Smart Contract Based E-commerce Payment Gateway

[1]Aluvala Keerthan Chand, [2]Dr. K.P. Kaliyamurthie

[2]Guide
Department of Computer Science and Engineering
Bharath Institute of Science & Technology
affiliated to Bharath Institute of Higher Education and Research
Chennai, Tamil Nadu, India.

***Abstract*- Digital payments have gained significant popularity in recent times, owing to the convenience and security they offer. Concurrently, there is a growing interest in digital currencies as they are widely accepted by numerous businesses and websites. The advent of Web3 has further simplified digital currency transactions, enabling anyone with a digital wallet to hold and transact digital currency with ease. However, this easy accessibility also poses a threat, as decentralized currencies lack ownership or control, and victims of scams or frauds have little or no recourse to recover their lost funds. In light of this challenge, a proposed system involves deploying a smart contract on the Ethereum network that safeguards the customer's funds by holding them and preventing their transfer to the vendor until the delivery partner enters the One-Time Password (OTP) provided by the smart contract. If the OTP verification fails, the contract will be timeout, and the funds will be returned to the customer, ensuring the prevention of fraudulent transactions. This system aims to mitigate the risk of digital currency scams and bolster the security of digital transactions, instilling confidence in users and promoting the wider adoption of digital payments.**

Keywords: OTP - One-Time Password

INTRODUCTION:

The third era of the internet has begun, and the web sector started adopting a decentralized online ecosystem that is trustable and hackproof, still, there are many E-commerce websites out on the internet that looks legit, but the product won't get delivered even after successful payment. These fake websites use genuine payment gateways which transfer money into the scammer's account after the customer makes a payment. If the money is transferred via web3 based payment gateway into the scammer's account it is almost impossible to recover the fund even after filing a complaint because of anonymity.

This problem can be solved when there is an entity that takes money from the customer and holds it without transferring it to the vendor's account until the product gets delivered to the customer. This service is called 'Escrow'. There are a lot of Escrow services out in the market which hold the fund of the customer until the customer approves manually when the product gets delivered, but there is no guarantee that the customer is trying to fraud by providing misleading information. The current solution adds an extra verification step on the customer side in order to overcome fraud from both parties.

When a customer makes a payment using the proposed payment gateway the money will be transferred into a newly generated smart contract deployed by the payment gateway on Ethereum main network. An OTP will be sent to the customer's account from the smart contract which will later be used during handing over the delivery to the customer. The smart contract will have a timeout feature that will be set by the vendor. This feature will ensure that the smart contract returns funds to the customer when the product is not shipped within the timeout period. When the vendor ships the product within the timeout period the vendor has to enter the tracking id of the shipment into the smart contract. The product can only be shipped by approved delivery partners as the smart contract needs to fetch details and verify delivery. During the final step of delivery which is handing over the shipment to the customer, the delivery agent verifies the customer by entering the OTP provided to the customer by the smart contract. The delivery will be marked successful upon OTP verification by the smart contract and the funds will be sent to the vendor. If the customer denies providing OTP or the verification fails the shipment will not be handed over to the customer. After a couple of unsuccessful delivery attempts the shipment will be canceled and sent back to the vendor, and the funds will be sent back to the customer.

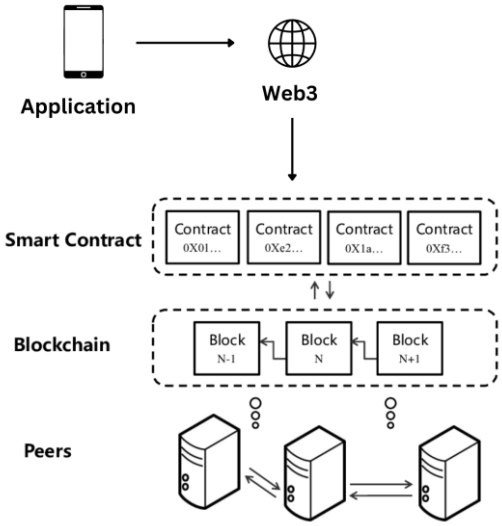
The smart contract is powered by Ethereum which is decentralized and runs on a network of computers around the world, making it resistant to censorship and tampering.

