

# **KRYPTX : A WEB 3.0 DECENTRALISED BLOCKCHAIN APPLICATION FOR CRYPTO EXCHANGE USING SMART CONTRACTS**

Submitted in partial fulfillment of the requirements for the award of  
Bachelor of Engineering degree in Computer Science and Engineering

By

**KARAN MAHTO (Reg No- 40110548)**

**KESHAV KUMAR (Reg No- 40110585)**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
SCHOOL OF COMPUTING**

## **SATHYABAMA**

**INSTITUTE OF SCIENCE AND TECHNOLOGY  
(DEEMED TO BE UNIVERSITY)**

**Category – I University by UGC**

**Accredited with Grade “A++” by NAAC | Approved by AICTE**

**JEPPIAAR NAGAR, RAJIV GANDHI SALAI,**

**CHENNAI – 600119**

**APRIL 2024**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**BONAFIDE CERTIFICATE**

This is to certify that this Project Report is the bonafide work of **Karan Mahto (40110548)** and **Keshav Kumar (40110585)** who carried out the Project entitled **"KRYPTX : A WEB 3.0 DECENTRALISED BLOCKCHAIN APPLICATION FOR CRYPTO EXCHANGE USING SMART CONTRACTS"** under my supervision from November 2023 to April 2024

  
Internal Guide  
Ms. V. Gowri Manohari, M.E.

  
Head of the Department

Dr. L. LAKSHMANAN, M.E., Ph.D.

HEAD OF THE DEPARTMENT  
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
**SATHYABAMA**  
INSTITUTE OF SCIENCE AND TECHNOLOGY  
(DEEMED TO BE UNIVERSITY)  
Jeyapathi Nagar, Rajiv Gandhi Salai,  
Chennai - 600 119.

Submitted for Viva voce Examination held on 12/04/2024

  
Internal Examiner

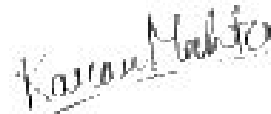
  
External Examiner

## DECLARATION

I, Karan Mahto (40110548) hereby declare that the Project Report entitled "KRYPTX  
A WEB 3.0 DECENTRALISED BLOCKCHAIN APPLICATION FOR CRYPTO  
EXCHANGE USING SMART CONTRACTS" done by me, under the guidance of  
Ms.V.Gowri Manohari, M.E., is submitted in partial fulfillment of the requirements for  
the award of Bachelor of Engineering Degree in Computer Science and Engineering

DATE: 13/04/2024

PLACE: Chennai



SIGNATURE OF THE CANDIDATE

## ACKNOWLEDGEMENT

We are pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

We convey my thanks to **Dr. T. Sasikala M.E., PhD, Dean**, School of Computing, **Dr. L. Lakshmanan M.E., PhD**, Head of the Department of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

We would like to express my sincere and deep sense of gratitude to my Project Guide **Ms. V.Gowri Manohari, M.E.**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of our project work.

We wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project

## **ABSTRACT**

This project aims to develop a decentralized crypto exchange platform using Web 3.0 technologies and smart contracts. The proposed platform leverages blockchain technology to create a transparent and secure environment for crypto trading. Smart contracts are utilized to automate trade executions, ensuring the integrity and immutability of transactions. The project focuses on designing a user-friendly interface allowing individuals to trade various cryptocurrencies directly without intermediaries. Additionally, the platform incorporates advanced security measures to protect user funds and prevent unauthorized access. The blockchain technology holds principal assurance for a difference of enterprises, including financial services, cryptocurrency exchange, laundering of anti-money tracking systems, unique identity security, healthcare, real estate, supply chain, and logistics monitoring. Results showed that blockchain is a considerably new technology and the nodes share their data in the network without trust in other nodes. Furthermore, key aspects of using this technology, the users in the crypto world buy, sell, or exchange the crypto-coins in the blockchain network. Many of the protocols are there to exchange cryptocurrencies. The main contributions of this work lie based on the protocol named uniswap protocol, which helps the users to exchange the crypto-coins. Uniswap protocol is defined to be the automated liquidity protocol provision on the blockchain Ethereum platform. With the uniswap, a user can buy or sell the ERC20 tokens in the decentralized distributed network by using an Ethereum smart contract. This paper will help the users in the blockchain network to use uniswap protocol as a trustworthy and efficient way of exchanging the crypto-coins or the tokens in the blockchain network.

## TABLE OF CONTENT

| CHAPTER<br>NO | TITLE                               | PAGE<br>NO |
|---------------|-------------------------------------|------------|
|               | ABSTRACT                            | v          |
|               | LIST OF FIGURES                     | viii       |
|               | LIST OF TABLES                      | ix         |
| 1             | INTRODUCTION                        | 1          |
|               | 1.1 Project Introduction            | 1          |
| 2             | LITERATURE SURVEY                   | 3          |
|               | 2.1 Inferences                      | 3          |
|               | 2.2 Related Works                   | 4          |
| 3             | REQUIREMENT ANALYSIS                | 6          |
|               | 3.1 Algorithm                       | 6          |
|               | 3.2 Modules Requirement             | 7          |
| 4             | PROPOSED SYSTEM                     | 10         |
|               | 4.1 Aim                             | 10         |
|               | 4.2 Description of Proposed System  | 10         |
|               | 4.3 Architecture of Proposed System | 11         |
| 5             | IMPLEMENTATION OF PROPOSED SYSTEM   | 12         |
|               | 5.1 Proposed Plan of Implementation | 12         |
|               | 5.2 Blockchain Integration          | 12         |
|               | 5.3 UML Diagrams                    | 15         |
|               | 5.4 Working Process                 | 18         |
| 6             | RESULT AND DISCUSSION               | 19         |
|               | 6.1 Result                          | 19         |
|               | 6.2 Future Scope                    | 20         |
| 7             | CONCLUSION                          | 22         |

|          |                             |           |
|----------|-----------------------------|-----------|
| <b>8</b> | <b>REFERENCES</b>           | <b>23</b> |
| <b>9</b> | <b>APPENDIX</b>             |           |
|          | <b>A. SOURCE CODE</b>       | <b>26</b> |
|          | <b>B. OUTPUT SCREENSHOT</b> | <b>32</b> |
|          | <b>C. RESEARCH PAPER</b>    | <b>37</b> |
|          | <b>D. CERTIFICATE</b>       | <b>42</b> |

## LIST OF FIGURES

| <b>Figures</b> | <b>Name of the figure</b>             | <b>Page no</b> |
|----------------|---------------------------------------|----------------|
| 3.1            | Steps of Consensus Protocol           | 7              |
| 4.1            | Architecture Diagram                  | 11             |
| 5.1            | Smart Contract Flow Diagram           | 14             |
| 5.2            | Sequence Diagram Get Cash Value       | 15             |
| 5.3            | Sequence Diagram of Get Transactions  | 15             |
| 5.4            | Class Diagram of Complete Transaction | 16             |
| 5.5            | Exchange of 10 of Coin A to Coin B    | 17             |
| 5.6            | Transaction Process in Blockchain     | 18             |
| B.1            | Desktop Main Page                     | 29             |
| B.2            | Desktop Transactions List             | 29             |
| B.3            | Desktop Main Page Details             | 30             |
| B.4            | Desktop Account Information           | 30             |
| B.5            | Android Home Page                     | 31             |
| B.6            | Android Account Information           | 32             |
| B.7            | Android Lower Home Page               | 33             |

## **LIST OF TABLES**

| <b>TABLE</b> | <b>NAME OF THE TABLE</b>         | <b>PAGE NO</b> |
|--------------|----------------------------------|----------------|
| 2.1          | Existing Work and Their Concepts | 5              |

# **CHAPTER 1**

## **INTRODUCTION**

### **1.1 PROJECT INTRODUCTION**

Our KryptX is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts. Smart contracts allow participants to transact with each other without a trusted central authority. Transaction records are immutable, verifiable, and securely distributed across the network, giving participants full ownership and visibility into transaction data. Transactions are sent from and received by user-created Ethereum accounts. A sender must sign transactions and spend Ether. Ethereum native cryptocurrency, as a cost of processing transactions on the network. The goal of this proposed work is to create encrypted blockchain applications. Anyone with an online connection can access this blockchain application system, which is an internet-based application, from anywhere on the internet.

This application enables a client to send and receive Ethereum over the blockchain network. Blockchain offers the security and infrastructure needed for cryptocurrencies to function. Blockchain uses proof of work to arrange these transactions and eliminate double spending problems. The process of organizing transactions in a specific order and determining the cost of adding them to the blockchain is known as proof of work. The word “blockchain” comes from the fact that each block in the chain has a link to the preceding one. Blockchain technology is the foundation of cryptocurrencies like Bitcoin. Blockchain offers the security and infrastructure needed for cryptocurrencies to function. Web 3.0 is being used in our project. Web 3.0 refers to the third generation of Internet services that enable the operation of websites and apps. Due to the system it is based on, Web 3.0 is anticipated to be more secure than its forebears. Since blockchain is a decentralized system, there is not one point of control that is vulnerable to hacking. This indicates that the Internet and websites are typically more protected against attacks. Users don't need to be concerned about their data being lost or hacked. These include sending and receiving Ethereum between wallets and exchanging it between them.

The existing system for cryptocurrency exchange predominantly operates on centralized platforms, where users trade digital assets through intermediaries that control the exchange infrastructure. In this setup, users must deposit their cryptocurrencies into wallets managed by the exchange, relinquishing a degree of control over their funds. Trading occurs through order books managed by the exchange, which match buy and sell orders. While centralized exchanges offer relatively fast and user-friendly trading experiences, they also present inherent risks such as potential security breaches, hacking incidents, and vulnerabilities that could compromise user data and funds. Additionally, these exchanges can sometimes face issues with transparency, regulatory compliance, and operational downtime. The centralized model contradicts the decentralization principles of blockchain technology and Web 3.0, where users have direct ownership and control over their assets, and transactions occur peer-to-peer without intermediaries.

