Blockchain-Based Unified Payment System

1Vaishnavi Todkar, 2Retik Singh, 3Rutuja Varale, 4Shailendra Singh, 5Pratush Jadoun

1Student, 2Student, 3Student, 4Student, 5Professor
1Department of Computer Engineering,
1Dhole Patil College of Engineering, Pune, India

Abstract - The blockchain-based unified payment system is an initiative to digitally transfer money to make it more secure with better efficiency. The number of transactions is increasing across the world. This increase in digital payments can be attributed to the significant increase in mobile data usage and mass adoption due to the convenient nature of the payment process. This system focuses on the aspect of transparency. The usage of the blockchain would firstly prevent the denial of service that has occurred when the Google and Flipkart servers are down. And secondly, the large transaction data would enable better fraud detection. This system keeps a record of the transaction made by the user in the past. Users can send or receive money in their digital wallets.

Index Terms - Blockchain, Transactions, Wallet.

I. Introduction

Online transactions continue to increase and become a significant part of the global economic system, the ability to accept these payments online becomes more important for businesses. Blockchain makes it easy to maintain the transactions as a whole and fastens the transactions where the current system fails. It is much slower compared to blockchain [6]. As part of this project, we will introduce blockchain for online payment transactions which will make the system reachable from everywhere in the world. As a result, it will show the transaction history of the user in the past.[4]

Users are registered as part of the Project Payment system, and users' transactions are stored in the system. Users must register before they can access the functionalities of the system, whether they must send the money or receive the money. Using their email address and password, the user can access the system [2]. The major goal of this software is to make the transaction simpler and faster and at the same time a secure one. Users have the option to see the transaction history record and access their digital wallet.

The primary features of this system include the user's dashboard, digital wallet, transaction history record, sending and receiving money digitally, checking whether the transaction is completed or not, and notification alert for transaction fail cases [12].

Transparency and data stabilization are the major issues in today's digital payment system. So, to overcome this problem we use blockchain technology to keep the record of the user's transaction for better transparency in the system usage. It will provide better security for the user's transactions and personal data. This system is the single app infrastructure for Android and iOS users. This software provides data stabilization for mobile app payment.[3]

Blockchain is the best and most convenient document database to keep information secure because it can be used in a variety of fields where preserving records is important. React Native, a frontend JavaScript framework that makes it simple to build sophisticated apps is used to build the app. Expresses Js framework and Node Js, a server-side platform for open-source development that supports JavaScript code, are used to build the project's backend APIs. The main feature of blockchain technology is its attractive flexibility for many business fields, such as banking, logistics, Networking, smart contracts, the medicine industry, Engineering, and cyber security. Cryptography is used in blockchain. It is a means of ensuring transactions are done safely while securing all information and storing the value. As a result, anyone using blockchain can ensure complete confidence that once something is recorded on a blockchain, it is done so legally and in a manner that conserves security.[8]

The integrity of the data is guaranteed using a digital signature, which is the main aspect of data recorded in the blockchain. The first block of the blockchain is termed the Genesis block. It contains its transactions that produce a unique hash when combined and validated. This hash and all the new transactions that are being processed after they are used as input to create a unique hash. This is used in the next block in the chain. In the blockchain, each block links to its previous block through its hash, forming a chain.[1]

II. Motivation

Mobile phone usage is highly elevated in the current era compared to its usage a decade before. The number of mobile phones is higher than the number of bank accounts that exist in the world. Due to its high usage level, most business organizations, the entertainment industry, banks, the education sector, and almost all fields turn towards mobile phone adaptability [5]. To benefit from this device, they launch their applications for better usage by people. Almost all banks facilitate consumers with mobile phone applications to use. People use mobile phones for shopping, transferring money, and getting various services done on time. The maximum use of mobile devices and versatility motivate us to use mobile payment systems (MPSs). Different models of payment systems have been proposed, but many limitations exist, such as security and privacy concerns [10].

III. Literature survey

[1] Showed the system stability under network disturbances and demonstrated the whole system operates well in resource-constrained, dynamic, intermittently connected environments.

[2] As a result of his research, giving a secure process for online transactions by overcoming the attacks such as man-in-the-middle attacks and eliminates third-party gateways which makes the entire process of online money transfer faster.

[3] The results indicated the effectiveness of our gateway selection in achieving high success rates. For these results, keeping the gateways open in terms of channel balance to send and receive payments is an important objective that can be achieved by considering inbound and outbound capacity balance.