METHODOLOGY:

The world is now looking towards web3, and a lot of technologies are being built over the web3 foundation. The proposed system targets the web3-based payment system by using the power of a decentralized network. The smart contracts are built using a solidity programming language as it can be deployed on the Ethereum network. The deployed contracts are immutable, so the contracts have to be intensively tested before deploying to the Ethereum network. The approach for pre-deployment testing will be conducted using a tool called hardhat. As the smart contracts interact with funds we need to use test funds for testing and the contract cannot be tested on the main Ethereum network as only original funds can be transacted on the main network. The test funds can be found on test networks such as the Goerli network. Goerli network simulates the Ethereum main network and won't be an issue if the funds are lost during the testing phase of the smart contract. The database function will also be tested on a simulated database provided by GunDb, the data won't be stored on the main network of the distributed GunDb network during the testing phase. The

application interacts with the Web 3 network using a service called Wagmi, and the Wagmi service can also be used with the Ethereum main net during production.

ARCHITECTURE DIAGRAM:



PROBLEM STATEMENT:

Fake E-commerce sites are popping up every day on the internet using traditional payment gateway which makes customers think the website is legitimate. Customers are getting cheated because of these websites as the product will not be delivered after the payment. Even after a case is reported with the payment gateway service the chances of recovering money are very little and time-consuming. The cases have skyrocketed since the public use of cryptocurrency. The payment method is strong but it doesn't guarantee the genuinity. The scammer cannot be traced because of the anonymity maintained by web3. The existing escrow solutions heavily depend on customer approval which can also be a point of concern when misleading information by customers is considered.

PROPOSED SYSTEM:

The system is supported by the world's second-largest cryptocurrency called Ethereum. A smart contract is deployed onto the Ethereum network which acts as a payment handler. When a user uses our payment gateway, the money will be transferred to the smart contract and the smart contract returns an OTP to the user which is used to verify the delivery. Every detail of the shipment is logged into the smart contract by the delivery partner. OTP has to be verified by the delivery partner before handing over the shipment to the user. The money will be then transferred to the seller's account.

LITERATURE REVIEW:

The industry is turning toward web3-based technology which ensures privacy and security[1]. Blockchain is now being used in various fields such as insurance, supply chain, and digital assets[2]. All these are possible because of smart contracts. The use of smart contracts has increased in the networks like Ethereum and Polygon.[3] But these smart contracts could also be the vulnerability that lets an attacker exploit the contract.[4] The vulnerability can also be caused because of a forever loop which is caused by the programmer's error[5]. The smart contract is also prone to Distributed denial of service(DDOS) attacks, which is flooding requests to the smart contract from different IP addresses Double spending is the most common problem, the user can spend the amount from his wallet two times if the second is payment request is requested immediately.

MODULES:

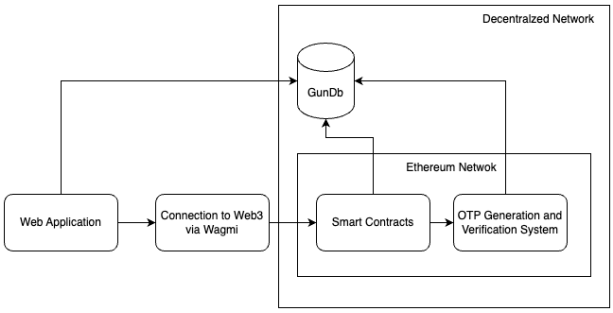
Step 1: The factory smart contract code which is capable of generating daughter contract code is written in solidity language, the code is tested against the available test networks such as the Goerli network. The code is then deployed to the test network and the smart contract address is noted.

Step 2: The daughter code is written in solidity as well. The Daughter code is the one that holds the funds from the customer. The code is tested against test networks and deployed onto test networks.

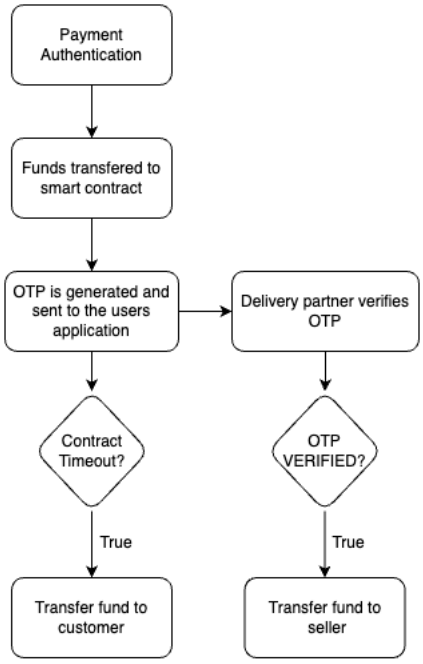
Step 3: GunDb for storing the history of transactions and the status is created using Node js. The created code is then deployed to the GunDb network for creating a decentralized database system.

Step 4: The application which is used to interact with the smart contract is built using React js the interaction happens via a service called Wagmi. The application is also connected to the GunDb for real-time updates on the shipment. Authentication of the user will be taken care of by browser wallets such as Metamask.