In the year 2008, unknown person or group of people introduced the concept of blockchain in a White paper by Satoshi Nakamoto [1]. In this paper, he mentioned the implementation of the block with timestamp without any of the third person as a trusted part and difficulty parameter protocol which helps to add the blocks in the form of a chain. The design was implemented in the next year by Nakamoto to use the currency as a digital cryptocurrency called Bitcoin Cryptocurrency [2]. Where it serves as a public ledger for all the transactions that occur in the distributed network, the computer crackers in a centralized point can be exploited because the security method uses public key cryptography. In this system, if data is uploaded by a node, then the copy of that data will be replicated to all the nodes. It resembles the transparency of data and the immutability of the data. This is not possible in the centralized servers it is controlled by a centralized authority.

Defi is known to be as Decentralized Finance and also called open finance. It is totally about reinventing traditional financial services such as borrowing, lending and trading built using decentralized infrastructure like public blockchain and smart contracts. The blockchain developer should have the Defi skills and also understand the problem that is solved in financial services, if not it will not be a good innovation. In the finance industry, there is no incentive to improve bank sectors. The core problem is that everything is handled or controlled by the central system.

## **CHAPTER 2**

### **LITERATURE SURVEY**

#### **2.1 INFERENCES**

The research discusses how Bitcoin-beyond blockchain development overcomes those weaknesses and some of the remaining issues. Cryptocurrency blockchain standards and assurances do not meet FinTech's security and privacy needs, from transaction throughput to primitives. It examines how distributed databases are protected and offers a Blockchain-based solution to the problems associated with maintaining information secrecy in them. According to the authors, without mining and tokens, blockchain would drastically disrupt the method for maintaining the secrecy and authenticity of knowledge regarding bank transactions. In this paper, the issue of cryptographic consensus is addressed using blockchain technology. And if there is a way to guarantee that financial activity and transaction activities are saved in a specific database without the participation of the central authority. It outlines situations in which blockchain applications may be used and analyzes the key conceptual and technological aspects of blockchain. Incorporating blockchain technology, this paper examines the difficulties and possibilities presented by banking. By adopting methods that are more efficient than they are now, blockchain technology will transform the world's financial system to promote sustainable growth. The study suggests a systemic innovation paradigm to investigate and monitor innovation channels. This model may be used in any business to comprehend the innovation growth cycle and the strategy for gaining market share in the banking sector. The empirical findings reveal that many banks have yet to create or transition their traditional banking systems to Blockchain technology.

The goal of this research study is to create a decentralized blockchain-based coin as well as an electronic wallet. The paper comprises developing a generic blockchain that will be utilized for future blockchain application development. This blockchain API will be used to build a coin from the ground up. Create a new hashing function for the blockchain that takes input and produces a set length output. Using an extremely private and individualized wallet to access and manage the

aforementioned currency. With the help of this digital wallet technology, the user will be able to properly manage and spend cash. The user has total control over the tokens. The objective is also to make the money as safe, easy to receive, quick, and cheap as possible.

The literature review is detailed in the below table. The table provides information on the paper's specifics as well as its overall thesis. Understanding how the present system operates and the constraints that must be removed to improve the system is helpful.

## **2.2 LITERATURE SURVEYS**

**TITLE :** Blockchain-based Decentralized Storage Scheme

**AUTHOR:** Yan Zhu

**SUMMARY:** Yan Zhu suggests a decentralized storage scheme instead of a conventional centralized system. The provider performs a data integrity certificate to the user and only after it is verified, the user pays the fee for storage. The payment information is stored in the secure blockchain.

**TITLE:** A peer-to-peer electronic cash system

**AUTHOR:** Satoshi Nakamoto

**SUMMARY:** Satoshi Nakamoto introduced peer-to-peer networking which changed the entire domain. The author suggests a user to send payments directly from one party to another without a need for financial institution. This paper provides a solution to the double-spending problem with the introduction of peer-to-peer networks

**TITLE :** Zerocash: Decentralized Anonymous Payments from Bitcoin.

**AUTHOR:** Eli Ben-Sasson

**SUMMARY:** Eli Ben-Sasson explains in detail about decentralized anonymous

payments where the author points out some of the flaws in the bitcoin privacy guarantees. This paper fulfills that flaw by unlinking the transaction from the payment's origin and also reveals the payment destinations and the amount

**TITLE:** Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS

**AUTHOR :** Jin Sun

**SUMMARY:** Jin Sun proposed an access scheme for electronic medical records in IPFS with blockchain-Based Secure Storage. The author constructed attribute-based encryption scheme for secure storage and efficient sharing of electronic medical records in IPFS environment. The ideology that the author suggests is that we encrypt the data based on attributes and determine the attributes of the users. Each user's private key is related to their respected attributes whereas the ciphertext is related to the policy.

TABLE I: EXISTING WORK AND THEIR CONCEPTS

| S<br>N<br>o. | Paper Title                                                                | General idea                                                                               |
|--------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1            | A survey on the security of blockchain systems [2017]                      | A thorough examination of the protection, vulnerabilities in current and available system. |
| 2            | Blockchain and Cryptocurrencies Model, Techniques, and Applications [2018] | A summary of current cryptocurrencies to better understand blockchain and its many forms.  |
| 3            | A Brief Survey of Cryptocurrency Systems[2017]                             | It assesses all main mining strategies' strengths, weaknesses, and potential dangers       |
| 4            | Bitcoin: A Peer-to-Peer Electronic Cash System[2008]                       | A system that operates within the blockchain architecture.                                 |

Table 2.1: Existing Work and Their Concepts

## CHAPTER 3

### REQUIREMENT ANALYSIS

#### 3.1 ALGORITHM

1. **SHA-2 Secure Hashing Algorithm.** The SHA version 2 offers a variety of output bit input and length with a variety of unique hash algorithms. The SHA-256 is a brand-new hash algorithm that operates on 32-bit words alone. Both x86-based and x86-64-based architecture may use SHA-256. Figure3 displays the SHA algorithm
2. **Consensus protocols:** A consensus protocol is a method of attaining a single data value inside a distributed or decentralized system. Ensuring dependability in the system with unreliable nodes is the key objective. A hybrid proof of work paradigm will be used by the system. The computational challenge used for the Proof-of-work must be solved by guesswork. Anyone may readily verify the accuracy of the answer after finding the solution. Through the use of identification as a stake in the consensus method, the proof of authority enables relatively quick transactions. Figure 4 displays the steps of the consensus protocol.
3. **The algebraic structure** of elliptic curves over finite fields is the foundation of the public-key encryption method known as elliptic curve cryptography (ECC). Elliptic curves may be used for a variety of things, including key agreement, digital signatures etc. By fusing the key agreement with a symmetric encryption technique, they might be utilised for encryption inadvertently. ECC produces keys utilising the properties of an elliptic curve equation, as opposed to the traditional method of production as the product of large prime integers.
4. **UUID (Universally Unique Identifier):** Another name for UUID is GUID. Unlike most other numbering schemes, UUIDs are for practical purposes unique when created using normal procedures, without relying on a central

registration body or cooperation between the people creating them. While the likelihood of a UUID being copied is not zero, it is near enough to be insignificant

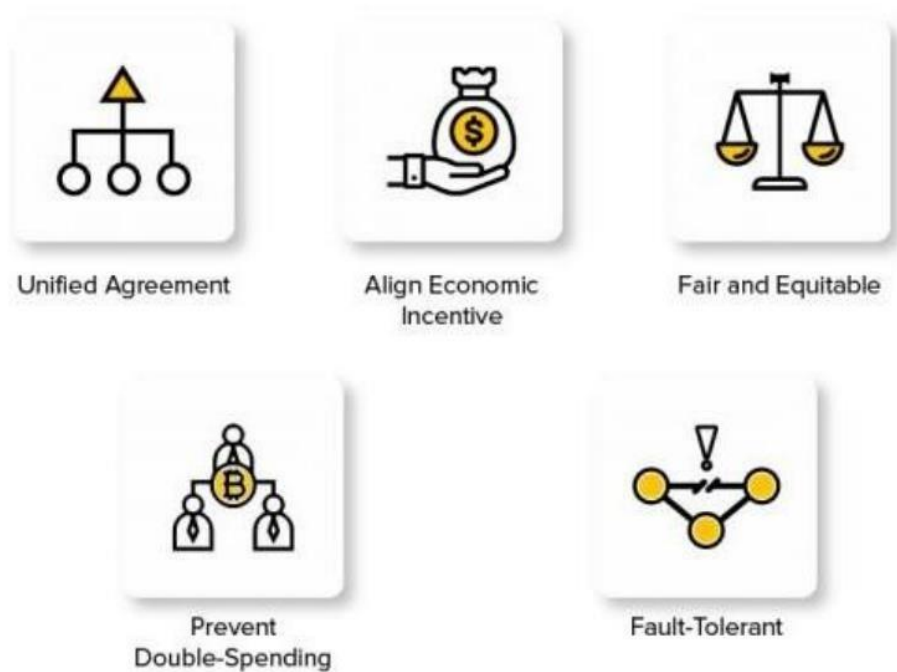


Fig 3.1: Steps of Consensus Protocol

## 3.2 Module Requirements

### 3.2.1 Web3j

Web3j is a lightweight, highly modular, reactive, type-safe Java and Android library for working with Smart Contracts and integrating with clients (nodes) on the Ethereum network. This allows you to work with the Ethereum blockchain, without the additional overhead of writing your integration code for the platform. It has a complete implementation of JSON-RPC client (Application Programming Interface)API over Hyper Text Transfer Protocol(HTTP) and Inter-Process Communication(IPC). It has a compatible version and supports Infura.It has complete support for the ethereum wallet.

### **3.2.2 Solidity**

Solidity is a contract-oriented programming language for writing smart contracts. Solidity is a statically-typed programming language designed for developing smart contracts that run on the EVM. It was influenced by C++, Python and JavaScript and is designed to target the Ethereum Virtual Machine (EVM). With Solidity, developers are able to write applications that implement self-enforcing business logic embodied in smart contracts, leaving a no-repudiable and authoritative record of transactions.