[4] Loss of data and access to confidential data can be avoided using the AES algorithm. The systems show a performance increase compared to many other techniques used in the network.

[5] The Smart Routing solution for payment transactions presented in this paper processes millions of transactions in real time and provides significant improvements in the success rate for payments.

[6] Implementation of the traditional wallet mechanisms of the banks in a blockchain ecosystem could provide enhanced security for the users. A much more secure system can increase the use of digital payment systems by people and can encourage more people to adopt it.

[7] The complete sync of processes, integrity, and uniqueness of all processed information are the main advantages of using blockchain. Due to the mechanism, tampering with data is not possible in the blockchain, which makes it possible to establish a high-cost global credit system.

[8] Combining traditional financial services with novel blockchain technology and smart contracts enables users currently excluded from the financial system to access services such as payment, remittance, currency exchange, and microlending. As a result, Everex renders existing capital transfer systems obsolete that are expensive for usage, suffer from long lines, exchange rate losses, counter-party risks, bureaucracy, and extensive paperwork for it.

IV. Algorithm

A. Consensus algorithm –

In a two-dimensional image, after a DWT transform, the image is divided into four corners, the upper left corner of the original image of the module, the lower left corner of the vertical details of the system, the upper right corner of the horizontal details, the lower right corner of the component of the original image detail (high frequency) of the system [13].

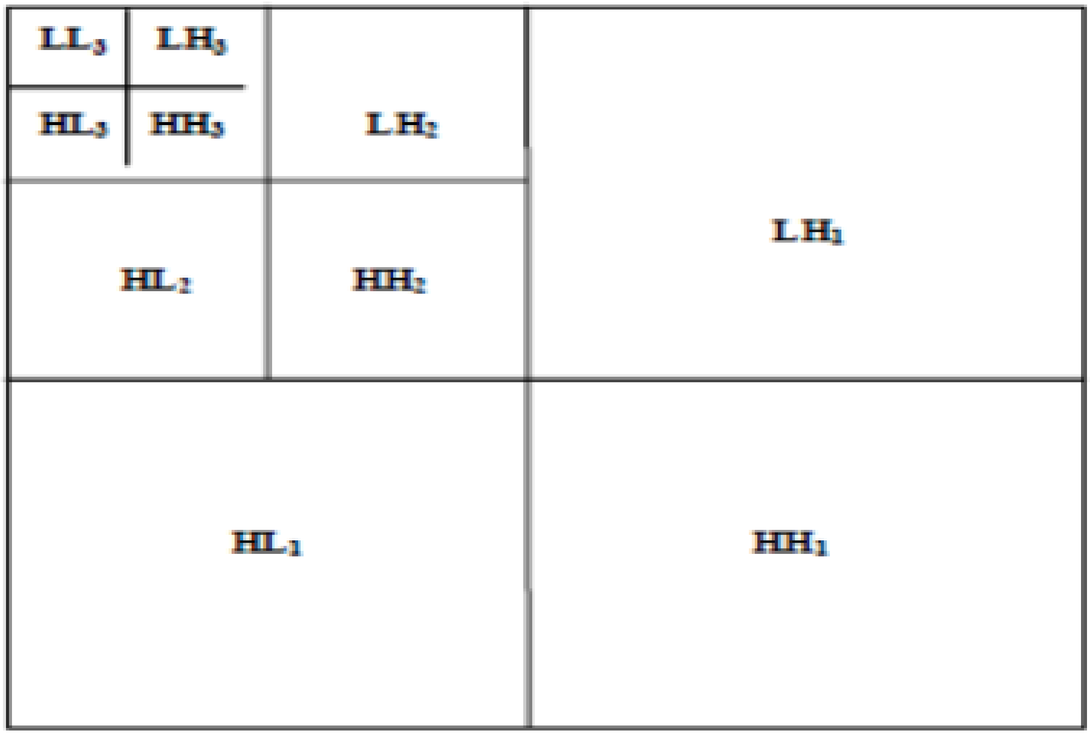


Fig.1 DWT Decomposition model

Based on this algorithm uses a different color image multiplied by the weighting coefficients of different ways to solve this visual distortion, and embedding the watermark of the module, and wavelet coefficients in many ways, enhances the robustness of the watermark that is available [15].