BLOCK DIAGRAM:



FLOW CHART:



CONCLUSIONS AND FUTURE WORK:

In conclusion, the proposed payment gateway offers numerous benefits to both buyers and sellers. The use of the Ethereum blockchain and smart contracts provides a secure, reliable, and efficient payment processing system that eliminates the need for intermediaries, reducing costs and processing times. The implementation of OTP authentication ensures that only authorized individuals can access the shipment, preventing fraudulent activities. The logging of shipment details in the smart contract ensures that every transaction is accounted for, providing a comprehensive record that can be utilized in case of disputes.

The Ethereum blockchain is considered one of the most secure and reliable blockchain networks globally, and it is renowned for its smart contract capabilities. Smart contracts are self-executing computer programs that facilitate, verify, and execute the negotiation and performance of a contract automatically. This technology has significant potential in the payments industry, as it reduces the need for intermediaries, such as banks, which typically slow down the payment process and increase costs. Furthermore, the proposed payment gateway provides an additional layer of security through the OTP verification system. This system ensures that only authorized individuals can access the shipment, preventing fraudulent activities such as impersonation, theft, or misplacement. By utilizing this authentication system, the payment gateway provides a higher level of security and reliability than traditional payment gateways. In addition to security benefits, the proposed payment gateway also offers transparency benefits. The logging of every shipment detail on the smart contract ensures that every transaction is accounted for, providing a comprehensive record that can be utilized in case of disputes. This transparency ensures that all parties involved in the transaction are aware of every detail, reducing the likelihood of disputes and increasing trust in the payment gateway. Overall, the proposed payment gateway is a highly secure, reliable, and efficient payment processing system that benefits both buyers and sellers. The implementation of the Ethereum blockchain and smart contracts provides a decentralized system that eliminates intermediaries, reducing costs and processing times.

The use of OTP authentication and logging of shipment details provide an additional layer of security and transparency, making the payment gateway an ideal solution for e-commerce platforms. With these benefits, the proposed payment gateway has the potential to revolutionize the payments industry and pave the way for future developments in the field.

The current project has a limitation in terms of accessibility, as it can only be interacted with through a webpage. To overcome this limitation, it is possible to develop a Software Development Kit (SDK) that can be integrated into mobile applications by developers. This will make it easier for users to interact with the project using their mobile devices, which are more convenient for many users.

In addition to the above, the current implementation of the smart contract is deployed manually. This means that each time a new instance of the contract needs to be created, it must be deployed manually. This process can be made more efficient and automated by using a factory contract. A factory contract is a smart contract that is designed to create other contracts. It can be programmed to deploy a new instance of the smart contract whenever a new user needs to use the application. This will save time and effort by automating the process of contract deployment.

The implementation of an SDK and factory contract are both important considerations for the future of the project. By enabling access through mobile applications, the project will become more accessible to a wider range of users. This will increase the potential reach and impact of the project. Additionally, by implementing a factory contract, the deployment process can be streamlined and made more efficient. This will reduce the likelihood of errors and make it easier to scale the project as it grows.

Overall, these improvements will help to make the project more user-friendly and scalable. They are important steps to take for the continued success and growth of the project. With these improvements in place, the project will be better positioned to achieve its goals and have a positive impact on its users.

REFERENCES:

1. I. Pavlova, “Blockchain etfs: dynamic correlations and hedging capabilities,” Managerial Finance, vol. 47, no. 5, pp. 687–702, 2020
2. H. Hellani, L. Sliman, A. Samhat, and E. Exposito, “Overview on theblockchain-based supply chain systematics and their scalability tools,” Emerging Science Journal, vol. 4, no. Special Issue, pp. 45–69, 2020.
3. Petar Tsankov, Andrei Dan, Dana Drachsler-Cohen, Arthur Gervais, Florian Buenzli, and Martin Vechev. Security: Practical security analysis of smart contracts. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pages 67–82, 2018
4. M. Dell’Erba, “Demystifying technology. do smart contracts require a new legal framework? regulatory fragmentation, self-regulation, public regulation.” SSRN Electronic Journal, 01 2018[1] Andrew Brosnan, Fionn Cox, Daryl Hemmingway, Lu Ren, “Leveraging Escrow in Ireland: A Guide to Acquisition and Implementation of Full In-House Escrow”, 2022.
5. 0xPredator. The ultimate smart contract auditing guide. https://medium.com/coinmonks/the-ultimate- smart-contract-auditing-guide-ddec6e78e7dc/, 2022.