A

Project Report on

CRYPTOTREND: A BLOCKCHAIN-BASED CRYPTOCURRENCY WALLET AND VALUE TRACKING APPLICATION

Submitted to the partial fulfillment of the requirement for the award of the degree of

BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE & ENGINEERING

Submitted by:
Rishi Sharma (RA1911003030293)
Vaibhav Agarwal (RA1911003030261)
Tushar Mukherjee (RA1911003030257)
Vaibhav Dhar (RA1911003030288)

Supervised by:
Dr. ABHILASHA SINGH
(Associate Professor, Department of CSE)

SRM Institute of Science and Technology
Delhi NCR Campus, Modinagar,
Ghaziabad (UP)-201204

MAY 2023

BONAFIDE CERTIFICATE

This is to certify that project Report entitled “CRYPTOTREND: A BLOCKCHAIN-BASED CRYPTOCURRENCY WALLET AND VALUE TRACKING APPLICATION”, which is submitted by Rishi Sharma (RA1911003030293), Vaibhav Agarwal (RA1911003030261) Tushar Mukherjee (RA1911003030257) and Vaibhav Dhar (RA1911003030288) in the partial fulfillment of the requirement for the award of degree B.Tech(CSE) of SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, Ghaziabad is a record of the candidate own work carried out by them under my own supervision.

….....
(Signature)
Dr. Abhilasha Singh
Project Supervisor
Associate Professor
Department of CSE

…….....
(Signature)
Dr. Akash Punhani
HOD (CSE)

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We would like to express our heartfelt appreciation to Dr Abhilasha Singh, Associate Professor and Project Supervisor at SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, for her invaluable insights and expertise in the subject matter, which motivated us to work diligently.

Our profound gratitude goes out to Dr. Jitendra Singh and Dr. Rakesh Kumar Yadav, Project Coordinators at SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, for their enlightening guidance and skillful coordination, which served as a perpetual source of inspiration.

We would also like to extend our sincere thanks to Dr. S. Vishwanathan, Director of SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, for his unwavering support that enabled us to undertake and complete our project work.

Our special thanks go to Dr. D. K. Sharma, Dean (Academics), and Dr. R. P. Mahapatra, Dean (E&T) at SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, for their valuable guidance and unconditional support.

We would like to express our gratitude to Dr. Akash Punhani, Head of the Department of Computer Science and Engineering at SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, for his suggestions and encouragement in completing this project.

We also owe our thanks to all the teaching and non-teaching staff members of our college who provided us with direct or indirect help throughout our studies and project work.

Finally, we would like to express our sincere appreciation to our parents, family members, and friends for their unwavering support and encouragement, and to all our well-wishers.

Rishi Sharma (RA1911003030293)

Vaibhav Agarwal (RA1911003030261)

Tushar Mukherjee (RA1911003030257)

Vaibhav Dhar (RA1911003030288)

DECLARATION

We, Rishi Sharma (RA1911003030293), Vaibhav Agarwal (RA1911003030261), Tushar Mukherjee (RA1911003030257) and Vaibhav Dhar (RA1911003030288) hereby declare that the work which is being presented in the project report "CRYPTOTREND: A BLOCKCHAIN-BASED CRYPTOCURRENCY WALLET AND VALUE TRACKING APPLICATION " is the record of authentic work carried out by us during the period from January '23 to May '23 and submitted by us in partial fulfillment for the award of the degree "Bachelor of Technology in Computer Science and Engineering" to SRM IST, NCR Campus, Ghaziabad (U.P.). This work has not been submitted to any other University or Institute for the award of any Degree/Diploma.

Rishi Sharma (RA1911003030293)

Vaibhav Agarwal (RA1911003030261)

Tushar Mukherjee (RA1911003030257)

Vaibhav Dhar (RA1911003030288)

ABSTRACT

The project is an Ethereum management dashboard that aims to give users an user-friendly and efficient way for managing Ethereum transactions and assets. Dashboard allows users to easily transfer ether to other clients along with a message. This feature allows users to keep track of their transactions and easily send ether to other people. The dashboard also displays the user's current ether balance, providing an overview of the user's assets. The transaction history feature allows users to view all of their past transactions, providing a complete record of their Ethereum transactions. The QR code functionality allows users to easily share their Ethereum address with others, making it easy to receive ether from other people. The dashboard also has a prediction column that predicts the price of ether whether it will rise or fall. This feature helps users to make informed decisions about their ether holdings. The prediction is based on historical data and AI models. The prediction column will assist the users in take an informed decision and making changes in their ether portfolio accordingly. The project is made to allow transactions of ethereum more efficient and user-friendly by providing an easy-to-use interface. The project's aim is to develop an efficient platform for managing Ethereum transactions and assets. The project aims in order to simplify the process of monitoring and organizing Ethereum transactions and assets for users.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS iii

DECLARATION iv

ABSTRACT v

LIST OF FIGURES vii

1 INTRODUCTION 1

1.1 Concept of Blockchain 1

1.2 Smart Contracts 3

1.3 Transaction System in BlockChain 5

1.4 Useability issues related to BlockChain 6

2 LITERATURE SURVEY 8

3 EXISTING PROBLEM AND PROPOSED SOLUTION 12

3.1 Problem Statement 12

3.2 Proposed Solution 12

4 Methodology 14

5 Implementation and Result 17

5.1 Implementation 17

5.2 Result 18

6 Conclusion and Future Scope 28

6.1 Conclusion 28

6.2 Future Scope 29

LIST OF FIGURES

1.1 Connecting blocks 2
1.2 Single Block 3
1.3 Smart Contract 4
1.4 Transaction System 6

4.1 Smart Contract with FrontEnd 15

5.1 Transaction System 18
5.2 Front Page 19
5.3 Metamask Connect 19
5.4 Account integrity check 20
5.5 User Dashboard 21
5.6 QR Scanner 22
5.7 Input Form 22
5.8 Validate Transaction 23
5.9 Latest Transaction 23
5.10 Transaction Update 24
5.11 Wallet Address 24
5.12 Ease of login 25
5.13 Transfer 25
5.14 Digital Holding 26

CHAPTER 1

INTRODUCTION

1.1 Concept of Blockchain

"Blockchain is a digital ledger that grants for the safe and clear exchange of information and value without the need for intermediaries". The fundamental technology underpinning the well known digital currency Bitcoin was initially released in 2008, although it has now grown to a range of different uses [1].

Blockchain is fundamentally a distributed and decentralized database. which retains information data across a computer network known as nodes. Every node in the chain have number of deals, formerly a node added to the chain, it is immutable and unchangeable. This creates a endless, tamper evidence record of all deals that have passed on the network [2].

Key features of blockchain is to operate without the need for intermediaries. Traditional transactions often require intermediaries such as banks, lawyers, or other third-party service providers to verify and process transactions. In contrast, blockchain uses a consensus algorithm that allows users to verify transactions themselves, without the need for a central authority.

This decentralization also provides increased security and privacy for users. Because the network is distributed, there is no single point of vulnerability, thereby increasing the level of difficulty for hackers or other bad actors to compromise the network. Additionally, because transactions are recorded on the blockchain using complex cryptographic algorithms, user identities are protected, providing a greater degree of privacy [3].

Blockchain technology are used for a wide range of applications beyond digital currencies. For example, it is possible to utilize it in the development of decentralized databases that can store and exchange information, as well as for developing smart contracts. They are contracts which execute themselves, where the contractual terms between the parties involved are coded directly into the system. These smart contracts are utilized to automate various types of transactions, including financial trades and supply chain management[4].

This technology has the potential to revolutionize various industries by offering improved security, transparency, and efficiency. As the blockchain technology continues to advance, we

expect greater adoption and integration of blockchain systems across various applications. Essentially, blockchain being a digital ledger that securely retains transactions across a network. This is accomplished through a series of nodes, where every node contains a comprehensive list of transaction records along with the previous node's block hash listed in the block header. The very first node in a blockchain is called the genesis block and has no parent block. Each block consists of a title and a body[5].