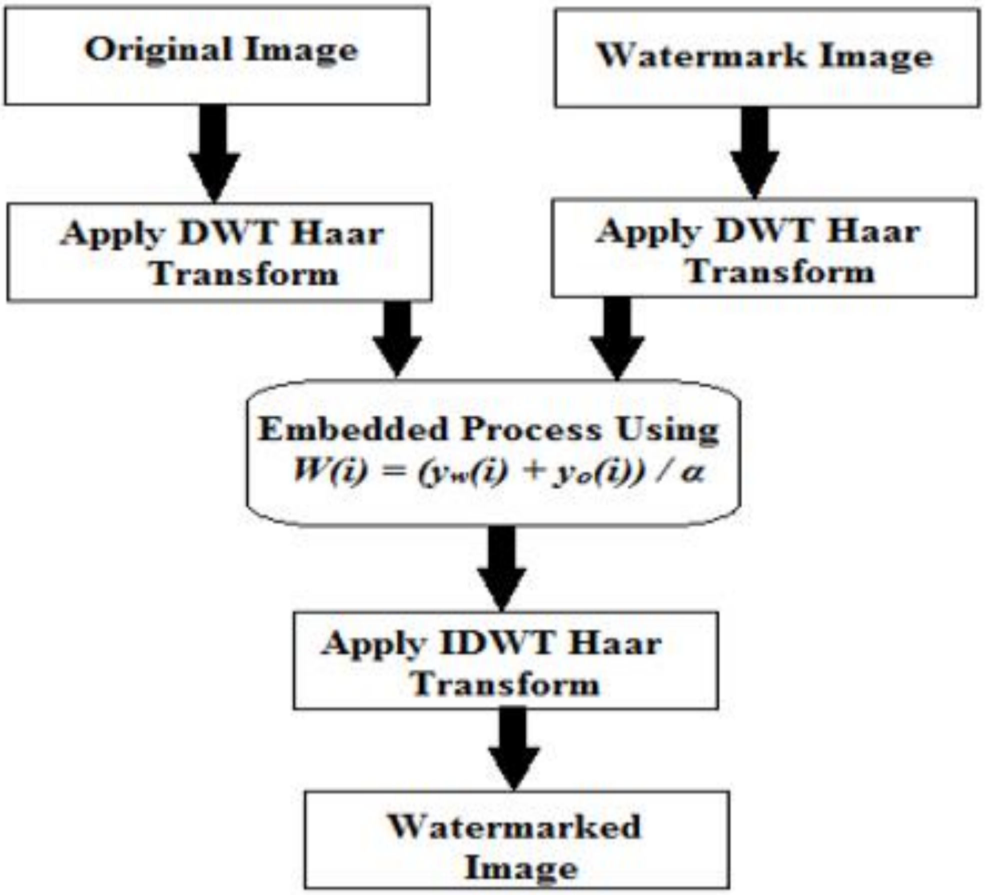


Fig.2 Watermark embedding algorithm Block Diagram

After that, we select the ordered coefficient from 1 to N to get the N coefficient. The formulae of watermark embedding are

$$\mathbf{C_w(i) = Y_o(i)+\alpha_1 w(i)} \qquad (1)$$

So, the parameter α is called embedding intensity and the effect of validity of the algorithm is directly applied after the process, then apply the inverse of the wavelet transform is to the image to find out the watermark image [15].

B. Hashing algorithm –

The extraction algorithm process is the inverse of the embedding process of the system module, to assume that the watermark, as well as the see value, is available at the receiver end of the module to the authorized users of it.

The operation of the channel separation on the system on the watermarked color image for generating its sub-part of original images from it, and then a two-level discrete wavelet image transform is applied to the sub-images to generate the approximate coefficients of module and detail coefficients from the system [12].

