A DECENTRALIZED ESCROW PROTOCOL THAT FACILITATES SECURE P2P PAYMENTS BETWEEN TRUSTLESS PARTIES

J. Ramesh Babu[1], Javvaji Naga Pavan Kumar[2], R Shashidhar[3], Yashovardhan Cheekoty[4], Amjan Shaik[5]

[1]Associate Professor, Department of Computer Science and Engineering, St. Peter's Engineering College, Dullapally, Maisammaguda, Medchal, Hyderabad, Telangana 500043.

[2,3,4]UG students, Department of Computer Science and Engineering, St. Peter's Engineering College, Dullapally, Maisammaguda, Medchal, Hyderabad, Telangana 500043

[5]Head of the Department, Department of Computer Science and Engineering, St. Peter's Engineering College, Dullapally, Maisammaguda, Medchal, Hyderabad, Telangana 500043.

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. The escrow holds the tokens until the conditions for payment are met. Both the agreed-upon product or service and the agreed-upon payment must be made by all parties involved in the transaction. 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. As soon as the smart contract code is put on the block chain, it can't be changed. This makes sure that the escrow functionality is safe. This gives everyone involved in the trade the peace of mind that they won't be taken advantage of.

Keywords: P2P, ESCROW, High efficiency, high Accuracy.

INTRODUCTION:

A smart contract can act as an escrow, holding the money until the conditions for payment are met. First, we make a smart contract that spells out the settlement process and conditions. Either the seller or the buyer could set up and use this smart contract. Second, the buyer sends the token(s) to the smart contract for the escrow. Third, when the conditions for token release are met by giving the desired product or server, the escrow smart contract is told about the event. Lastly, the escrow checks that the conditions have been met and gives the tokens to the seller. If the buyer doesn't tell the escrow about the event within the time limit or if the event shows that the product or service wasn't delivered according to the terms agreed upon, the tokens are sent back to the buyer. If the payment conditions depend only on data on the blockchain, a delegated call can be made to the escrow contract to let it know when the product or service should be sent.

MOTIVATION:

Fairly exchanging digital content is an epic problem. A fair exchange protocol guarantees that at the end either one of them obtains what (s)he wants, or neither of them does. In digital commerce, it is a requirement to include fair exchange since one or both of the parties are using digital currencies as subject matter Protocols that rely on the fact that the digital asset can be reproduced and re-sent. Broadly, these schemes resolve disputes by enabling the mediator to reconstruct the desired asset. The disputing party in essence deposits a copy of its digital asset with the mediator.

PROBLEM DEFINITION:

Traditional escrow systems rely on centralized intermediaries, such as banks or third-party service providers, to facilitate and secure transactions between parties. Decentralized escrow solutions aim to leverage blockchain technology and smart contracts to create a trustless and transparent environment for escrow services. By removing the need for a centralized intermediary and enabling peer-to-peer transactions, decentralized escrow offers increased trust, reduced costs, improved accessibility, enhanced security, and greater transparency, revolutionizing the escrow industry.

OBJECTIVE OF THE PROJECT:

Fairness: After exchange, either both seller and buyer can obtain all the goods (digital currencies, digital assets, physical goods) they want, or they can obtain nothing (All-or-nothing);

Security: None of the parities can transfer the digital funds during the period of exchange;

Passivity: If no dispute arises, there is no need for the thirdparty to take part;

Correctness: Ensure transactions and settlement of disputes are executed by the protocol agreed in advance;

Dependability: Mitigate single point failure and DoS attacks;

Privacy: In case of no disputes, the

third-party can't be aware of if the transaction completes, and only related parties can be aware of if disputes arise

LITERATURE SURVEY:

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above considerations are taken into account for developing the proposed system.

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

In this paper, we present absolution and a general framework using the popular permissionless Ethereum blockchain to create a trusted, decentralized Pod system that ensures accountability, auditability, and integrity. The solution uses Ethereum smart contracts to prove the delivery of a shipped item between a seller and a buyer irrespective of the number of intermediate transporters needed.

Shingling wang, ixia yang, yawling Jahan, “Auditable Protocols for Fair Payment and Physical Asset Delivery Based on Smart Contracts”, Xi’an university of technology conference in science,2019

The survey before the result is a very good step to find out a better output. With the rapid development of electronic information technology, online transaction will gradually surpass traditional market transaction, among which online payment and asset delivery become the focus of attention. But in fact, due to the incomplete third-party payment mechanism and the intrusion risk of various charging Trojan, it is easy to cause a trust crisis.