Important details including the block interpretation, "Merkle tree root hash, timestamp, nBits, nonce, and parent block hash are all included in the block title". The block body consists of a sale counter and deals, with the block size and the size of each sale determining the maximum number of deals that a block may include.[6].

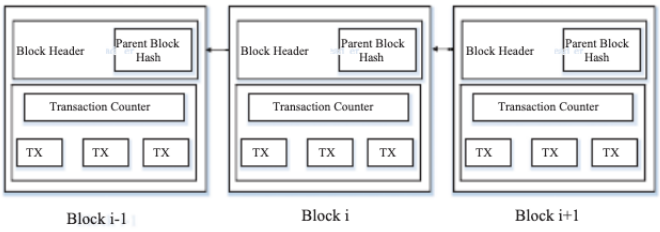

Figure 1.1: Connecting blocks

Using asymmetric cryptography, blockchain verifies the validity of transactions. This involves each user possessing a private and public key pair, where the private key is used to sign transactions, and these signed transactions are then transmitted throughout the network. The elliptic curve digital signature algorithm (ECDSA) is commonly utilized as the digital signature algorithm in blockchains [7].

In blockchain technology, a block is a data structure that holds transaction records and relevant information, such as a header that contains significant details about the block. These blocks are then sequentially linked together to create the blockchain, which is an unchangeable ledger of all transactions.

Blockchain technology boasts several noteworthy characteristics, including decentralization, security, and transparency. With decentralization, there is no central authority that governs the network, while advanced cryptographic techniques are employed to safeguard the blockchain, ensuring its security. Additionally, the blockchain furnishes an open and transparent record of all transactions.

Another significant aspect of blockchain technology is its immutability, which means that

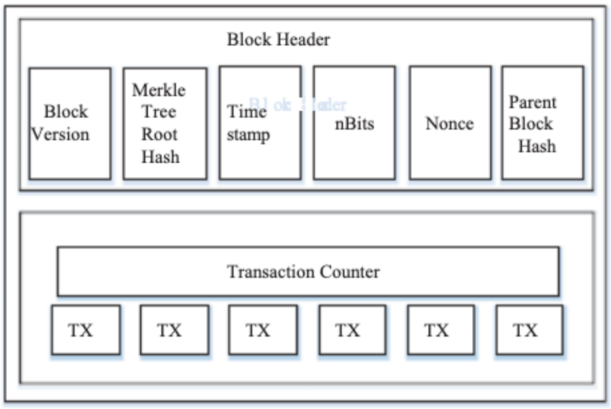

Figure 1.2: Single Block

once a block is added to the blockchain, it cannot be modified or deleted. Moreover, the blockchain employs a consensus mechanism to maintain its integrity. Overall, blockchain technology has the potential to transform numerous by offering a safe, open, and decentralised network, means of conducting and transactions exchanging information.

"The use of blockchain technology is to secure a network and decentralised digital ledger that keeps track of transactions.It is composed of a sequence of blocks, each containing a complete list of transaction records along with the previous block hash found in the block header. The first block in a blockchain is known as the genesis block and is the only block in the chain without a parent block".

They found that people who control keys might encounter challenging security problems.They employed a cognitive walk-through inspection approach in addition to a set of rules with four key responsibilities for bitcoin, however they did not offer any data or numerical depiction of the usability issues with bitcoin wallets.

In blockchain technology, a block is a data structure that holds transaction records and relevant information, such as a header that contains significant details about the block. These blocks are then sequentially linked together to create the blockchain, which is an unchangeable ledger of all transaction.

1.2 Smart Contracts

Smart contracts are digital understanding between multiple parties that is stored on a blockchain. It is essentially a computer program that is able to keep data, processing inputs, and produce

outputs according to its predetermined functions. For example, "a smart contract may have a constructor function that allows it to be created on the blockchain. When a user submits a transaction to create the smart contract, the constructor function is executed, and the sender becomes the owner of the contract. A further instance of a function that might be created in a smart contract is a self-destruct function that can only be used by the contract owner.
In its most basic form, a smart contract can be thought of as a class that contains state variables, functions, function modifiers, events, and structures. These elements work together to execute and enforce the terms of the contract. Additionally, a smart contract can call other smart contracts, creating a network of interlinked contracts".

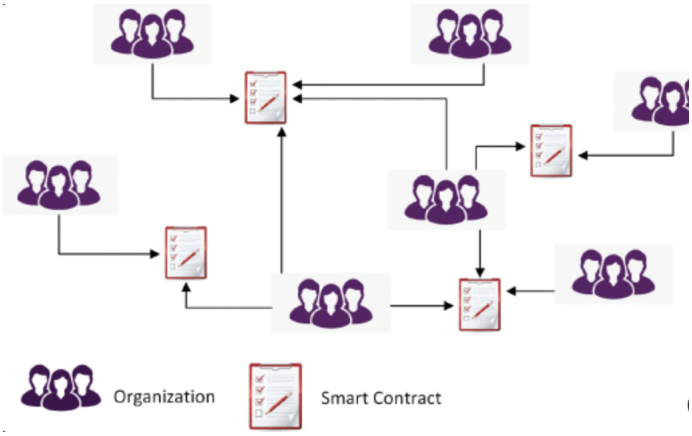

Figure 1.3: Smart Contract

Each smart contract includes state variables and functions. State variables are responsible for storing data or the contract owner's address. There are two categories of state variables: constant and writable. The former cannot be modified, while the latter can be modified by the contract's functions and saved on the blockchain. Functions, on the other hand, are code snippets that can read or modify state variables. There are two types of functions: read-only functions that do not consume gas when executed and write functions that do require gas consumption since they must be processed by the blockchain[8].

The deployment of a smart contract on the blockchain involves the invocation of its constructor function through a transaction, following which the final code of the smart contract is recorded on the blockchain. This code is immutable, indicating that it cannot be modified once deployed. Given that smart contracts are executed on the blockchain, it necessitates a cryptocurrency payment to incentivize miners to process the contract's transactions and avoid infinite contract runs. In essence, a smart contract refers to a digital agreement stored on a

blockchain and executed by a computer program. It encompasses state variables, functions, and other elements that function together to enforce the contract's terms. To host a smart contract on the blockchain, its constructor function must be invoked via a transaction. Thus, smart contracts require payment in cryptocurrency to avoid infinite contract runs.

1.3 Transaction System in BlockChain

In the world of electronic currencies, we define an electronic coin as a chain of digital autographs, wherein the current proprietor transfers the coin to the coming proprietor by digitally subscribing a hash of the former sale and the public key of the coming proprietor and adding these to the end of the coin. To ensure that the chain of power is valid, a payee can corroborate the autographs of the former possessors. Still, one of the major problems with electronic coins is the possibility of double-spending, where a proprietor could spend the same coin multiple times, which is hard to describe. A common result to this problem is to calculate on a trusted central authority, also known as a mint, to check every sale for double spending. still, this approach has the strike of counting on a central authority to manage the entire plutocrat system, just like a bank [9].

To address this issue without the need for a central authority, we need a system that allows the payee to confirm the absence of any earlier transactions by the coin's previous owners. To achieve this, all transactions must be publicly announced, and participants must agree on a single history of the order in which they were received. To ensure that a transaction was the first received, the payee needs proof that the majority of nodes agreed at the time of the transaction that it was indeed the first.

Therefore, to eliminate the need for a central authority and enable a trustless system, we need a mechanism that allows transactions to be publicly announced and agreed upon by the network participants. This would enable payees to confirm the validity of the chain of ownership and the absence of any earlier transactions without relying on a central authority. By eliminating the need for a central authority, we can create a decentralized system that empowers users to manage their electronic currency with greater security and independence[10].