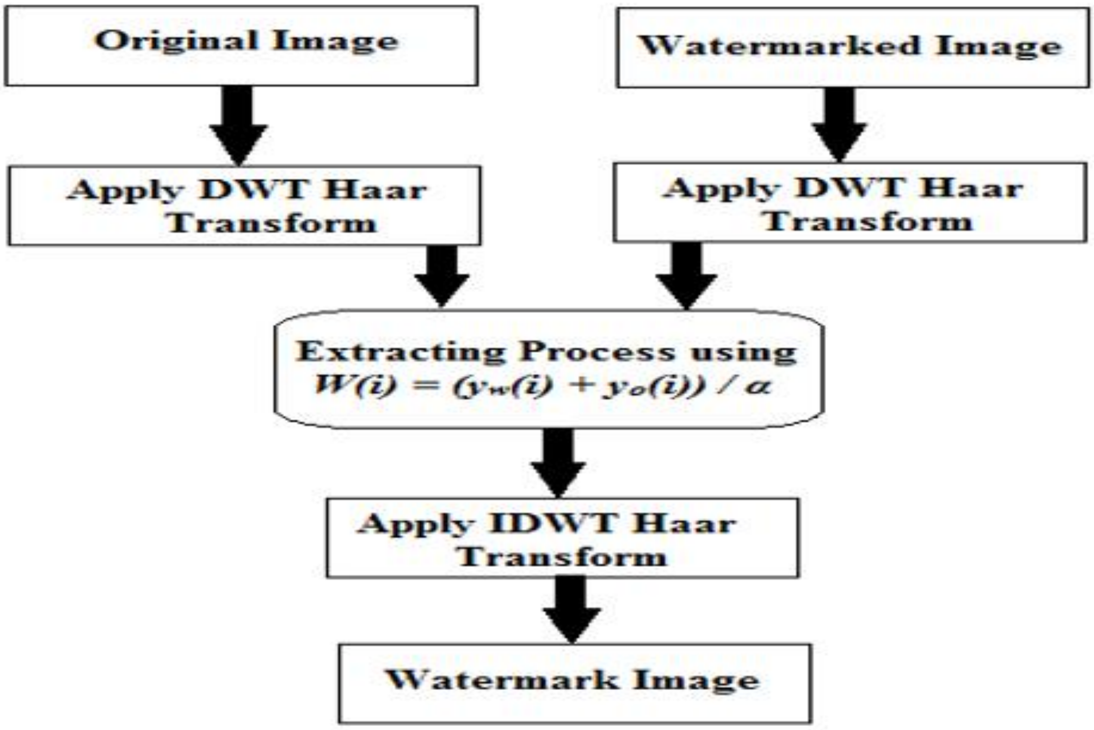


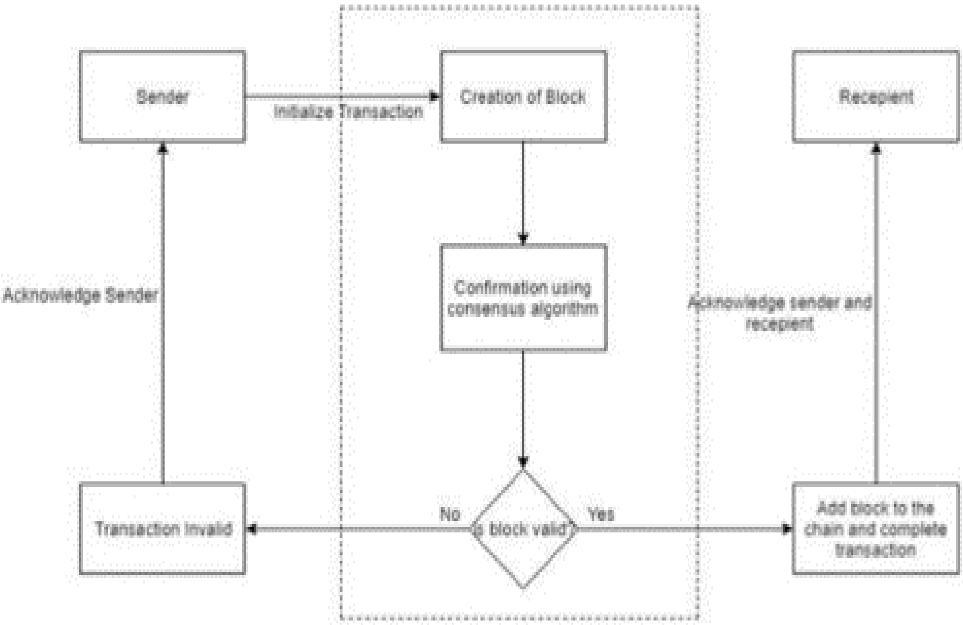
Fig. 3 Watermark Extraction Algorithm Block Diagram

For this purpose, the formulae used are-

$$\mathbf{W(i) = (y_w(i) + y_o(i)) / \alpha} \qquad (2)$$

The Execution Inverse 2-level discrete wavelet transforms it to generate the level-three watermark image extracted from the system [12].