### **3.2.3 Metamask**

MetaMask is an extension for accessing Ethereum-enabled distributed applications, or "Dapps" in your browser! The extension injects the Ethereum web3API into every website's JavaScript context, so that dApps can read from the blockchain. MetaMask is a cryptocurrency wallet used to interact with the Ethereum blockchain. MetaMask allows users to store and manage account keys, broadcast transactions, send and receive Ethereum-based cryptocurrencies and tokens, and securely connect to decentralized applications through a compatible web browser.

### **3.2.4 CSS**

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation of a document written in a markup language such as HTML. CSS is a cornerstone technology of the World Wide Web, alongside HTML and JavaScript. CSS is designed to enable the separation of presentation and content, including layout, colors, and fonts. This separation can improve content accessibility, provide more flexibility and control in the specification of presentation characteristics, enable multiple web pages to share formatting by specifying the relevant CSS in a separate .CSS file which reduces complexity and repetition in the structural content as well as enabling the .CSS file to be cached to improve the page load speed between the pages that share the file and its formatting. Separation of formatting and content also makes it feasible to present the same markup page in different styles for different rendering methods, such as on-screen, in print, by voice (via speech-based browser or screen reader), and on Braille-based tactile devices. CSS also has rules for

alternate formatting if the content is accessed on a mobile device.

### **3.2.5 HTML**

The Hypertext Markup Language, or HTML(Hypertext Markup Language) is the standard markup language for documents designed to be displayed in a web browser. It can be assisted by technologies such as Cascading Style Sheets (CSS) and scripting languages such as JavaScript. Web browsers receive HTML documents from a web server or from local storage and render the documents into multimedia web pages. HTML describes the structure of a web page semantically and originally included cues for the appearance of the document. HTML elements are the building blocks of HTML pages. With HTML constructs, images and other objects such as interactive forms may be embedded into the rendered page. HTML provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. HTML elements are delineated by tags, written using angle brackets. HTML can embed programs written in a scripting language such as JavaScript, which affects the behavior and content of web pages. Inclusion of CSS defines the look and layout of content. The World Wide Web Consortium (W3C), former maintainer of the HTML and current maintainer of the CSS standards, has encouraged the use of CSS over explicit presentational HTML. An HTML Application (HTA; file extension ".hta") is a Microsoft Windows application that uses HTML and Dynamic HTML in a browser to provide the application's graphical interface. A regular HTML file is confined to the security model of the web browser's security, communicating only to web servers and manipulating only web page objects and site cookies. An HTA runs as a fully trusted application and therefore has more privileges, like creation/editing/removal of files and Windows Registry entries. Because they operate outside the browser's security model, HTAs cannot be executed via HTTP, but must be downloaded (just like an EXE file) and executed from local file system.

## **CHAPTER 4**

### **PROPOSED SYSTEM**

#### **4.1 AIM**

By creating a decentralized cryptocurrency exchange application that prioritizes user control, transparency, and security, the project aims to foster a new era of financial autonomy and redefine the way digital assets are traded on the internet. The successful completion of this project will contribute to the advancement of blockchain technology and the realization of the Web 3.0 vision.

#### **4.2 Description of Proposed System**

The rapid evolution of blockchain technology has laid the foundation for a new era of decentralized applications and financial systems. This project aims to develop a cutting-edge Web 3.0 Cryptocurrency Exchange Application that leverages the power of blockchain to create a secure, transparent, and user-centric platform for trading digital assets.

The proposed application will be built upon the principles of Web 3.0, focusing on user empowerment, data ownership, and decentralized architecture. The key features and components of the application include:

1. **Decentralized Trading Platform:** The core of the application will be a decentralized trading platform, allowing users to securely trade a wide range of cryptocurrencies. Blockchain technology ensures that trades are executed transparently and without the need for intermediaries, thus enhancing trust and reducing the risk of fraud.
2. **User-Controlled Wallets:** Users will have complete control over their cryptocurrency holdings through personal wallets. Private keys will be securely stored on the user's device, ensuring that only the user has access to their funds.



## **CHAPTER 5**

### **IMPLEMENTATION**

#### **5.1 PROPOSED PLAN OF IMPLEMENTATION**

For our proposed plan of implementation, we are considering two modules that are to be completed in three phases. Two modules are as follows: Front-end for the application and Back-end using Solidity to implement Blockchain

Each of these modules will be considered as one phase and the remaining one phase will cover the connection and testing of these modules.

- Phase 1: In this phase, we will cover the front-end module, in which we will build the interactive user interface for the admin as well as the user. In parallel the research work related to the implementation of Blockchain in decentralized applications will be done.
- Phase 2: In this phase, we will cover the back-end module, we will implement the Blockchain using the Ethereum framework and convert the system into a decentralized application.
- Phase 3: The connection of two different modules along with the testing of the platform will be completed in this phase.

#### **5.2 BLOCKCHAIN INTEGRATION**

##### **5.2.1 Blockchain**

Blockchain is the growing list of records called blocks, containing structured information linked using the art of cryptography distributed globally . Each block in blockchain contains the cryptographic hash of previous block along with timestamp and data which typically varies with use-cases. Merkle trees are the fundamental part of blockchain. Every block contains the block header which is outcome of recursive cryptographic hashes of all the data nodes or transaction from bottom to

up approach. During hash generation, the order of data matters for the final hash of the block. If single detail of transactions or order of transaction changes then changes the merkle hash. Therefore, Merkle Root summarizes all of the data in the related transactions, and is stored in the block header. This feature makes blockchain resistance to modification which is considered secure by design. A database is a collection of information that is stored electronically on a computer system. Information, or data, in databases is typically structured in table format to allow for easier searching and filtering for specific information. Large databases achieve this by housing data on servers that are made of powerful computers. These servers can sometimes be built using hundreds or thousands of computers in order to have the computational power and storage capacity necessary for many users to access the database simultaneously. While a spreadsheet or database may be accessible to any number of people, it is often owned by a business and managed by an appointed individual that has complete control over how it works and the data within it. Blockchain is P2P network which relies on protocol for inter- node communication and validating the blocks. Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. Blocks in blockchain are the holder of valid transactions that are hashed and encoded in Merkle tree. Every block contains the cryptographic hash of previous blocks along with its own data which therefore forms the chain. This iterative mechanism in each block conforms the integrity of previous block all the way back to genesis block. Block time is the average time it takes in the network to generate 1 extra block in blockchain. By the time block is generated, the data of that block is verified. This means lesser the block typeface the transactions. A hard fork is a rule change such that the software validating according to the old rules will see the blocks produced according to the new rules as invalid. Storing data in P2P network allows Blockchain to eliminate the pitfalls of centralization. There will be no central point vulnerability ,no center point of failure in blockchain. It is open to public which makes it more user- friendly than traditionally owned records. Being permissionless and open, there is no need to guard against bad actors. Ethereum Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract(scripting) functionality.

### 5.2.2 Smart Contract Development

Smart contract acts as an agreement between client and postman during the transaction of data. Therefore, we have tried to ensure(look) from both parties during its development. We have tried to keep as less data as possible in blockchain network without compromising services. The key to these contracts is the decentralized network known as blockchain. Smart contracts use blockchain technology to verify, validate, capture and enforce agreed-upon terms between multiple parties. Smart contracts on the blockchain allow for transactions and agreements to be carried out among anonymous parties without the need for a central entity, external enforcement, or legal system. The transactions are transparent, irreversible, and traceable. Blockchain is the perfect environment for smart contracts, as all the data stored is immutable and secure. The data of a smart contract is encrypted and exist on a ledger, meaning that the information recorded in the blocks can never be lost, modified, or deleted. Smart Contract act as a global database which gets deployed in the blockchain.