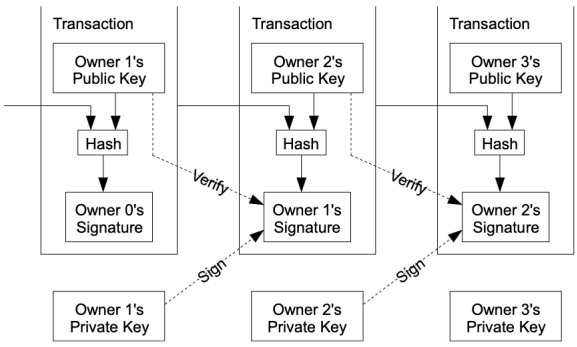

Figure 1.4: Transaction System

1.4 Useability issues related to BlockChain

"The emergence of blockchain technology has been seen as a revolutionary development that has the potential to disrupt several industries, including financial domains. However, the technology has been subject to criticism for its complexity, which has been cited as a barrier to its widespread adoption. One of the most successful applications of blockchain is cryptocurrency, and as such, identifying potential obstacles and usability issues that may hinder its adoption is crucial. To this end, a study was conducted to investigate common usability issues with desktop and mobile-based wallets used to manage cryptocurrencies. The study aimed to identify potential obstacles and usability issues that may hinder the widespread adoption of blockchain wallets. The study applied the analytical cognitive walk-through usability inspection method along with a set of guidelines with four fundamental tasks for Bitcoin".

The four fundamental tasks identified in the study include:

1. Starting a wallet on a device and checking one's balance.
2. Making a transaction of some Ether amount to a valid receiving address.
3. Having a permanent proof of record that a transaction has occurred.
4. Having a backup of an account in case of failure.

The study investigated three existing wallet applications: Exodus wallet, Bitcoin core wallet, and Ethereum MetaMask wallet. The results of the study reveal that both desktop-based and smartphone-based wallets lack good usability in performing even the fundamental tasks.

The study found that around 20 percent of fundamental task completion problems exist in the case of Exodus and Ethereum wallets, and up to 40 percent in the case of the Bitcoin core wallet. The study highlights the importance of addressing these usability issues to improve the

user experience and adoption of blockchain wallets.

Based on the findings of the study, a user-friendly Ethereum management web-based app is being designed using NextJS, Solidity for smart contract creation, TailwindCSS for UI, and SQL for data backup. The aim is to create a wallet application that performs better than the existing wallet applications and addresses the usability issues identified in the study.

The design of the new wallet application will incorporate user-friendly features and intuitive navigation to make it easy to use for both novice and experienced users. Additionally, the app will provide a seamless experience for performing the fundamental tasks identified in the study.

The use of Solidity for smart contract creation will enable the app to provide a secure and transparent platform for managing Ethereum-based transactions. This will ensure that users have a permanent proof of record for every transaction they make using the app.

The use of TailwindCSS for UI design will enable the app to have a modern and attractive design that is both aesthetically pleasing and easy to navigate. The app's UI will also be responsive, ensuring that it works seamlessly on both desktop and mobile devices.

In conclusion, the study highlights the importance of addressing the usability issues that exist in existing blockchain wallets. The design of a new user-friendly Ethereum management web-based app using NextJS, Solidity, TailwindCSS, and SQL aims to provide a seamless experience for users and address the usability issues identified in the study. The new app has the potential to improve the user experience and adoption of blockchain wallets, thereby contributing to the widespread adoption of blockchain technology.

CHAPTER 2

LITERATURE SURVEY

The author Monika di Angelo; Gernot Salzer states that The paper addresses an important issue of smart-contract wallets in blockchain technology. Paper presents a comprehensive analysis of contracts of wallet deployed on Ethereum, which is one of the most popular platform for smart contracts and tokens. The paper provides a detailed explanation of the six types of wallet contracts and their characteristics. The paper presents a reliable approach to identifying contracts of wallet by analyzing execution traces, bytecode and source code. The paper provides useful insights into usage scenarios and patterns of wallet contracts. The paper's analysis is limited to Ethereum blockchain and may not be applicable to other blockchain platforms. The paper does not provide any new solutions to address potential security issues with wallet contracts. The paper does not discuss the ethical implications of the use of wallet contracts, such as the potential for fraud or misuse. The paper's focus on technical aspects may make it difficult for non-technical readers to understand the content.[11]

The author Rui Liu; Tien Tuan Anh Dinh; Meihui Zhang; Ji Wang; Beng Chin Ooi; Gang Chen proposes a comprehensive survey of state of the art in private blockchain mechanism, which can help readers gain a better understanding of core technologies their capabilities. The BLOCKBENCH benchmarking framework introduced in the paper can be a useful tool for evaluation of performance of private blockchains against data processing workloads. The evaluation of three major blockchain systems (Parity, Hyperledger Fabric, and Ethereum) using the BLOCKBENCH framework provides insights into the design trade-offs and performance gaps between blockchain and database systems. The paper discusses research directions for bringing blockchain performance closer to the realm of databases, which can help enhance the efficiency and scalability of private blockchain systems. Paper focuses only on private blockchains, which may not provide a complete picture of the entire blockchain landscape. The performance evaluation conducted in the paper may not reflect the real-world performance of blockchain systems in all scenarios, as the performance of blockchain systems can vary depending on the specific use case and network conditions. The paper does not address the

environmental impact of blockchain technology, which is a growing concern as the energy consumption of blockchain systems is significant. .[12]

The author S. Eskandari et al. "first evaluated the usability and security issues in bitcoin key management and summarised the bitcoin key management approaches analysing 6 representative bitcoin clients and found that users performing tasks involving key management can be stuck with complex security issues. They also applied a cognitive walk-through inspection method along with a set of guidelines with four fundamental tasks for bitcoin but didn't showed any stats or numerical representation regarding the usability issues in bitcoin wallets".[13]

The author Kazerani et al. performed a study using Coinbase and Changetip to determine the extent to which usability and user experience were factors for bitcoin utilizing Changetip and Coinbase. Participants in their research had never used bitcoin before, and they were asked to remark as they worked through a given assignment. They discovered that almost half of those who took part had difficulty comprehending the ideas and were perplexed by their behaviour. They used a cognitive step-through method of inspection along with a set of guidelines with four essential tasks for bitcoin, but they did not provide any numerical or statistics representation of the usability problems with bitcoin wallets[14]

The author Krombholz et al. presented the first large scale survey to investigate how users experience Bitcoin ecosystem in terms of anonymity, privacy and security. They discovered that most of the users did not make full use of the security features of the Bitcoin management application that they chose and had serious misconceptions about how to safeguard their privacy and remain anonymous on bitcoin network. Additionally, they discovered that 22% participants had lost money as a result of self-inflicted mistake or security flaws.[15]

The author Xin, Praitheeshan, P., L., Y.W., Pan, R., Doss proposes the paper addresses an important issue of security vulnerability in the Ethereum wallets. The systematic analysis conducted in the paper provides valuable insights into the existing literature on hacking methods in Ethereum wallets. The experiments conducted by the authors add empirical evidence to the paper's findings. The paper highlights the importance of using complex password credentials to secure keystore files. The paper's scope is limited to only one aspect of Ethereum wallet security, i.e., the vulnerability of keystore files. The paper does not provide any new solutions to address the security vulnerability of keystore files in Ethereum wallets. The paper's findings are not generalizable to other types of cryptocurrency wallets. The paper does not discuss the

potential ethical implications of its findings, such as the responsibility of wallet providers to ensure their users' security.[16]

The author Nilesh P. Sable; Vijay U. Rathod; Rachna Sable; Gitanjali Rahul Shinde proposes "a payment system that is based on permission and privacy laid by blocks-to-blocks for use in the financial sector, which could potentially lead to more secure transactions. The proposed architecture integrates digital wallets with various banks to give a strong foundation of blockchain for secure transactions. The peer-to-peer network that shares transaction and distributes the load can help minimize the load on central banking systems and keep overall data centers secure." The paper recognizes the importance of addressing security concerns in online payment systems, which is a critical issue in the digital age. The paper does not provide details on how the proposed payment system will be implemented and the potential challenges that might arise. The paper does not discuss the potential cost of implementing the proposed payment system, which could be a significant barrier for smaller financial institutions. The paper does not address the potential impact on customer experience and usability, which is an important factor in the adoption of any new payment system. The paper does not provide evidence or research to support the claims made about the proposed payment system[17]