V. SYSTEM ARCHITECTURE


Sender
Initialize Transaction
Creation of Block
Recepient
Confirmation using consensus algorithm
Acknowledge Sender
Acknowledge sender and recepient
Transaction Invalid
No
Is block valid?
Yes
Add block to the chain and complete transaction

In this project, we propose a blockchain-based unified payment gateway. The above figure explains the workflow of the usage of blockchain in online payment systems [9].

The main processing steps for the proposed system are as follows:

- Creation of block
- Confirmation of block
- Check whether the created block is valid or not.

First, the user initializes a transaction, and a block has been created which is sent for confirmation. The confirmation is verified using the consensus algorithm. Blockchain networks depend on a consensus algorithm that is to meet the agreements among various distributed nodes of the system. It is checked whether the block is valid or not. If the block is not valid then acknowledge the sender. After the successful verification, the block gets added to the chain, and the transaction is done [17].

VI. WORKING

The software has a ton of features, including the ability to manage and access the digital wallet, and has recorded generated of past transactions made by the users. All these characteristics support the payment management and handling of the digital transaction system. The following list of the app's modules in detail:

1) User Dashboard

The basic details about the user are made available, including name, age, phone number, email, and password are the activities carried out inside the app. All these things work together to collect data about the user so that it can be used for authentication purposes Afterwords, and this information is necessary for creating the account on the system so that the user can do the transaction without worrying about the safety of data.

2) Transaction

The main part of the system is the transaction page where all the transactions are going to happen. The transaction history of the record of transactions will be maintained here for future needs. The date, time, the money receiver name, mobile number, and how much amount has been sent or received will be shown in the record sheet.

3) A Digital Wallet

Digital money creates doubt of safety and security, so we are providing a blockchain-based wallet that can securely save the money of the user for the making transaction easy for the user to do. Getting money from the bank or physical money is not an easy process nowadays, so having a digital locker/wallet that can save your money securely is important.

4) Send or Receive Money

The system application will also have a send or receive page where the user can see the amount, he/she debited or credited in the account. It makes it more secure and transparent for the user to handle the device and use it easily while making transactions online through the system.

5) Blockchain Verification

Blockchain verification helps to handle a large amount of data records and easily go through them for managing purposes. Blockchain is a secure technology that helps to handle the data online and handle the money of the user by giving the feature like a digital wallet. So, we added blockchain for authorization purposes to manage the data and the information.

6) **Transaction Status**

At the end of the process, the system will show the transaction status of the user's transactions that he/she made. If the transaction is completed, then the system will send a notification to the user that the transaction has been completed. And if the transaction fails due to circumstances, then it will send the message that the transaction has failed.