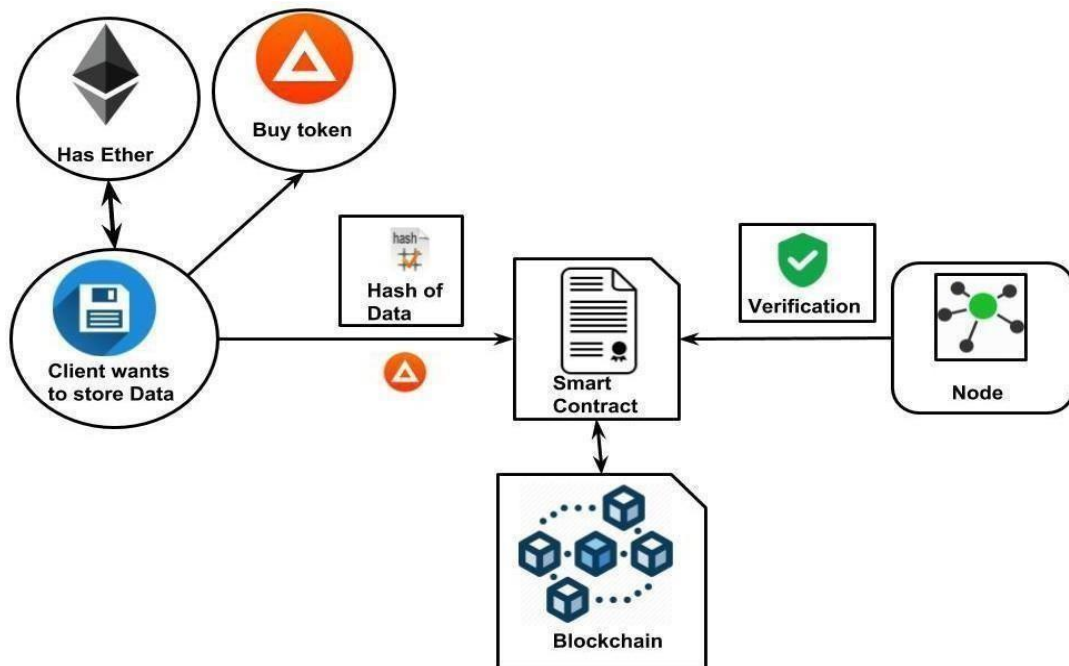


Fig.5.1: Smart Contract Flow Diagram

## 5.3 UML DIAGRAMS

### 5.3.1 Get Cash value of Coin 'X'

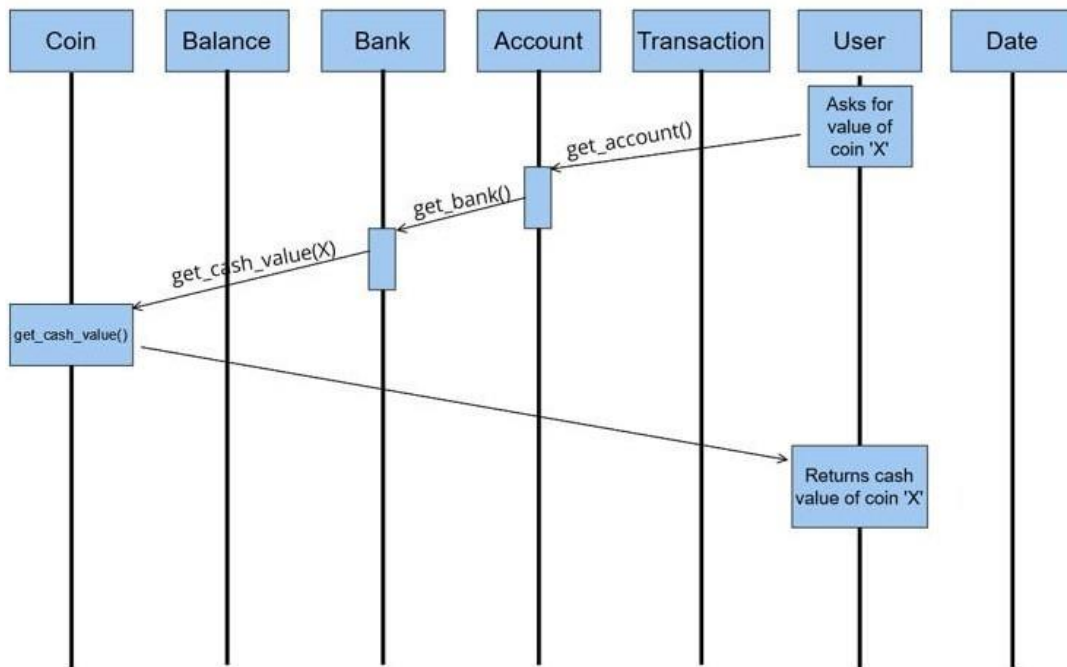


Fig 5.2: Sequence Diagram Get Cash Value of Coin 'X'

### 5.3.2 Get Transactions from date 'X'

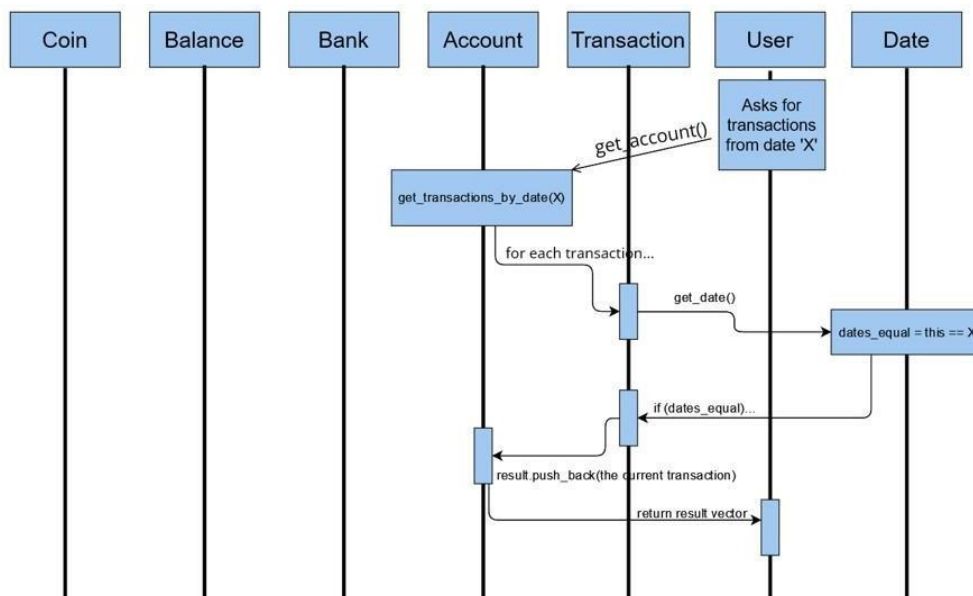


Fig 5.3: Sequence Diagram of Get Transactions from date 'X'