The author Saurabh Suratkar; Mahesh Shirole; Sunil Bhirud states that The paper provides a detailed overview of different multi-currency wallets and their features, which can be helpful for people who are new to cryptocurrency. The paper covers important aspects of wallets such as cost, supported currencies, platform support, anonymity, wallet recovery methods, key management and fiat currencies supported, which can help readers make informed decisions when choosing a wallet. The paper acknowledges the blockchain's increasing penetration in many industries, which highlights the relevance and importance of understanding wallets. The paper does not provide any new or groundbreaking insights, as the information presented is readily available online. The paper does not provide any analysis or comparison of different wallets, which may not be helpful for readers looking for a detailed comparison between different wallets. The paper does not provide any recommendations or suggestions on which wallets are best suited for specific use cases or preferences.[18]

The author Mihai, Razvan and Ozkul, Omer Faruk and Datta, Gora and Goga, Nicolae

and Grybniak, Sergii and Marian proposes a blockchain-based prototype that can address fundamental financial, economic, and accounting challenges. The prototype showcases an innovative solution for recording and tracking recurring economic transactions more effectively, efficiently, and in quasi-real-time. The paper utilizes the Ethereum blockchain, which is a widely used and evolved smart contract platform that offers various functionalities and capabilities. The asset rental contract is used as an example to show how economic transactions can be recorded and tracked on the blockchain, and how the prototype can be extended to a range of recurring transactions. The research paper focuses only on the asset rental contract and does not explore other types of recurring transactions. Therefore, the scope of the paper is limited. The paper includes technical jargon that may not be easily understandable by readers who are not familiar with blockchain technology.The paper does not discuss the risks associated with blockchain technology, such as cybersecurity threats, regulatory challenges, and scalability issues. [19]

On continuing research paper conducted by the author Saurabh Suratkar; Mahesh Shirole; Sunil Bhirud we have created an application cryptotrend. One advantage of this project over the research paper is that it offers a practical solution for managing Ethereum transactions and assets, whereas the research paper provides only an overview of different multi-currency wallets without providing any analysis or recommendations on which wallets are best suited for specific use cases or preferences. Additionally, the Ethereum management dashboard project offers a user-friendly interface that simplifies the process of monitoring and organizing Ethereum transactions and assets, making it easier for users to manage their holdings. Overall, the project appears to be a useful tool for anyone looking to manage their Ethereum transactions and assets efficiently.

CHAPTER 3

EXISTING PROBLEM AND PROPOSED SOLUTION

3.1 Problem Statement

Based on previous research paper we can show that blockchain useability issues specifically lies in:

Lack of user-friendly interfaces: Many blockchain-based applications have interfaces that are difficult to use and understand, which can create usability issues for non-technical users.

Technical knowledge requirements: Using blockchain-based applications often requires significant technical knowledge, which can create a barrier to entry for many users.

Complexity of smart contracts: The smart contracts are self-executing contracts with the terms of the agreement between seller and buyer being directly written into lines of code, can be complex and difficult to understand for non-technical users.

Difficulties with private key management: Private key management is an essential aspect of using blockchain-based applications, but it can be difficult for non-technical users to manage and keep secure.

Lack of standardization: The lack of standardization in blockchain can create usability challenges, as users may need to interact with different blockchains or blockchain-based applications that have different interfaces and require different technical knowledge.

3.2 Proposed Solution

We are providing solution to this by creating an Ethereum management dashboard, which is designed to provide users with a streamlined and efficient way to manage their Ethereum transactions and assets. The dashboard offers a range of user-friendly features that simplify the process of transferring ether to other clients, as well as providing users with an easy-to-use interface for keeping track of their transaction history and current asset balances.

One of the main features of the Ethereum management dashboard is the ability to easily transfer ether to other clients, complete with a message. This feature allows users to quickly and easily send ether to other people, while also providing them with a record of their transactions. By offering users a simple and intuitive way to manage their transactions, the dashboard aims to make Ethereum transactions more accessible and user friendly.

In addition to the transfer feature, the dashboard also displays the user's current ether balance, providing an overview of their assets. This allows users to keep track of their assets in real-time, helping them to make informed decisions about their portfolio. Furthermore, the transaction history feature allows users to view all of their past transactions, providing a complete record of their Ethereum transactions. This gives users a comprehensive overview of their transaction history, which can be useful for tax or auditing purposes.

The dashboard also includes a QR code functionality, which allows users to easily share their Ethereum address with others. This makes it simple for other people to send ether to the user's account, without the need for manual input of the wallet address. This feature not only saves time but also reduces the potential for errors when transferring assets between users.

Another unique feature of the Ethereum management dashboard is its prediction column, which predicts the price of ether and whether it is likely to rise or fall. This feature is based on historical data and AI models, providing users with valuable insights into the market trends of Ethereum. By providing users with accurate and reliable predictions, the dashboard can assist users in making informed decisions about their ether holdings and adjusting their portfolios accordingly.

Overall, the Ethereum management dashboard is a powerful tool that simplifies the process of managing Ethereum transactions and assets. By providing users with an intuitive interface, real-time asset tracking, and advanced prediction tools, the dashboard aims to make Ethereum more accessible and user-friendly. Whether you are an experienced cryptocurrency trader or a newcomer to the world of blockchain, the Ethereum management dashboard offers a range of features that can help you to achieve your investment goals and manage your assets more efficiently.

CHAPTER 4

METHODOLOGY

Once the smart contract is created, we will develop a web application using the NextJS, a React-based framework, and implement the UI using tailwindcss. The webpage will have a front page describing the project, a login button that will connect to the Metamask, a dashboard page, and transaction history page.

After authentication, user will get redirected to the dashboard page, where they can see their ether holdings and other information, such as balance, transaction history, and an ether prediction column. The dashboard page will also have a QR code mechanism that will enable users to share their wallet address in hexadecimal format with others quickly. It will also include an option to transfer ether, which will open the camera through which users can scan or paste the recipient's QR code to send the money.

When the user clicks on send ether, the smart contract function will get triggered, enabling the transfer of ether and holding the information in the blockchain.

The backend will help connect with the smart contract using the hardhat package. After creating a smart contract, it needs to be compiled and deployed to a network to be usable. Hardhat is a popular tool that developers use to compile and deploy smart contracts. During deployment process, a certain amount of cryptocurrency or tokens must be transferred to the network to cover the transaction fees. "Once the smart contract is deployed to the network, it responds with a bytecode and Application Binary Interface (ABI). Every smart contract provides an ABI and a contract address deployed on the network. The contract address helps to identify the smart contract on the network, and we can use the ABI to execute the functions related to the smart contract".

React, popular frontend JavaScript library, can interact with the smart contract by communicating with the ABI. To do this, developers must first import the ABI into their React project. This allows the React app to access the smart contract's functions and variables. Once the ABI has been imported, the next step is to connect the React app to a Web3 provider. Web3.js is a JavaScript library that allows you to interact with the Ethereum blockchain. Developers can use a library like Web3.js to connect their React app to a Web3 provider such as Metamask or

Infura. Once the React app is connected to a Web3 provider, it interacts with the smart contract by calling the appropriate functions from the ABI. For example, if the smart contract has a function for transferring tokens, the React app can call that function using the ABI.

To call a function from the ABI, the developer must first create an instance of the contract using the web3.eth.Contract() method. This creates an object that represents the smart contract and its functions. The developer can then call the appropriate function using the object's methods. When a function is called from the smart contract, it typically returns a transaction hash. This hash can be used to track the status of the transaction and determine whether it was successful or not. If the transaction was successful, the state of the smart contract will be updated accordingly. When a function is called from the smart contract, it typically returns a transaction hash. This hash can be used to track the status of the transaction and determine whether it was successful or not. If the transaction was successful, the state of the smart contract will be updated accordingly. As soon as transaction gets successful it will be shown on the dashboard page. The transaction will also gets reflected on the transaction history page.