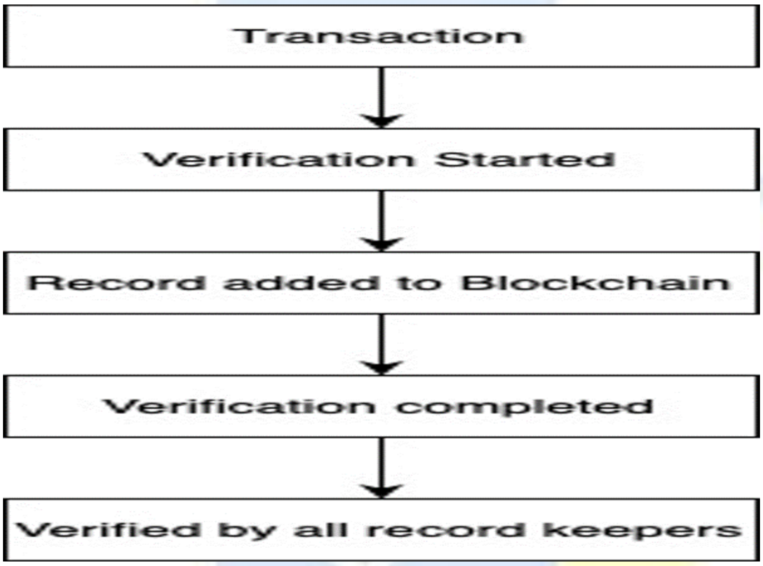


Fig 1. Process Flow Diagram

VII. Implementation

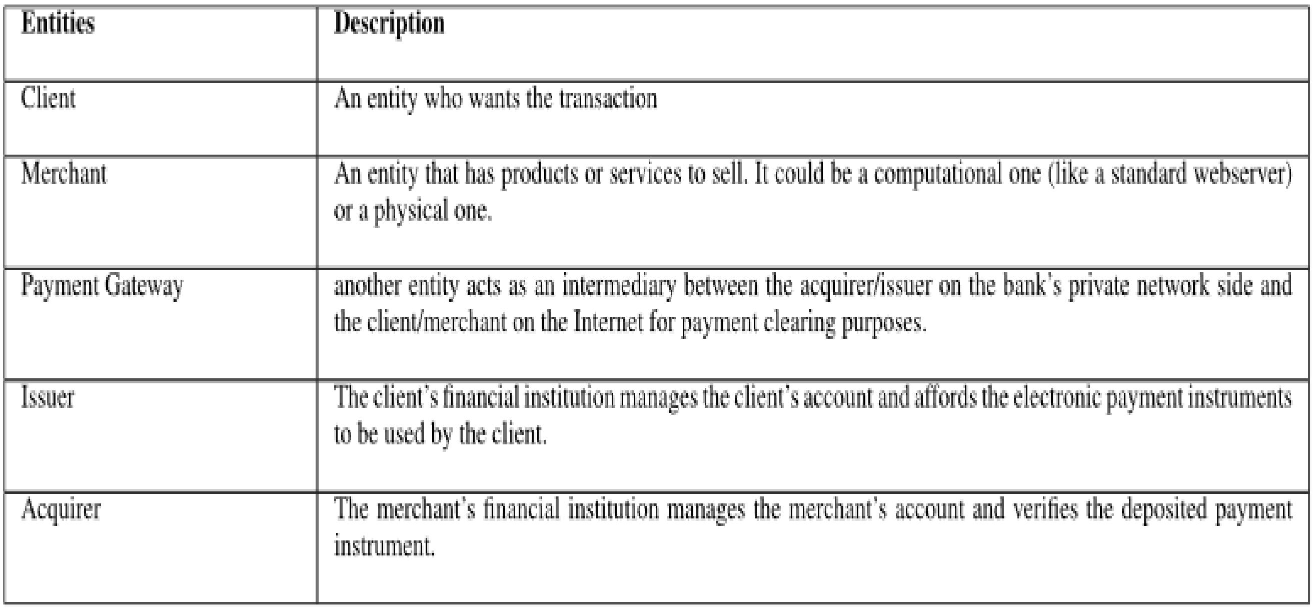
The system is developed using React Native, a JavaScript Framework. It is owned by one stakeholder I.e., User. This application can be run across all Android and IOS phones. To develop applications that can run on Android and iOS devices, Android Studio and Xcode are used to verify their integrated development environment.

1) User Module:

Users can register themselves on the system and make their transactions using the transaction tab inside the dashboard, they can access their wallet, keep records of past transactions, check the transaction status, get the notification of status, etc. They can maintain their profile and digital wallet safe and secure digitally using the software. They can maintain their profile and digital wallet safe and secure digitally using the software.

2) Mobile Payment System Security Mechanism:

MPS security mechanism includes Encryption technology, authentication, and a firewall [12].



Entities	Description
Client	An entity who wants the transaction
Merchant	An entity that has products or services to sell. It could be a computational one (like a standard webserver) or a physical one.
Payment Gateway	another entity acts as an intermediary between the acquirer/issuer on the bank's private network side and the client/merchant on the Internet for payment clearing purposes.
Issuer	The client's financial institution manages the client's account and affords the electronic payment instruments to be used by the client.
Acquirer	The merchant's financial institution manages the merchant's account and verifies the deposited payment instrument.

3) Authentication:

Authentication included: Digital signature and certificate authority.

a) DIGITAL SIGNATURE

A digital signature (DS) is used to verify the origin of the received text and prove whether the received text is without any changes or not. To certify the availability of DS, public key infrastructure (PKI) is frequently used. It suggests a complete set of security assurance and follows different public key encryption standards for different sectors like online banking, e-banking, e-government, and e-commerce securities [17].

b) CERTIFICATE AUTHORITY

The Certificate Authority (CA) is a trusted organization that publishes and manages network security PKI and credentials for message encryption. As part of the PKI, the CA will use the registry for verification. Users have the right to verify the information in the digital certificate provided by the applicant. Suppose RA (Register Authorities) verifies the applicant's data and issues a digital certificate. Users are responsible for distributing and revoking certificates in a communication system. Depending on the PKI, upon request, the certificate may contain the holder's public key, the data of the holder, the certificate, the name of the certificate holder, and other information about the holder of the public key [20].

c) FIREWALL

The firewall can simultaneously protect the system network or local network against network-based threats. The firewall allows access to the outside world to the local network of the system. In most scenarios, a firewall is necessary because it is difficult to equip all devices with different security devices. Typically, her firewall is inserted between two networks [20].