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

Blockchain technology has attracted tremendous attention in both academia and capital market. However, overwhelming speculations on thousands of available cryptocurrencies and numerous initial coin offering scams have also brought notorious debates on this emerging technology .

EXISTING SYSTEM:

In the existing system, centralized escrow system refers to a traditional escrow arrangement where a centralized intermediary, such as a bank or a dedicated escrow service provider, facilitates and safeguards transactions between parties. In this system, the intermediary acts as a trusted third party responsible for holding and disbursing funds or assets based on the agreed-upon terms and conditions.

PROPOSED SYSTEM:

A decentralized escrow protocol makes it easy for people who don't trust each other to make safe payments. The Eskro protocol is used. Before a transaction can be made, tokens are sent to an escrow, which is a third-party smart contract. The escrow holds the tokens until the conditions for payment are met. Both the agreed-upon product or service and the agreed-upon payment must be made by all parties involved in the transaction. One party shouldn't be able to back out of a deal at the other party's expense.

ADVANTAGES OF THE PROPOSED SYSTEM:

Trustless Transactions: Decentralized escrow protocols utilize smart contracts and blockchain technology to automate and enforce transaction terms. This eliminates the need for trust in a centralized intermediary, as the protocol itself ensures the execution of the agreed-upon conditions. Participants can have increased confidence in the security and fairness of transactions, even when dealing with unknown or untrusted parties.

Enhanced Security: Decentralized escrow protocols leverage the immutability and cryptographic security of blockchain technology. Transactions recorded on the blockchain are tamper-resistant, reducing the risk of fraud or unauthorized modifications. The use of cryptographic keys and multi-signature schemes provides robust protection against unauthorized access or manipulation of funds.

Reduced Costs: By eliminating the need for intermediaries, decentralized escrow protocols can significantly reduce transaction costs. There are no fees associated with using a centralized escrow service, which typically charges for their services. Additionally, the absence of middlemen allows for direct peer-to-peer transactions, eliminating additional administrative and processing costs.

Accessibility and Inclusivity: Decentralized escrow protocols are accessible to anyone with an internet connection and a compatible digital wallet. This inclusivity enables individuals in underserved regions or underbanked populations to engage in secure transactions, promoting financial inclusion and economic empowerment.

WORKING METHODOLOGY:

A smart contract can act as an escrow, holding the money until the conditions for payment are met. First, we make a smart contract that spells out the settlement process and conditions. Either the seller or the buyer could set up and use this smart contract. Second, the buyer sends the token(s) to the smart contract for the escrow. Third, when the conditions for token release are met by giving the desired product or server, the escrow smart contract is told about the event. Lastly, the escrow checks that the conditions have been met and gives the tokens to the seller. If the buyer doesn't tell the escrow about the event within the time limit or if the event shows that the product or service wasn't delivered according to the terms agreed upon, the tokens are sent back to the buyer. If the payment conditions depend only on data on the blockchain, a delegated call can be made to the escrow contract to let it know when the product or service should be sent. 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. As soon as the smart contract code is put on the blockchain, it can't be changed. This makes sure that the escrow functionality is safe. This gives everyone involved in the trade the peace of mind that they won't be taken advantage of.