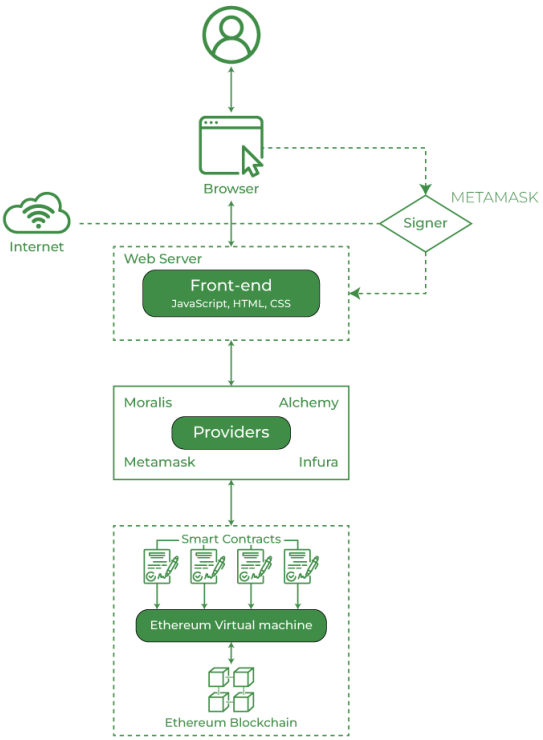

Figure 4.1: Smart Contract with FrontEnd

The primary objective of this project is to make blockchain transactions more user-friendly and accessible so that more users can use it with ease. By creating an intuitive dashboard that simplifies the process of transferring ether, viewing transaction history, and predicting ether price, users can keep track of their assets and make informed decisions about their ether holdings. Additionally, the project aims to eliminate the need for a trusted central authority or mint, allowing for more decentralized and democratic control over the money system. With this project, we aim to contribute to the growth and development of the blockchain ecosystem while ensuring that it remains accessible and user-friendly for all.

CHAPTER 5

IMPLEMENTATION AND RESULT

5.1 Implementation

The aim of our project is to simplify the process of managing blockchain transactions and assets through the creation of a user-friendly and efficient Ethereum management dashboard. To achieve this, we are first creating a smart contract, which will act as the backbone of the project. The smart contract will help connect with the blockchain and provide control over all transaction features. We will create middleware to check if the user has sufficient balance to transfer ether to another address. If this condition is satisfied, the transaction will proceed.
The constructor function will also check for the middleware condition. We have created a function that accepts three parameters: the amount to be transferred, the receiver's wallet address, and an attached message.
This function will make changes to the blockchain, requiring gas fees that will be transacted from the sender's wallet. We will then create a mapping from a struct. The struct datatype will consist of the name of type string, amount of type uint256, and a message of string type.
This mapping will help identify which address the struct belongs to. After the transaction takes place, the map object will be updated. The smart contract function will get triggered, enabling the transfer of ether and holding the information in the blockchain.

This smart contract has been designed to facilitate the transfer of Ether between accounts while also keeping track of transaction history. To achieve this, a struct named Transaction has been created to store details about each transaction, such as sender's address, receiver's address, amount transferred, and an optional message. All transactions are recorded using a mapping called transactions.
The constructor function initializes the transactionCount variable to zero. The transferEther function is responsible for transferring Ether between accounts. It requires three parameters, namely receiver's address (_to),amount of Ether to be transferred (_amount), and optional message (_message).

Two require statements have been added to ensure that the specified (_amount) is equal to the msg.value and that the smart contract has sufficient balance to complete the transfer. If these conditions are not met, the transaction will be reverted.

Assuming that the conditions have been met, the transfer function is used to transfer the specified (_amount) of Ether to the receiver's address (_to). A new Transaction struct is created with receiver's address, sender's address, transferred amount, and optional message, which is then stored in the transactions mapping. The transactionCount is then incremented.

The getTransactionCount function returns the total number of transactions that have been made through the smart contract, while the getTransaction function takes an index as input and returns the details of the transaction at that index.

Then this smart contract needs to be compiled down. On compiling smart contract it returns ABI and byte code which is again use further via integrating it with the frontend.

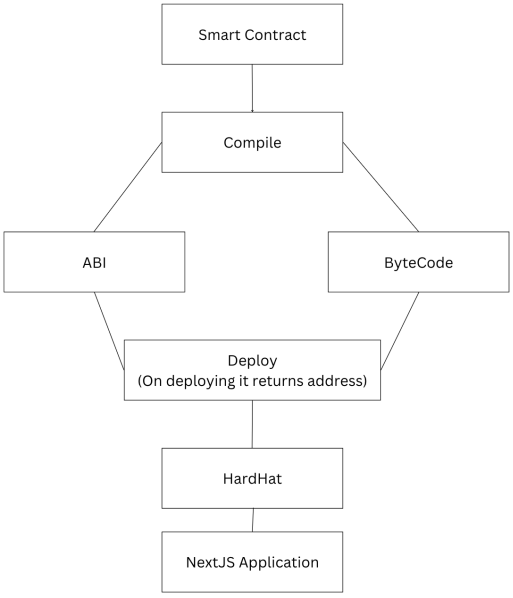

Figure 5.1: Transaction System

5.2 Result

On the front page, you'll find information about the project, along with four buttons. These buttons allow you to download the project report in PDF or ZIP format, as well as the research paper. Additionally, there's a button that enables you to connect the website with your wallet, specifically Metamask.

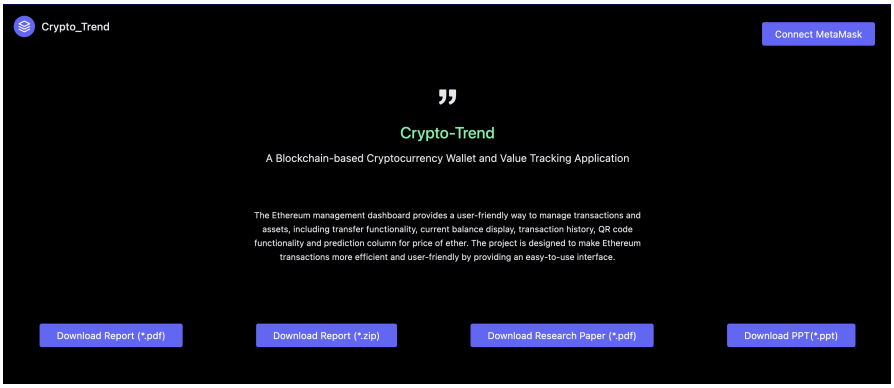

Figure 5.2: Front Page

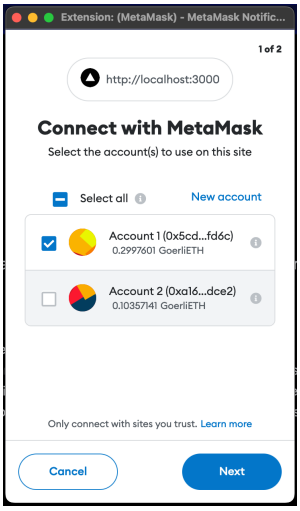

Figure 5.3: Metamask Connect

The pop-up window enables user to connect to Metamask, which is an authentication setup required for website connectivity. Once the user clicks on the "Next" button, Metamask verifies connection to the website. From there, user can specify the Metamask account they wish to use for website connectivity.

This pop-up is responsible for conducting an account integrity check.

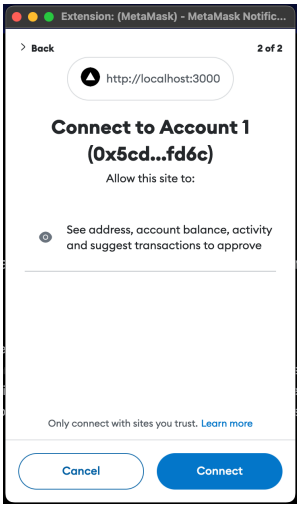

Figure 5.4: Account integrity check

Once the authentication process is completed, the user is redirected to the dashboard. On the dashboard, the user can view their ether holdings, transactions, and converted ether prices. Additionally, a prediction graph is also displayed.