VIII. Results and Discussions

The user is led to a screen where they must log in or register as soon as they install the application. After completing the registration process, users can log in using their email address and password. Once logged in, the user can see the dashboard. Users can send or receive money using the system [8]. If the user requires a transaction history of the record, then they need to navigate toward the transaction page in the feed. There is also a feature of the wallet that keeps the digital money safe and secure for the user for the transaction purpose. After the transaction is done the user will get the notification/message whether the transaction is completed or not.

When all the information is confirmed then the block is valid in the system. This leads to successful transactions on the system and the user is informed about it. The block is added to the blockchain, and the user gets the receipt of the transaction. If the block created is invalid, then the transaction is invalid, and the user gets notified about it.

IX. CONCLUSIONS

To sum up, the digital transaction system needs to digitalize its transparency and stabilization effectively so that managing the user's data will be easier and much simpler and takes less time. The Blockchain Payment System is simpler to keep track of the user transaction history record and personal data information and keep the individual digital wallet of the user for the money transaction. Android and iOS users can access the features of this system on a single software program only [9].

This paper discussed various payment schemes and their usage, and technology, and provided security mechanisms. Most payment methods are account-based payment systems, and their focus is on security, privacy, confidentiality, and authentication. We present an overview and discuss the different components of MPS. We presented a detailed survey of the existing MPS structure and its limitations; provided detailed history, development, and deployment of MPS [13]. We discussed different aspects of MPS, including socioeconomic conditions, cost efficiency, diffusion of mobile phones, convenience, new initiatives, heavy restrictions and regulations, limited collaboration, an underdeveloped ecosystem, and security problems entity roles in MPS form different aspects. We discussed different security mechanisms involved in MPS. We also provide an analysis of the encryption technologies, authentication methods, and firewalls in MPS [17].

Thus, the application aims to give a secure process for online transactions by overcoming the attacks such as man-in-the-middle attacks. This system will provide a reduced number of steps in transactions which would be beneficial for the users. And it will also reduce API calls. We hope that this application causes improvements in the blockchain industry that are advantageous to both the user and the company.

X. FUTURE WORK

With blockchain technology, enterprises can automate their business processes while maintaining high security and transparency side by side. In many industries, the payments and finance industry also banking have been behind the hype of the trend [4]. The whole landscape surrounding the idea of transparency, and consensus increases the prospect of a global operation without pushing the risks. Mobile payment solutions will increase the user base, which is already sufficient compared to other traditional methods. This increase will ultimately result in a load on the network infrastructure, which is the backbone of the success of such solutions. Advancement in next-generation network systems and their impact on mobile payment system solutions will be another research area to explore in the future. Further, research can be done on current bottlenecks resulting in fewer mobile payment solutions and remedial measures using network advancements [13].

This research has some practical and theoretical limitations that may provide valuable findings for future research. For example, we do not consider the potential impact of digitization on mobile payment systems, making behaviors more complex than those resulting from modular reorganization alone [6]. Our goal is to record dynamics that cannot be found in developed countries. We hope our findings can be applied for reference.

XI. REFERENCES

1) **Yining Hu, Ahsan Manzoor, Parinya Ekparinya**, **Kanchana Thilakarathna, and Aruna Seneviratne, (**2019**)** "Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain System".

2) **Suat Mercan, Enes Erdin and Kemal Akkaya,** Department of Computer Engineering, Florida University, (2020), "Improving Transactions Success Rate via the Smart Gateway Selection in Cryptocurrency Payment ".

3) **Karthikeya Thanapal, Karthik Mudaliar, Dhiraj Mehta, and Bushra Shaikh**, SIES Graduate School of Technology, University of Mumbai, India, ITM Web of Conferences, (2020), "Online Payment Using

Blockchain Technology", ICACC-2020

4) **Pon Sangeetha. J, Ramya. S.S, ChristalAntony.V,** Department of Information Technology, Sri Krishna College of Technology, "Secured payment gateway for authorizing E-commerce websites and transactions using Machine Learning Algorithm", (2020), International Conference, India.