### 5.3.3 Complete Transaction

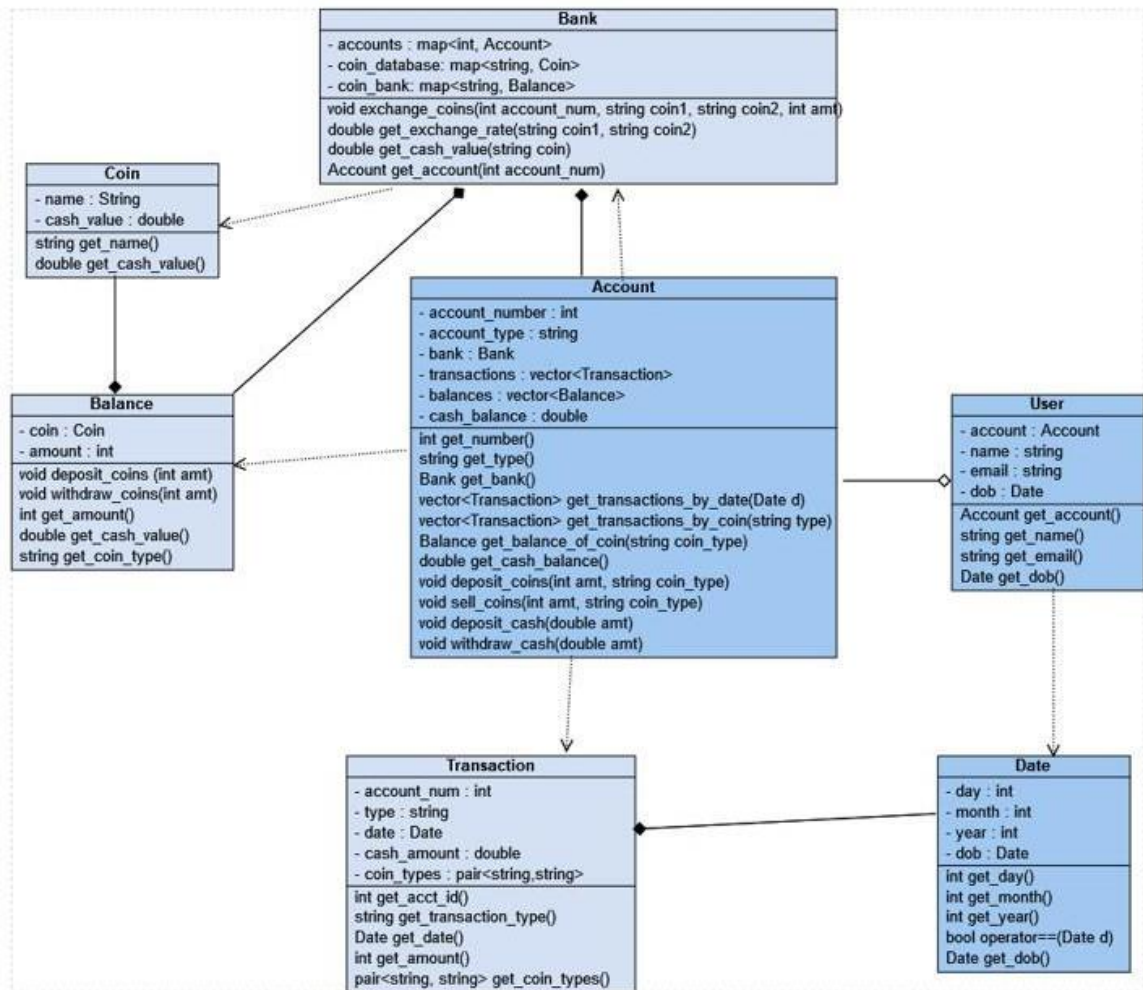


Fig 5.4: Class Diagram of Complete Transaction

### 5.3.4 Exchange of Coins

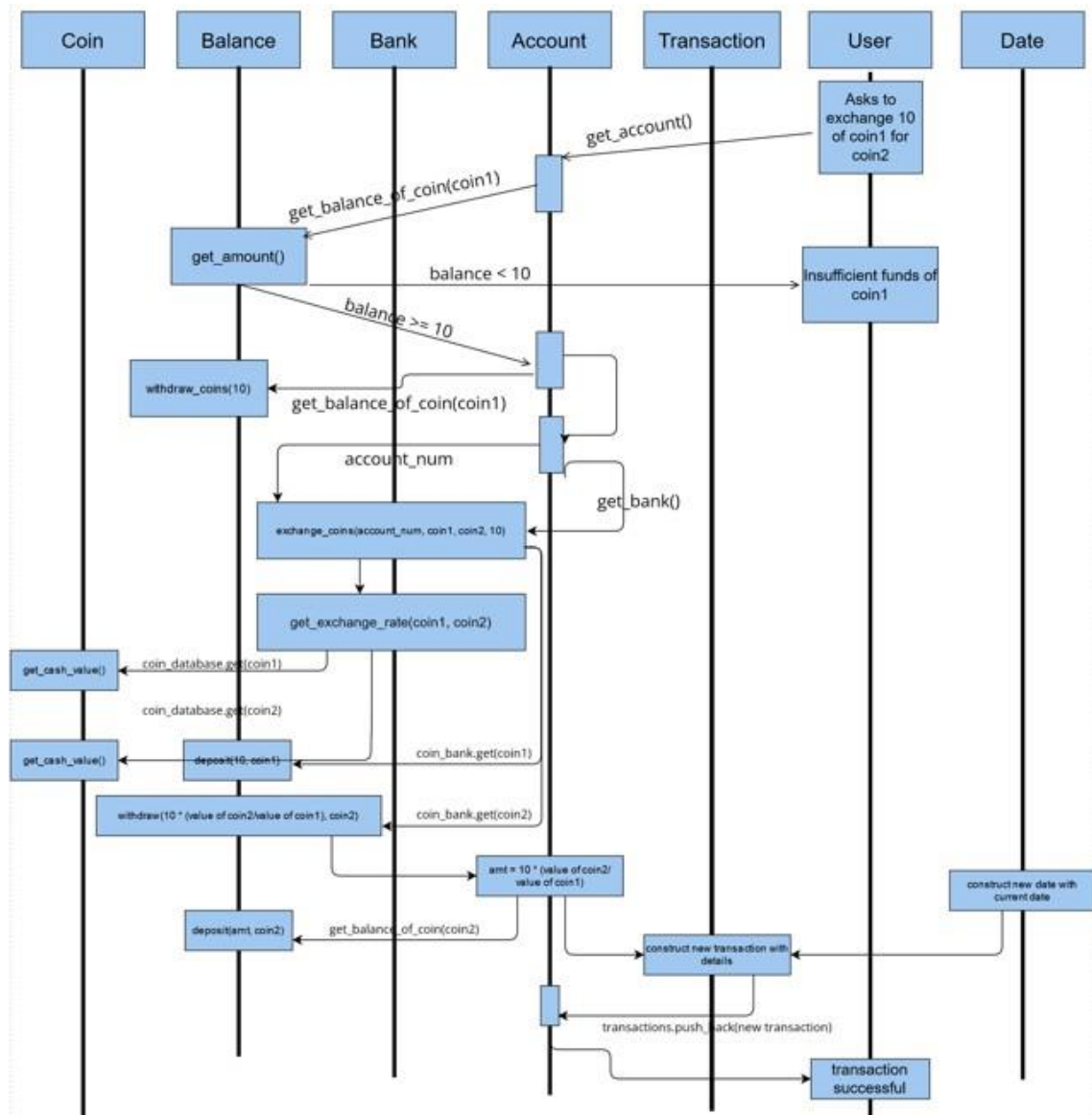
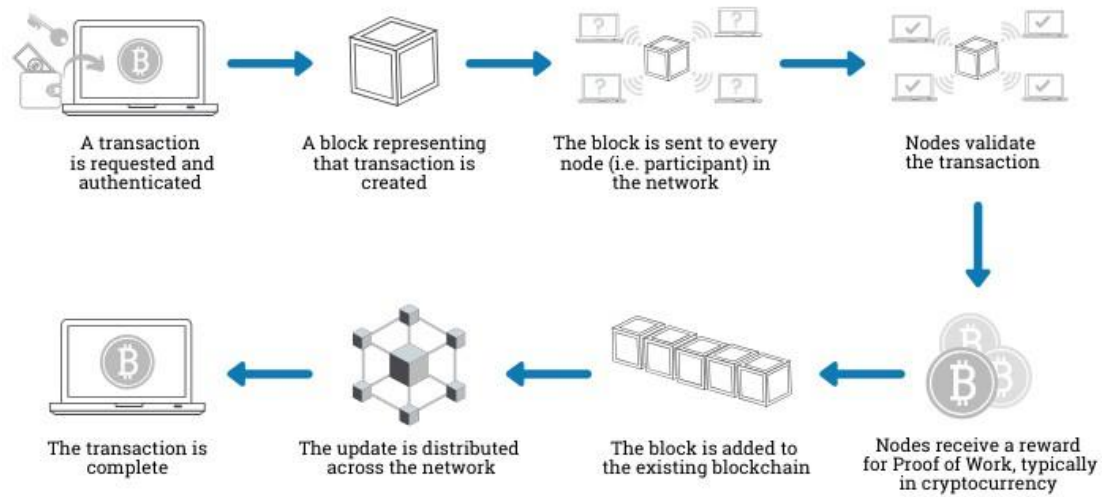


Fig 5.5: Exchange of 10 of Coin A for the Corresponding amount of Coin B

## 5.4 WORKING PROCESS

### How does a transaction get into the blockchain?



© Euromoney Learning 2020

Fig 5.6: Transaction Process in Blockchain

## **CHAPTER 6**

### **RESULTS AND DISCUSSION**

#### **6.1 RESULT**

The culmination of our final year engineering project is the development of a cutting-edge Web 3.0 based cryptocurrency exchange system leveraging blockchain technology. Our project marks a significant advancement in the realm of digital finance, offering users a secure, transparent, and decentralized platform for trading cryptocurrencies.

Through meticulous design and implementation, our system seamlessly integrates the principles of Web 3.0, embracing decentralized protocols and fostering peer-to-peer interactions. This architecture ensures enhanced security, resilience against cyber threats, and reduced dependency on centralized authorities, aligning with the ethos of blockchain technology.

The core functionality of our exchange system revolves around facilitating the seamless exchange of various cryptocurrencies while prioritizing security and user experience. Utilizing blockchain technology, transactions are executed with utmost transparency and immutability, eliminating the risk of fraud or manipulation often associated with traditional financial systems.

One of the standout features of our system is its intuitive user interface, designed to accommodate both novice and experienced traders. Through thoughtful user experience design, we aim to democratize access to cryptocurrency trading, making it accessible to a broader audience.

Furthermore, our project emphasizes scalability and interoperability, allowing for seamless integration with existing blockchain networks and protocols. This ensures that our exchange system remains adaptable to the evolving landscape of cryptocurrencies, accommodating new assets and technologies as they emerge.

In terms of performance, our system undergoes rigorous testing to ensure optimal speed, reliability, and efficiency. By leveraging advanced algorithms and distributed ledger technology, we strive to deliver a trading experience that meets the highest industry standards.

Overall, the results of our final year project underscore the transformative potential of Web 3.0 and blockchain technology in revolutionizing the financial sector. Through innovation, collaboration, and dedication, we have laid the foundation for a decentralized exchange ecosystem that empowers users and reshapes the future of finance.

## 6.2 FUTURE SCOPE

The future scope for a Web 3.0 cryptocurrency exchange blockchain application using smart contracts is highly promising and encompasses a range of advancements that align with the principles of decentralization, security, and user empowerment. Some of the potential directions for future development include:

1. **Enhanced Decentralization:** As blockchain technology continues to evolve, the application could further decentralize its architecture by exploring distributed ledger technologies beyond the traditional proof-of-work and proof-of-stake mechanisms. This might involve integrating newer consensus algorithms that improve scalability, energy efficiency, and consensus mechanisms, enabling a higher number of transactions while maintaining security.
2. **Interoperability:** Expanding cross-chain compatibility to support an even wider array of blockchain networks could enable seamless asset transfers between different ecosystems. This would facilitate a more comprehensive range of tradable assets and improve overall liquidity.
3. **DeFi Integration:** Integrating the application with decentralized finance

(DeFi) protocols could allow users to directly lend, borrow, and earn interest on their digital assets within the exchange platform, eliminating the need for intermediaries and enhancing financial autonomy.

4. **Decentralized Identity (DID):** Implementing DID solutions would give users full control over their personal data and identities. This can enhance security, privacy, and user trust by allowing them to verify their identity without divulging unnecessary information.
  
5. **Governance and DAOs:** Implementing decentralized autonomous organizations (DAOs) could empower users to participate in the platform's decision-making processes, enabling them to vote on important issues such

## **CHAPTER 7**

### **CONCLUSION**

In conclusion, the development of a Web 3.0 decentralized blockchain application for a cryptocurrency exchange utilizing smart contracts represents a significant advancement in the realm of financial technology. Through this project, we have explored the potential of blockchain technology to revolutionize traditional financial systems by introducing decentralization, transparency, and security.

The implementation of smart contracts has facilitated trustless transactions, enabling users to exchange digital assets directly without the need for intermediaries. This not only reduces transaction costs but also eliminates the risk of censorship or manipulation by third parties. Furthermore, the use of blockchain technology ensures immutability, meaning that transaction records are tamper-proof and cannot be altered retroactively, enhancing the overall integrity of the exchange platform.

By embracing decentralization, our application promotes financial inclusivity by providing access to cryptocurrency trading for individuals around the globe, regardless of geographical location or socioeconomic status. This democratization of finance aligns with the principles of decentralization, empowering users to have full control over their assets without relying on centralized authorities.

However, it is essential to acknowledge that the development of a decentralized exchange is not without challenges. Scalability, user experience, and regulatory compliance remain significant hurdles that must be addressed to achieve widespread adoption. Additionally, the security of smart contracts is paramount, as any vulnerabilities could potentially lead to financial losses for users.

Moving forward, continued research and development in blockchain technology, along with collaboration between industry stakeholders and regulators, will be crucial for realizing the full potential of decentralized exchanges.

## REFERENCES

- [1] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
- [2] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin.
- [3] Buterin, V. (2013). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. [White paper]. Ethereum Project. Retrieved from <https://github.com/ethereum/wiki/wiki/White-Paper>
- [4] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from <https://bitcoin.org/bitcoin.pdf>
- [5] Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. [White paper]. Ethereum Project. Retrieved from <https://ethereum.org/en/whitepaper/>
- [6] Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2017). Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services, 13(4), 352–375. <https://doi.org/10.1504/IJWGS.2017.10006689>
- [7] Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.
- [8] Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media.
- [9] Zohar, A. (2015). Bitcoin: Under the Hood. Communications of the ACM, 58(9), 104–113. <https://doi.org/10.1145/2818993>
- [10] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292–2303.