With the scanning-based transfer functionality, users can easily send ether to another user's address without the need for manual input. Once the user scans the recipient's address, the form is automatically populated with the necessary information. The user simply needs to enter the desired amount of ether to be transferred and confirm the transaction. This eliminates the potential for errors that may occur when manually inputting the recipient's address. The scanning-based transfer functionality is a convenient and efficient feature that simplifies the process of sending ether to other users.

The scanning process is an essential feature for transferring ether directly to another user's address with ease. Once the recipient's address is scanned, the form is automatically populated, and the user only needs to input the transaction amount to complete the transfer. This functionality significantly reduces the risk of errors that could arise from manual input. It streamlines the transfer process, providing a smooth and efficient experience for the user. By enabling users to send ether to other users' addresses with minimal effort, this feature enhances the accessibility and user-friendliness of the transfer process.

After the user inputs the desired amount of ether to be transferred, they can click the send button, which triggers a confirmation page to appear. This page provides a summary of the transaction details, such as the recipient's address, transaction amount, and associated fees.

Figure 5.5: User Dashboard

Once the user confirms the details and clicks on the confirmation popup, the ether is transferred from one user to the other. The confirmation page acts as a safety net, ensuring that the user has a chance to review and verify the transaction details before proceeding with the transfer. This feature enhances the security and accuracy of the transfer process.

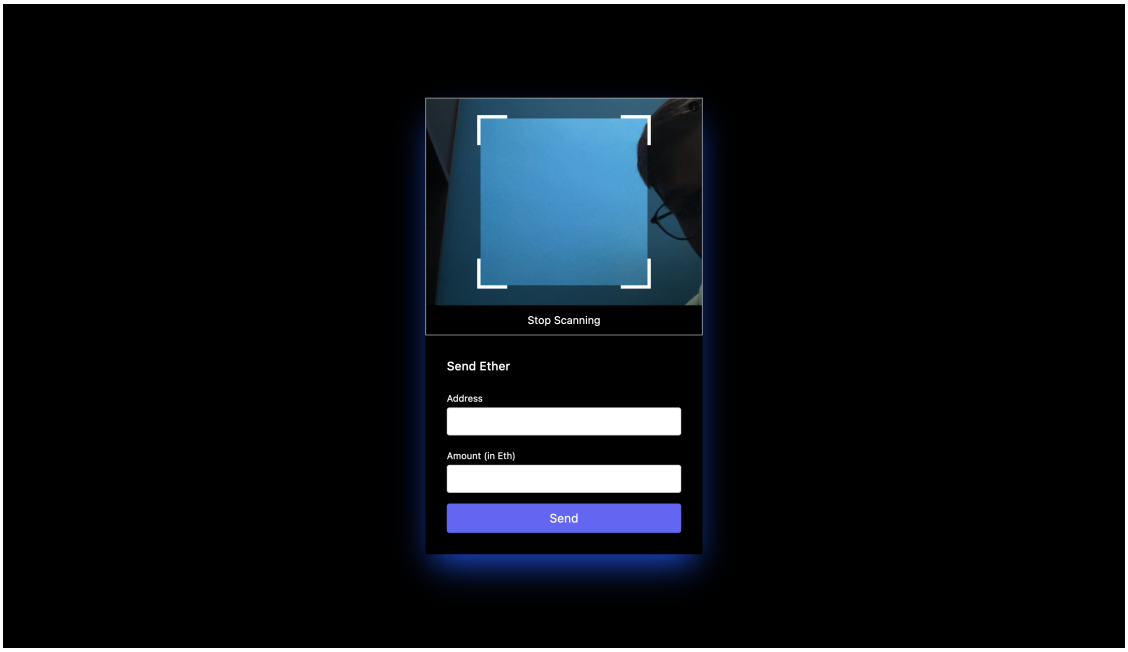

Figure 5.6: QR Scanner

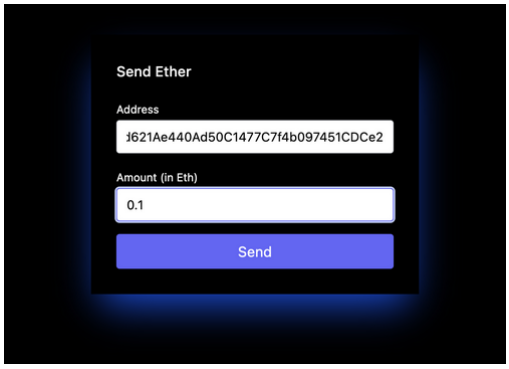

Figure 5.7: Input Form

Once the transaction has been successfully completed, it is automatically reflected on the transaction side. This means that the user can view the details of the completed transaction, including transaction amount, fees, and timestamp. This information is stored securely and can be accessed by the user at any time for reference. The ability to view the transaction history provides transparency and accountability for all transactions made on the platform. It also enables the user to track the movement of their ether and monitor their transaction history, ensuring that they have complete visibility over their assets.

In addition to the transaction side, any updates or changes to the transaction are also automatically reflected on the Metamask wallet. This means that the user can view their updated transaction details, including the transaction amount, fees, and status, directly from their

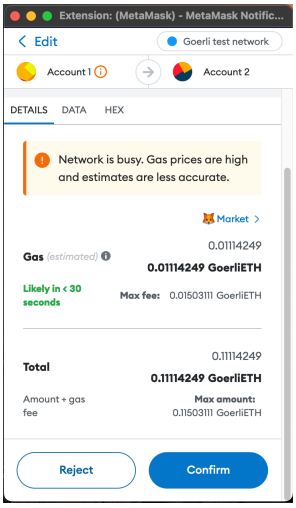

Figure 5.8: Validate Transaction

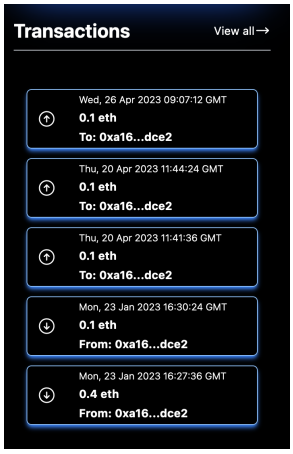

Figure 5.9: Latest Transaction

Metamask wallet. The ability to view these details in real-time provides the user with transparency and confidence in the transaction process, ensuring that they are fully informed about any changes to their transactions. With the ability to view transaction details from multiple sources, the user has a complete and accurate overview of their transaction history.

This is a unique QR code that is specific to each user. The user can copy their QR code and share it with anyone they wish to receive ether from. The QR code serves as a quick and convenient way for users to receive ether without the need for manual input. The user can simply share their QR code, and the sender can scan it to initiate the transaction. This feature enhances the accessibility and user-friendliness of the transfer process, providing a seamless experience for both the sender and the recipient. With the user's QR code, receiving ether has never been easier.

