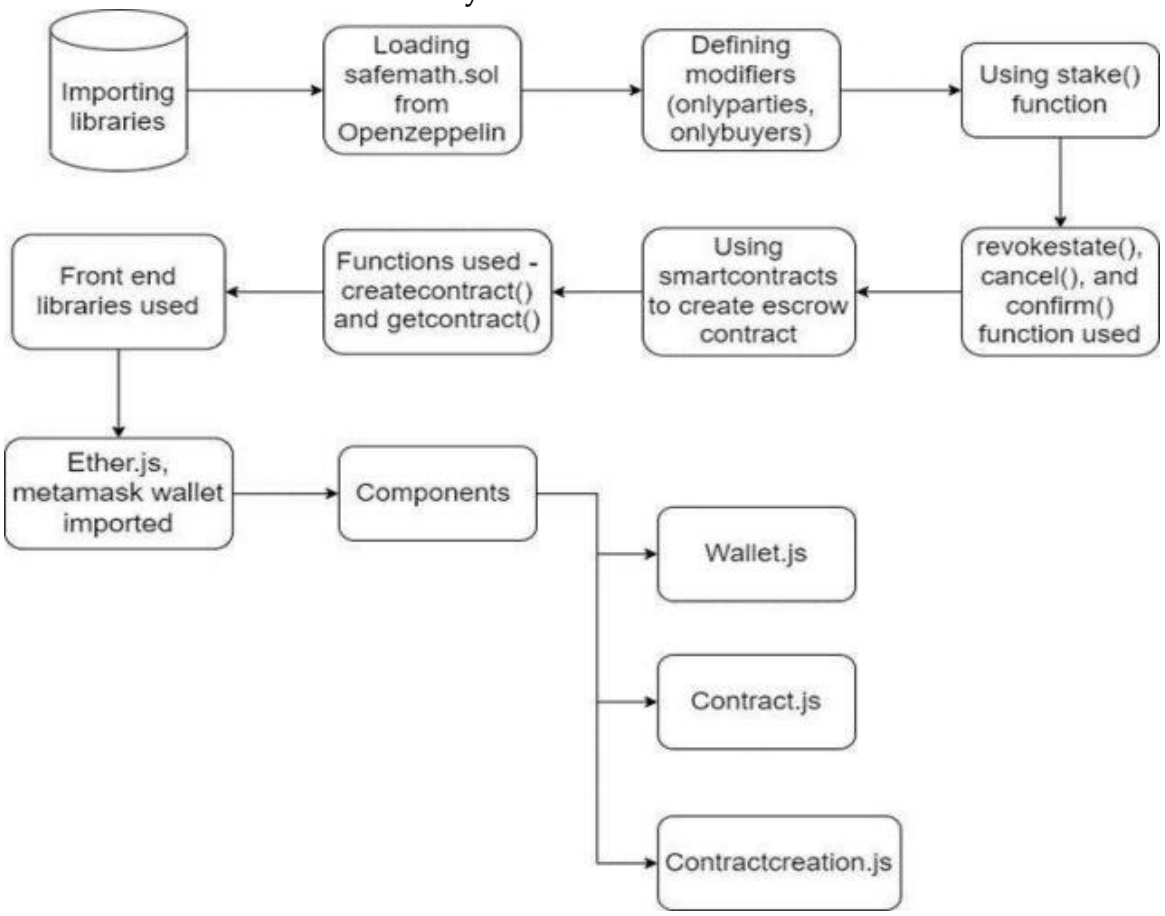
In the current system, the proof associated with each transaction stored on the blockchain is excessively large. Additionally, the system lacks trustworthiness and reliability. It depends on third-party intermediaries, which results in higher fees than necessary. Furthermore, existing escrow protocols are often neither transparent nor secure.

Proposed System

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.

- **Trust and Safety –** An escrow smart contract enhances security by acting as a neutral third party, ensuring that the agreed-upon conditions are properly met and reducing the risk of fraud.
- 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.

System Architecture



Conclusion

The escrow methods we propose are entirely independent of the actual file transfer process between peers. Both the escrow functionality and content verification can be managed either directly by the peer-to-peer platform or by an external third-party entity. Through our research, we aim to encourage further exploration of this important challenge within the blockchain ecosystem.

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 TradingThrough 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 reducedtransaction 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