<https://doi.org/10.1109/ACCESS.2016.2566339>

[11] Dai, J., Vasarhelyi, M. A., & Kogan, A. (2019). Accounting for the Blockchain Information Risk in Audit and Assurance Services. *Journal of Emerging Technologies in Accounting*, 16(1), 59–74. <https://doi.org/10.2308/jeta-52223>

[12] Zheng, Z., Xie, S., Dai, H.-N., Wang, H., & Pan, Y. (2016). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In 2016 IEEE International Congress on Big Data (pp. 557–564). <https://doi.org/10.1109/BigDataCongress.2016.85>

[13] Grigg, I. (2019). Triple-Entry Accounting. Available at: [http://iang.org/papers/triple\\_entry.html](http://iang.org/papers/triple_entry.html)

[14] Mullan, M., & Reitz, K. (2018). Blockchain: Opportunities and Challenges for Accounting and Financial Reporting. *Journal of Information Systems*, 32(3), 81–93. <https://doi.org/10.2308/isys-52188>

[15] Yermack, D. (2017). Corporate Governance and Blockchains. *Review of Finance*, 21(1), 7–31. <https://doi.org/10.1093/rof/rfw074>

[16] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

[17] Consensys. (2019). *Understanding Ethereum: A Complete Guide*. Available at: <https://consensys.net/ethereum-guide/>

[18] Clark, J., Dorri, A., & Tucker, R. (2019). A Survey of Blockchain Enabled Applications: Challenges, Solutions, and Future Trends. *IEEE Access*, 7, 159160–159191. <https://doi.org/10.1109/ACCESS.2019.2948577>

[19] Szabo, N. (1996). *Smart Contracts: Building Blocks for Digital Markets*. Available at:

[http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\\_contracts\\_2.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html)

[20] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials*, 18(3), 2084–2123. <https://doi.org/10.1109/COMST.2016.2535718>

## APPENDIX

### A. SOURCE CODE:

#### **TransactionContext.jsx**

```
import React, { useEffect, useState } from "react";
import { ethers } from "ethers";
import { contractABI, contractAddress } from "../utils/constants";
import BN from "bn.js";
import { blockTimestampToViewFormatter } from "../utils/timeFormat";

export const TransactionContext = React.createContext();

const { ethereum } = window

const getEthereumContract = async () => {
  if (ethereum) {
    const provider = new ethers.BrowserProvider(ethereum)
    const signer = await provider.getSigner()
    const transactionContract = new ethers.Contract(contractAddress, contractABI,
    signer)
    console.log({
      provider,
      signer,
      transactionContract,
    });
    return transactionContract
  }
  return null
}

export const TransactionProvider = ({ children }) => {
  const [currentAccount, setCurrentAccount] = useState("")
  const [formData, setFormData] = useState({ addressTo: "", amount: "", keyword:
  "", message: "" })
```

```

const [isLoading, setIsLoading] = useState(false)
const [transactionCount, setTransactionCount] = useState(0)
const [allTransactions, setAllTransactions] = useState([])
// ethereum.on('accountsChanged', (accounts) => {
//   console.log(accounts);
//   setCurrentAccount(accounts[0])
// });

useEffect(() => {
  if (!ethereum.isMetaMask) {
    alert("Please install metamask")
  }
}, [])

useEffect(() => {
  if (currentAccount[0]) {
    fetchAllTransactions()
  }
}, [currentAccount])

const handleChange = (e, name) => {
  setFormData((prevState) => ({
    ...prevState,
    [name]: e.target.value
  }))
}

const checkIfWalletIsConnected = async () => {
  try {
    if (!ethereum) return alert("Please install metamask")
    const accounts = await ethereum.request({ method: 'eth_accounts' })
    if (accounts.length) {
      const account = accounts[0]
      console.log("Found an authorized account:", account)
    }
  }
}

```

```

    } else {
      console.log("No authorized account found")
    }
  } catch (error) {
    console.log(error)
  }
}

const connectWallet = async () => {
  try {
    const accounts = await ethereum.request({ method: 'eth_requestAccounts' })
    console.log("connectWallet accounts", accounts);
    setCurrentAccount(accounts[0])
  } catch (error) {
    console.log(error)
  }
}

const fetchAllTransactions = async () => {
  try {
    const transactionContract = await getEthereumContract()
    const allTransactions = await transactionContract.getAllTransactions()
    console.log("allTransactions", allTransactions);

    const structuredTransactions = allTransactions.map((transaction) => ({
      addressTo: transaction.receiver,
      addressFrom: transaction.sender,
      timestamp: blockTimestampToViewFormatter(transaction.timestamp),
      message: transaction.message,
      keyword: transaction.keyword,
      amount: ethers.formatEther(transaction.amount),
    }));
    console.log("structuredTransactions", structuredTransactions);
    setAllTransactions(structuredTransactions);
  }
}

```

```

} catch (error) {
  console.log(error);
}

const sendTransaction = async () => {
  const transactionContract = await getEthereumContract()

  const { addressTo, amount, keyword, message } = formData
  console.log("currentAccount", currentAccount);
  console.log(formData);
  const parsedAmount = ethers.parseEther(amount)
  const parsedAmountBN = new BN(parsedAmount, 10)
  console.log(parsedAmount);
  // It has been abandoned, use BN.js
  console.log(parsedAmount._hex);
  ethereum.request({
    method: 'eth_sendTransaction',
    params: [{
      from: currentAccount,
      to: addressTo,
      value: parsedAmountBN.toString(16),
    }]
  }).then((txHash) => console.log("ethereum txhash", txHash))
  .catch((error) => console.error(error));

  const transactionHash = await transactionContract.addToBlockchain(addressTo,
    parsedAmount, message, keyword)

  console.log("transactionHash", transactionHash.hash);
  const count = await transactionContract.getTransactionCount()
  console.log(count);
  setTransactionCount(count)
  setIsLoading(true)
  await transactionHash.wait()

```

```
setIsLoading(false)
}
```

```
return (
  <TransactionContext.Provider value={{ connectWallet, currentAccount, formData,
    setFormData, handleChange, sendTransaction, isLoading, transactionCount,
    allTransactions }}>
    {children}
  </TransactionContext.Provider>
)
}
```

### **Transactions.sol :**

```
pragma solidity ^0.8.9;
```

```
contract Transactions {
  uint256 transactionCount;
```

```
  event Transfer(address from, address receiver, uint amount, string message,
    uint256 timestamp, string keyword);
```

```
  struct TransferStruct {
    address sender;
    address receiver;
    uint amount;
    string message;
    uint256 timestamp;
    string keyword;
  }
```

```
TransferStruct[] transactions;
```

```
function addToBlockchain(address payable receiver, uint amount, string memory  
message, string memory keyword) public {  
transactionCount += 1;  
transactions.push(TransferStruct(msg.sender, receiver, amount, message,  
block.timestamp, keyword));  
emit Transfer(msg.sender, receiver, amount, message, block.timestamp, keyword);  
}
```

```
function getAllTransactions() public view returns(TransferStruct[] memory) {  
return transactions;  
}
```

```
function getTransactionCount() public view returns(uint256) {  
return transactions.length;  
}  
}
```