5) **Ramya Bygari, Aayush Gupta, Shashwat Raghuvanshi, Aakanksha Bapna, Birendra Sahu**, Bengaluru, India, (2021), "An AI-powered Smart Routing Solution for Payment Systems".

6) **Mathew Koshy Karunattu, Akeel Mohammed Ashique, Dr. Ansamma John, Dr. Manu J Pillai**, Department of Computer Science and Engineering TKM College of Engineering Kollam, India, (ICOSEC 2020) IEEE Xplore Part Number: CFP20V90-ART; ISBN: 978-1-7281-5461-9, "Digital Payments: Blockchain-based Security Concerns and Future".

7) **Varsha Naik, Riya Pejawar, Riya Pejawar, Prof. Anagha Aher, Prof. Sneha Kanchan**, Department of Information Technology, AP Shah Institute of Technology, IEEE International Conference on Computational Intelligence for Smart Power System (CISPSSE-2020), July 29-31, 2020, India, "Expeditious banking using Blockchain Technology".

8) **Alex Norta, Benjamin Leiding, Alexi Lane,** Blockchain Technology Group, Akadeemia tee 21/1, 12618 Tallinn, Estonia, University of Gottingen, ¨ Institute of Computer Science, Gottingen, Germany, Everex.io, Singapore, (2019), "Lowering Financial Inclusion Barriers in Blockchain-Based Capital Transfer System".

9) **Mahmoud Saleh Obaid Arab,** American University, "Mobile Payment Using Blockchain Security", (2021), **R. Guhan**, School of Management, Deemed University, **(**2022).\

10)Behavioural Intention of Unified Payments Interface (UPI) Usage in the Pandemic: Evidence from Tamil Nadu", (2022), International Conference on Interdisciplinary Research in Technology & Management (IRTM 2022).

11)**Dr.A.Latha, Dr.Deepa.M**, KCT Business School, Kumaraguru College of Technology, Coimbatore, India, International Conference on Interdisciplinary Research in Technology & Management (IRTM 2022), "Consumer Perspective on Mobile wallet Payment system".

12)**Waqas Ahmed1, Aamir Rasool1, Abdul Rehman Javed1,** (Member, IEEE), **Neera Kumar** 2,3, (Senior Member, IEEE), **Thippa Reddy Gadekallu 4, Zunera Jalil 1,** (Member, IEEE), and **Natalia Kryvinska 5**, "Security in Mobile Payment Systems, A Comprehensive Survey on online payments".

13)**J. Sun and N. Zhang**, ‘‘The mobile payment based on public-key security technology,’ J. Phys., Conf. Ser., vol. 1187, no. 5, Apr. 2019, Art. no. 052010.

14)**S. F. Verkijika,** "An affective responses model for acceptance of mobile payment system Electron in the system". Commerce Res. Appl., vol. 39, Jan. 2020, Art. no. 100905.

15)**C. Iwendi, Z. Jalil, A. R. Javed, T. Reddy G., R. Kaluri, G. Srivastava, and O. Jo**, 2020, "Key Split Watermark, Zero watermarking algorithms for software protection against cyber-attacks", IEEE Access, vol. 8, pp. 72650–72660.

16)**A. Saranya and R. Naresh,** 'Efficient mobile security for the e-health care applications in the cloud for secure payment online, Neural Processes". Lett., pp. 1–12, Mar. 2021.

17)**I. R. de Luna, F. Liébana-Cabanillas, J. Sánchez-Fernández, and F. Muñoz Leiva**, "Mobile payment is not for all the same, the adoption of mobile payment systems depending on the current technology," Forecasting Social Changes in it, vol. 146, pp. 931–944, Sep. 2019.

18)**Ms. P. Jayanthi1, Dr.S.Kamaksh**i(2021), "Consumer Preference on Mobile Wallet during COVID-19 with special reference to Chengalpet District", svādhyāya - International Journal of Transdisciplinary Research and Development (SIJTRD) VOL.1(2), DEC 2021, PP 57-69.

19)**Sarikaraj, Dr. S. Vasantha** (2020), "Security and Challenges of Mobile Wallet Adoption", Tathapi, Vol-19-Issue-10.

20)**Jamie Mew, Elena Millan,** (2021), DOI: 10.1080/09593969.2021.1879208, "Mobile wallets, the key drivers and deterrents of consumers in the intention to adopt it", The Review of the Retail, Distribution, and Consumer Research.