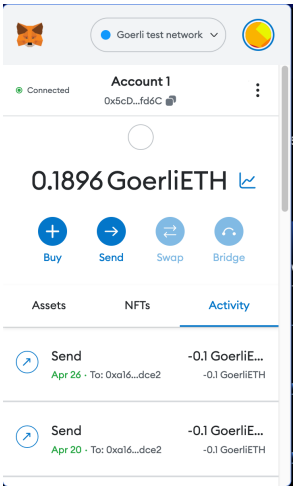

Figure 5.10: Transaction Update

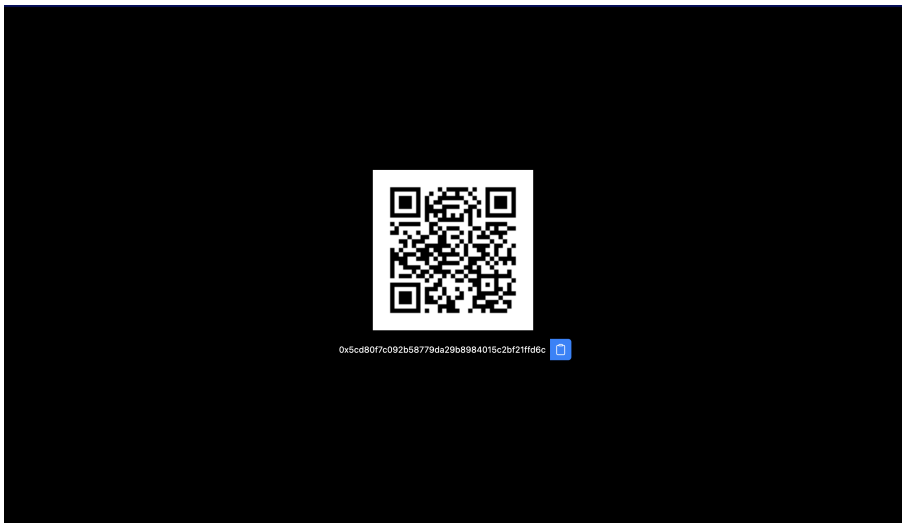

Figure 5.11: Wallet Address

Apart from this we conducted a survey with 100 participants. We compare the cryptotrend project with other wallets like exodus wallet, bitcoin core and metamask. In the result we found out that cryptotrend wallet is much more easier to use than other wallet and basic functionalities of an application like:

1. Ease of login
2. Making a transaction of a given amount to other users
3. Starting a new wallet for the first time in a new account and checking its balance.
4. Providing complete insights about ether holding on the dashboard .

Below are the results for the conducted survey

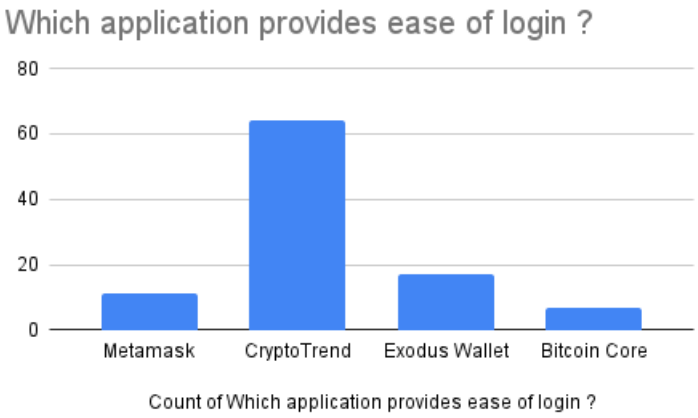

Figure 5.12: Ease of login

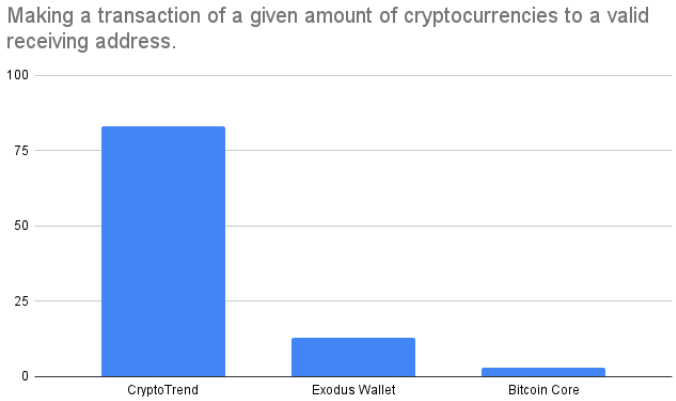

Figure 5.13: Transfer

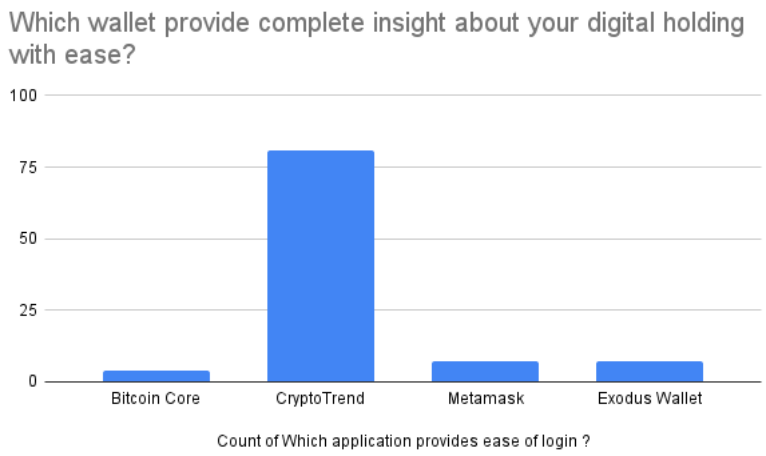

Figure 5.14: Digital Holding

The above graph shows that in every case more than 70 percent of the users find cryptotrend wallet more easier to use and is more friendly than any other wallet. Blockchain technology has been growing rapidly in recent years, with many industries explor- ing its potential applications. However, one of the main challenges in the widespread adoption of this technology is its usability. Fortunately, there are now user-friendly applications that simplify the complex nature of blockchain and help individuals perform basic tasks such as logging in, creating new wallets, checking account balances, and making transactions. Among these applications, CryptoTrend stands out as a promising solution for improving the usability of blockchain technology. It was found that CryptoTrend is much easier to use compared to other crypto wallets. This user-friendliness is due to its intuitive design and simplified features, which make it accessible to both novice and experienced users. With CryptoTrend, users can easily manage their digital assets and perform transactions with just a few clicks.

Additionally, CryptoTrend provides insightful predictions about users' Ethereum holdings through its AI-powered prediction model. This feature utilizes historical data and machine learning al- gorithms to forecast the future price of Ethereum, helping users make informed decisions about their investments and optimize their portfolio. The management dashboard also presents users with their current Ethereum balance, transaction history, and a QR code feature for easy sharing of Ethereum addresses. With its combination of user-friendliness, security, and insightful prediction features. The need for user-friendly blockchain applications is crucial in driving the adoption of this technology. As more industries and businesses explore the potential applications of blockchain, it is important that they have access to user-friendly tools

that simplify the complex nature of this technology. With its user-friendly design, enhanced security features, and simplified features, CryptoTrend is a promising solution for improving the usability of blockchain technology and driving its widespread adoption.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

Blockchain technology has the potential to revolutionize various industries, but its adoption has been hindered by its complexity and usability issues. However, the development of user-friendly blockchain applications like CryptoTrend can help overcome these issues and promote wider adoption.

CryptoTrend offers enhanced security, prediction models for cryptocurrencies, and a user-friendly interface that simplifies tasks like creating a wallet, checking balances, and making transactions. These features make managing cryptocurrencies easier and reduce the risk of losses.

The development of user-friendly blockchain applications like CryptoTrend is a positive step towards wider adoption of blockchain technology. As more people become familiar with blockchain and its potential, it is likely to become more widely adopted. This will lead to greater innovation and opportunities in different industries.

In conclusion, blockchain technology has the potential to revolutionize various industries, but its adoption has been hindered by its complexity and usability issues. The development of user-friendly blockchain applications like CryptoTrend is changing this by making blockchain technology more accessible to the general public. With enhanced security features and prediction models for cryptocurrencies, CryptoTrend is making it easier for users to manage their cryptocurrencies.

As a result, blockchain technology is evolving to become more user-friendly and accessible, which is likely to lead to greater adoption in the future and greater innovation and opportunities in various industries.

6.2 Future Scope

CryptoTrend, a user-friendly blockchain application, has plans for future work to enhance its features and user experience.

Firstly, it aims to integrate more cryptocurrencies, expanding users' options for managing their digital assets.

Secondly, the user interface will be improved to make it more intuitive for new users.

Moreover, CryptoTrend plans to refine its prediction models to provide users with more accurate forecasts of cryptocurrency prices. This will enable users to make better-informed investment decisions, reducing the risk of losses.

To ensure the security of users' digital assets, advanced security measures such as biometric authentication, two-factor authentication (2FA), and decentralized storage will be incorporated. These security measures will provide users with greater peace of mind and protection against potential security breaches.