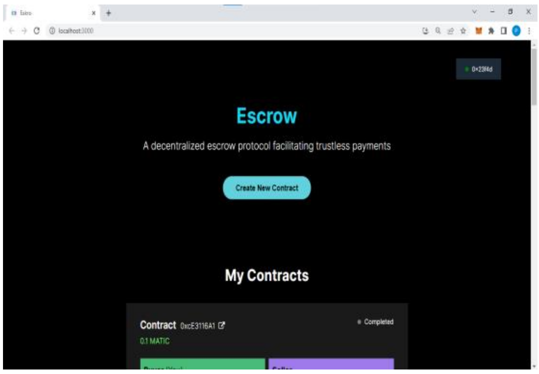

Fig.1 Home Screen

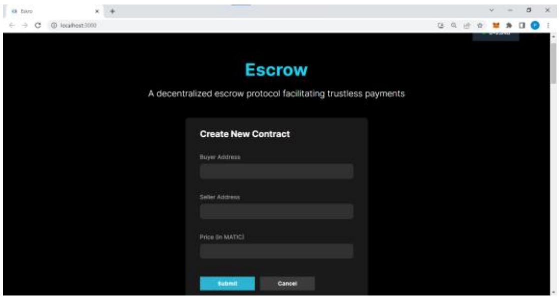

Fig.2 Contract Creation

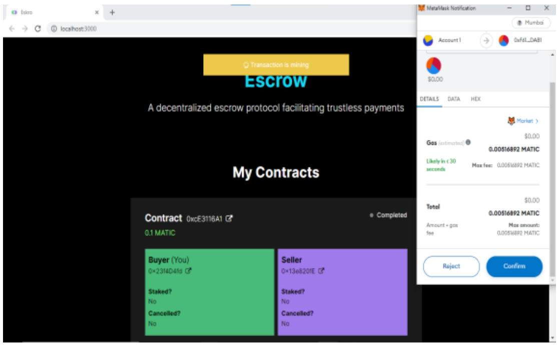

Fig.3 Metamask Approval

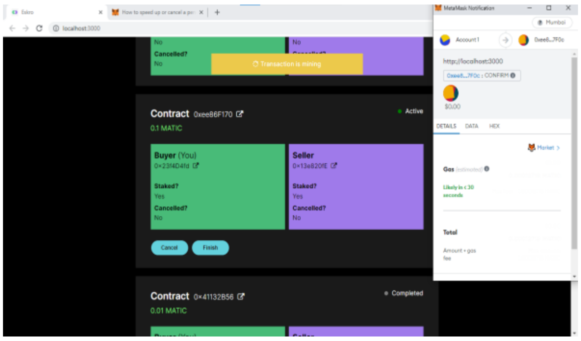

Fig.6 Completed Transaction

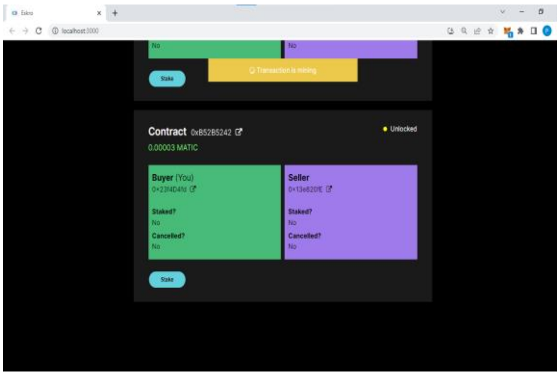

Fig.4 Contract

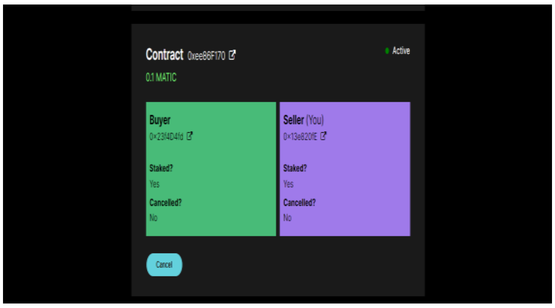

Fig.5 Staked Transaction

CONCLUSION

We proposed a decentralised Escrow Protocol to facilitate trustable ans secure payments between two parties.This protocol is secure, optimistic, internally-hiding, externallyhiding, and dispute-hiding. We have used Smart Contracts as Solidity as our programming language.The proposed project has various advantages over the existing systems.If the buyer doesn't tell the escrow about the event within the time limit or if the event shows that the product or service wasn't delivered according to the terms agreed upon, the tokens are sent back to the buyer. If the payment conditions depend only on data on the blockchain, a delegated call can be made to the escrow contract to let it know when the product or service should be sent.We hope that our study can stimulate more future research endeavors on this crucial problem in blockchain.

FUTURE ENHANCEMENTS:

The future enhancements of decentralized protocols are driven by ongoing research, technological advancements, and the evolving needs of the decentralized ecosystem. Here are some potential areas of improvement and future enhancements for decentralized protocols:

● Scalability : Enhancing scalability is a key focus for decentralized protocols. Solutions like sharding, layer-2 scaling solutions (such as state channels and sidechains), and improved consensus algorithms (like proof-of-stake) are being developed to increase transaction throughput and reduce network congestion. These advancements aim to enable decentralized protocols to handle a significantly higher number of transactions per second, making them more practical for widespread adoption.

● Interoperability: Enabling seamless interoperability between different blockchain networks and protocols is crucial for the growth of the decentralized ecosystem. Efforts are being made to establish common standards, protocols, and cross-chain communication mechanisms, allowing assets and data to flow freely between different blockchains. This would facilitate increased liquidity, efficient asset transfers, and improved collaboration between decentralized applications.

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 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.