Overall, CryptoTrend's future work is focused on improving user experience, enhancing the accuracy of prediction models, and implementing advanced security measures. By doing so, CryptoTrend aims to maintain its position as a leading blockchain application that provides users with a secure and user friendly platform for managing their digital assets.

REFERENCES

[1] Nakamoto, S. (2009). "Bitcoin: A peer-to-peer electronic cash system." *Cryptography Mailing list at https://metzdowd.com*.

[2] Shi, N. (2016). "A new proof-of-work mechanism for bitcoin." *Financial Innovation*, 2.

[3] Acar, Y., Backes, M., Fahl, S., Garfinkel, S., Kim, D., Mazurek, M. L., and Stransky, C. (2017). "Comparing the usability of cryptographic apis." *2017 IEEE Symposium on Security and Privacy (SP)*, IEEE. 154–171.

[4] Numen (2023). "What is a smart contract audit?

[5] Welligton dos Santos Abreu, A., Coutinho, E. F., and Ilane Moreira Bezerra, C. (2022). "Performance evaluation of data transactions in blockchain." *IEEE Latin America Transactions*, 20(3), 409–416.

[6] Blog, H. "A deep dive into the blockchain architecture - helios blog.

[7] Wang, X. (2019). "Research on ecdsa-based signature algorithm in blockchain." *Finance and Market*, 4, 55.

[8] Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., and Bani-Hani, A. (2021). "Blockchain smart contracts: Applications, challenges, and future trends." *Peer-to-Peer Networking and Applications*, 14(5), 2901–2925.

[9] "How bitcoin transactions work | how do bitcoin and crypto work? | get started with bitcoin.com. (n.d).

[10] Patel, R., Sethia, A., and Patil, S. (2018). "Blockchain – future of decentralized systems." *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, 369–374.

[11] di Angelo, M. and Salzer, G. (2020). "Characteristics of wallet contracts on ethereum." *2020 2nd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*. 232–239.

[12] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., and Wang, J. (2018). "Untangling blockchain: A data processing view of blockchain systems." *IEEE Transactions on Knowledge and Data Engineering*, 30(7), 1366–1385.

[13] Eskandari, S., Barrera, D., Stobert, E., and Clark, J. (2015). "A first look at the usability of bitcoin key management.

[14] Kazerani, A., Rosati, D., and Lesser, B. (2017). "Determining the usability of bitcoin for beginners using change tip and coinbase." *Proceedings of the 35th ACM International Conference on the Design of Communication*.

[15] Krombholz, K., Judmayer, A., Gusenbauer, M., and Weippl, E. R. (2016). "The other side of the coin: User experiences with bitcoin security and privacy." *Financial Cryptography*.

[16] Praitheeshan, P., Xin, Y. W., Pan, L., and Doss, R. R. M. (2019). "Attainable hacks on keystore files in ethereum wallets–a systematic analysis.

[17] Singh, K., Singh, N., and Singh Kushwaha, D. (2018). "An interoperable and secure e-wallet architecture based on digital ledger technology using blockchain." *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*. 165–169.

[18] Suratkar, S., Shirole, M., and Bhirud, S. G. (2020). "Cryptocurrency wallet: A review." *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, 1–7.

[19] Mihai, R., Ozkul, O. F., Datta, G., Goga, N., Grybniak, S., and Marian, C. V. (2022). "Blockchain-enabled economic transactions: Recurring financial accruals and payments." *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain Beyond (iGET-blockchain)*. 1–5.

report

ORIGINALITY REPORT

7%	6%	4%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	link.springer.com Internet Source	1%
2	www.barcouncil.org.uk Internet Source	<1%
3	ijres.org Internet Source	<1%
4	www.scilit.net Internet Source	<1%
5	Stefano Bistarelli, Marco Mantilacci, Paolo Santancini, Francesco Santini. "An end-to-end voting-system based on bitcoin", Proceedings of the Symposium on Applied Computing - SAC '17, 2017 Publication	<1%
6	"Blockchain – ICBC 2018", Springer Science and Business Media LLC, 2018 Publication	<1%
7	www.igi-global.com Internet Source	<1%

8	Submitted to University of Sydney Student Paper	<1 %
9	www.researchgate.net Internet Source	<1 %
10	vocal.media Internet Source	<1 %
11	www.ijnrd.org Internet Source	<1 %
12	dokumen.pub Internet Source	<1 %
13	Submitted to University of Greenwich Student Paper	<1 %
14	Submitted to University of Stirling Student Paper	<1 %
15	Yaron Kanza, Eliyahu Safra. "Cryptotransport", Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems - SIGSPATIAL '18, 2018 Publication	<1 %
16	publisher.uthm.edu.my Internet Source	<1 %
17	scholar.sun.ac.za Internet Source	<1 %

18	tudr.thapar.edu:8080 Internet Source	<1 %
19	scholararchive.ohsu.edu Internet Source	<1 %
20	Abdullah Umar, Deepak Kumar, Tirthadip Ghose. "Blockchain-based decentralized energy intra-trading with battery storage flexibility in a community microgrid system", Applied Energy, 2022 Publication	<1 %
21	Dinh Tien Tuan Anh, Meihui Zhang, Beng Chin Ooi, Gang Chen. "Untangling Blockchain: A Data Processing View of Blockchain Systems", IEEE Transactions on Knowledge and Data Engineering, 2018 Publication	<1 %
22	Felix Hoffmann. "Challenges of Proof-of-Useful-Work (PoUW)", 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain), 2022 Publication	<1 %
23	bspace.buid.ac.ae Internet Source	<1 %
24	cybersec4europe.eu Internet Source	<1 %
25	dspace.lu.lv Internet Source	

		<1%
26	"Cyber Security and Computer Science", Springer Science and Business Media LLC, 2020 Publication	<1%
27	"Web Information Systems Engineering – WISE 2019", Springer Science and Business Media LLC, 2019 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Submission Summary

Conference Name
2nd International Conference on Communication, Security and Artificial Intelligence

Track Name
ICCSAI2023

Paper ID
202

Paper Title
CRYPTOTREND: A BLOCKCHAIN-BASED CRYPTOCURRENCY WALLET AND VALUE TRACKING APPLICATION

Abstract
The project is an Ethereum management dashboard that aims to give users an user-friendly and efficient way for managing Ethereum transactions and assets. Dashboard allows users to easily transfer ether to other clients along with a message. This feature allows users to keep track of their transactions and easily send ether to other people. The dashboard also displays the user's current ether balance, providing an overview of the user's assets. The transaction history feature allows users to view all of their past transactions, providing a complete record of their Ethereum transactions. The QR code functionality allows users to easily share their Ethereum address with others, making it easy to receive ether from other people. The dashboard also has a prediction column that predicts the price of ether whether it will rise or fall. This feature helps users to make informed decisions about their ether holdings. The prediction is based on historical data and AI models. The prediction column will assist the users in take an informed decision and making changes in their ether portfolio accordingly. The project is made to allow transactions of ethereum more efficient and user-friendly by providing an easy-to-use interface. The project's aim is to develop an efficient platform for managing Ethereum transactions and assets. The project aims in order to simplify the process of monitoring and organizing Ethereum transactions and assets for users.

Created on
13/5/2023, 11:17:32 am

Last Modified
13/5/2023, 11:17:32 am

Authors
Dr. Abhilasha Singh (SRMIST Delhi NCR Campus Modinagar) < abhilass1@srmist.edu.in>
Rishi Sharma (SRMIST Delhi NCR Campus Modinagar) < rs1965@srmist.edu.in>
Vaibhav Dhar (SRMIST Delhi NCR Campus Modinagar) < vd4974@srmist.edu.in>
Vaibhav Agarwal (SRMIST Delhi NCR Campus Modinagar) < va8613@srmist.edu.in>
Tushar Mukherjee (SRMIST Delhi NCR Campus Modinagar) < tm3707@srmist.edu.in>

Submission Files
Research_Paper.pdf (493.7 Kb, 13/5/2023, 11:16:05 am)