B. SCREENSHOTS

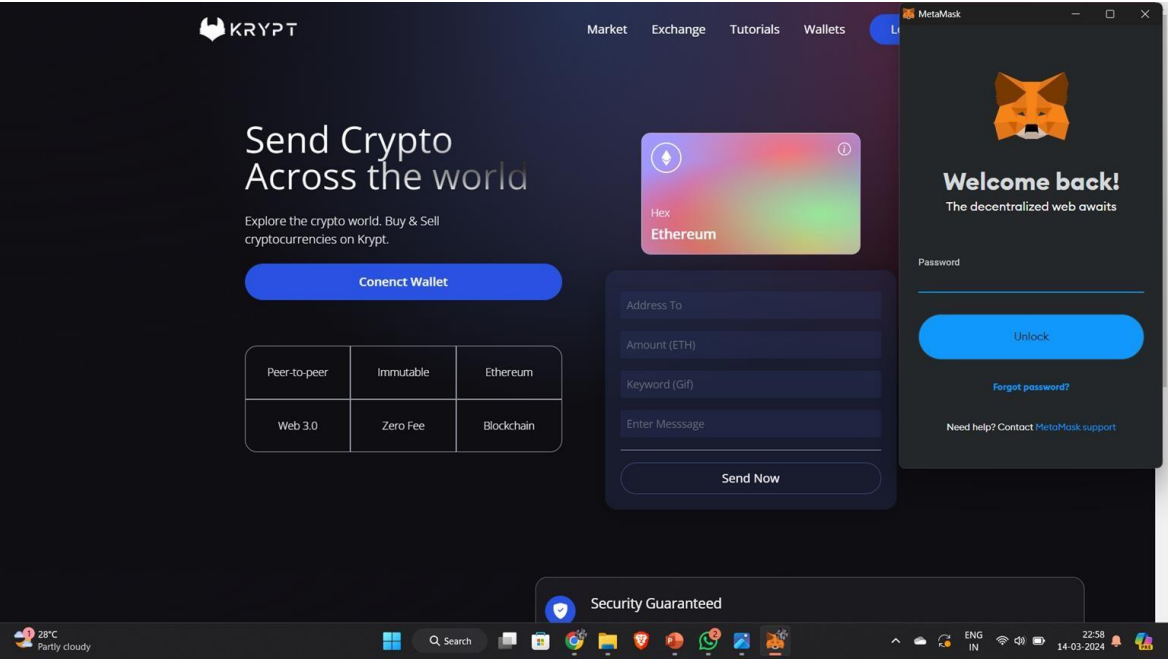


Fig B.1: Desktop Main Page

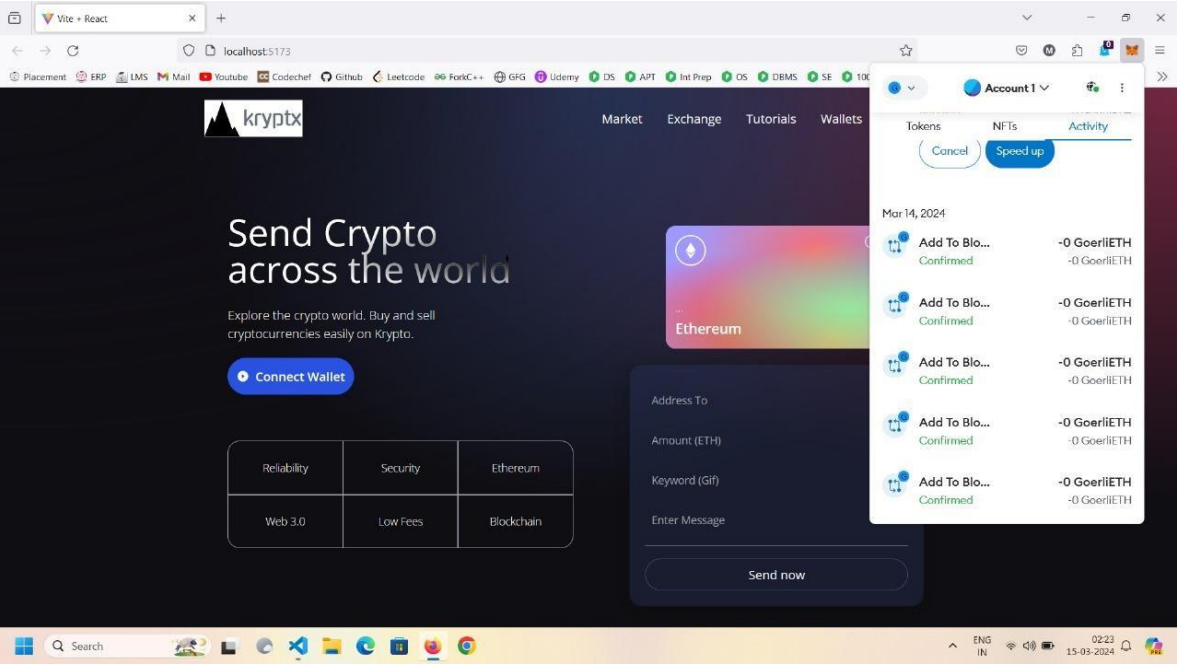


Fig B.2 : Desktop Transactions List

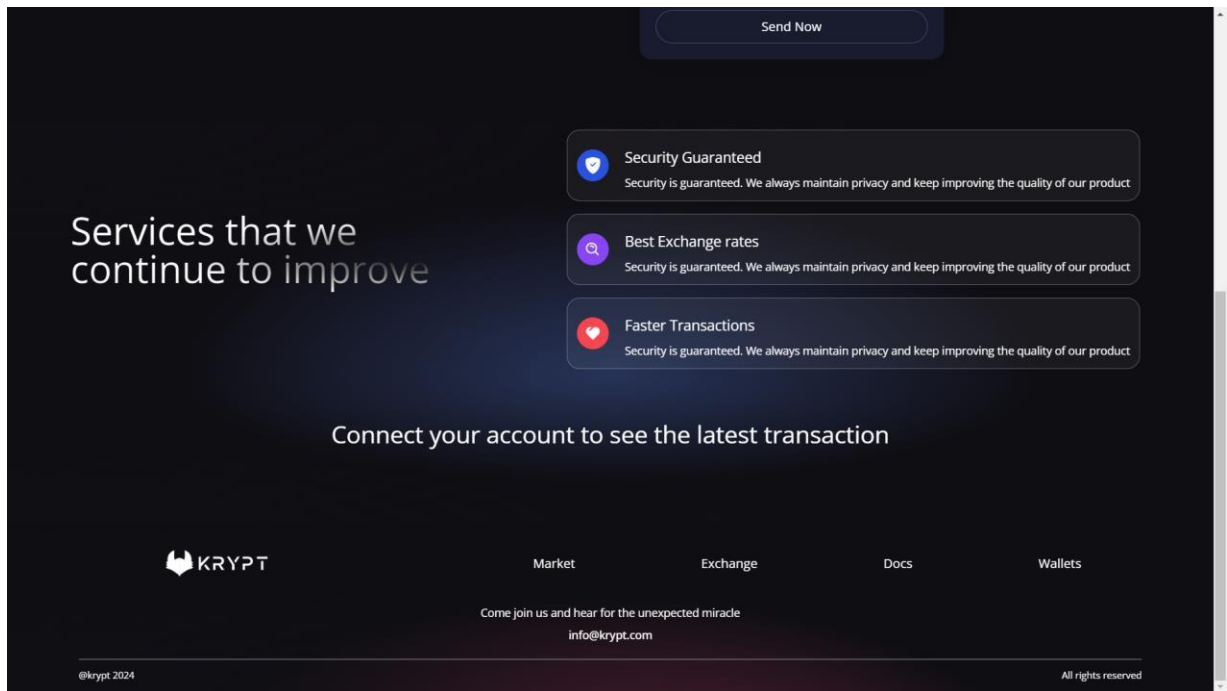


Fig B.3 : Desktop Main Page Details

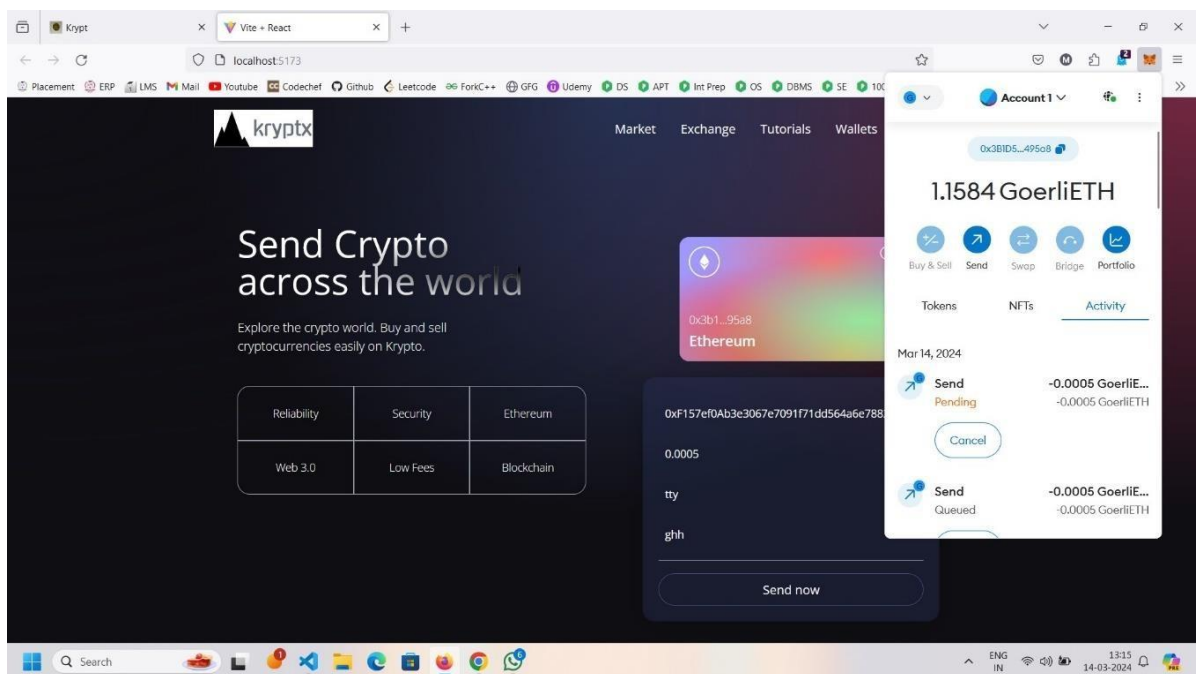


Fig B.4: Desktop Account Information

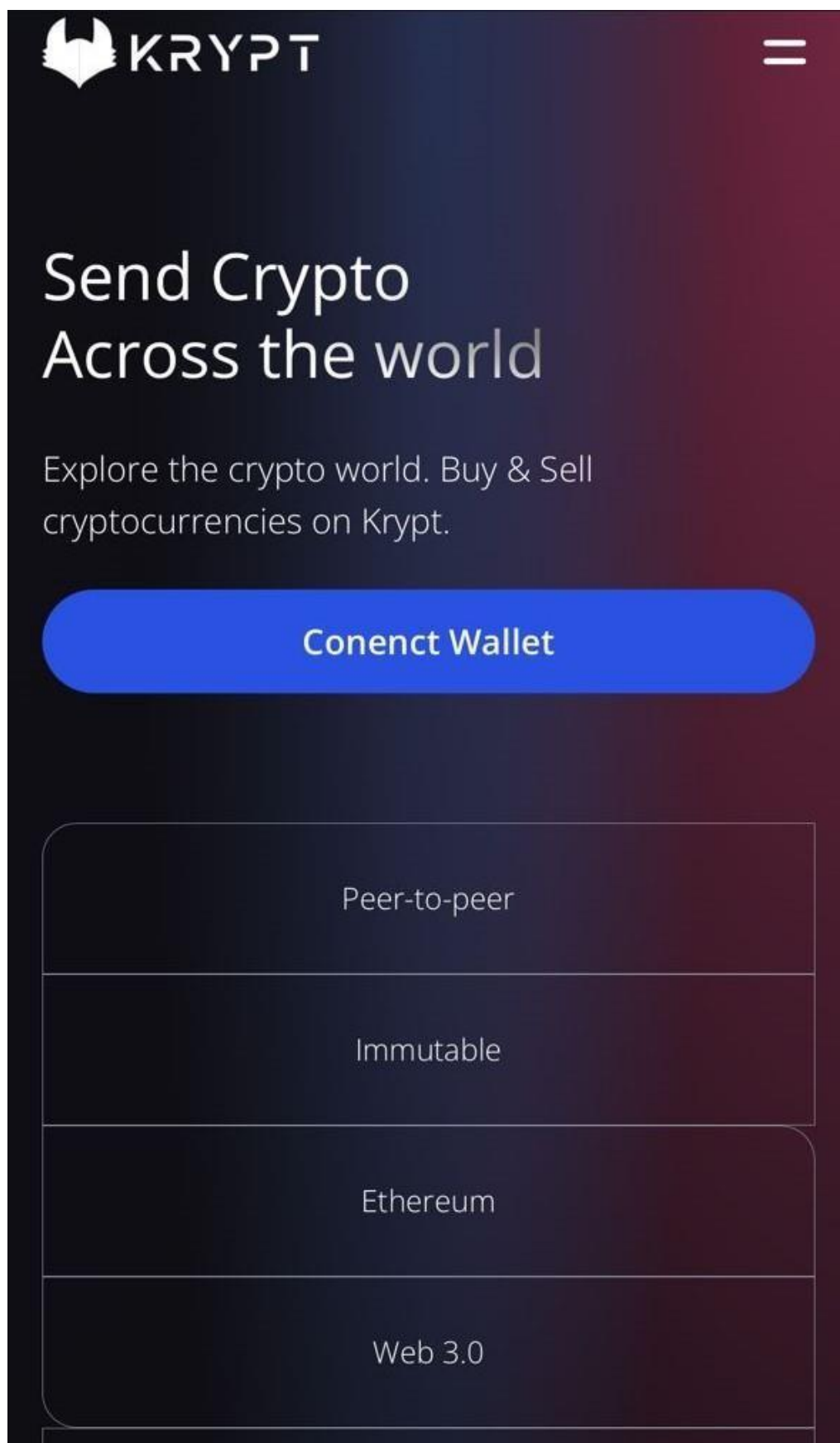


Fig B.5: Android Home Page

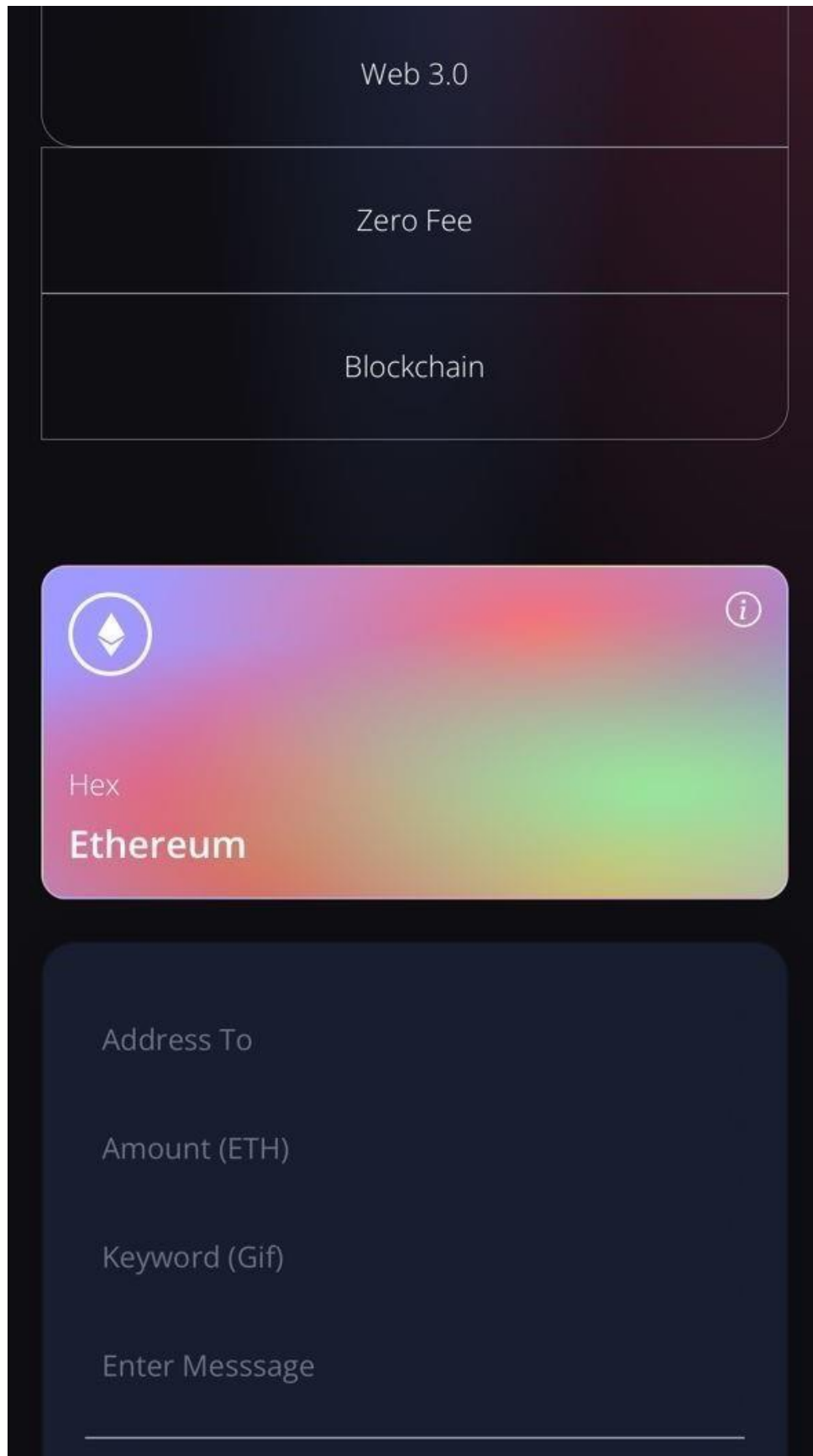


Fig B.6: Android Account Information

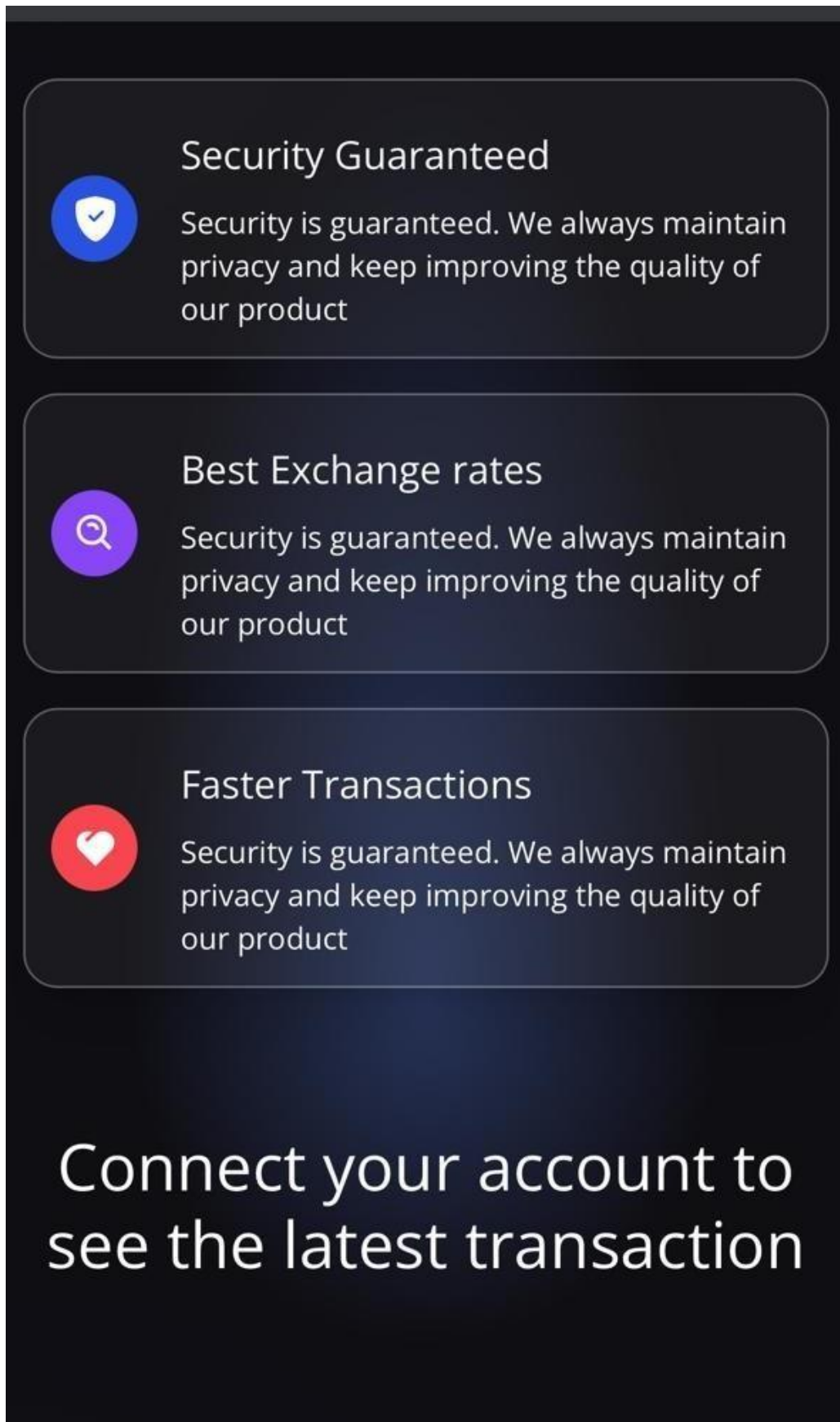


Fig B.7: Android Lower Home Page

## C. RESEARCH PAPER

# WEB 3.0 DECENTRALISED BLOCKCHAIN APPLICATION FOR CRYPTO EXCHANGE USING SMART CONTRACTS

Keshav Kumar<sup>1</sup>, Karan Mahto<sup>2</sup>, Ms. V. Gowri Manohari<sup>3</sup>, Dr J. Jeslin Shanthamalar<sup>4</sup>,  
Ms S.Nithya<sup>5</sup>

<sup>1,2</sup> U.G. Student, Department of CSE, Sathyabama Institute of Science and Technology,  
Chennai

<sup>3,4,5</sup> Assistant Professor, School of Computing, Sathyabama Institute of Science and  
Technology, Chennai

<sup>1</sup> kk9197707@gmail.com, <sup>2</sup> mahtokaran8058@gmail.com, <sup>3</sup>  
gowrimanohari.cse@sathyabama.ac.in,

<sup>4</sup> jeslinshanthamalar.cse@sathyabama.ac.in, <sup>5</sup> nithya.cse@sathyabama.ac.in

## I. ABSTRACT

**This initiative is dedicated to constructing a decentralized cryptocurrency exchange platform through the utilization of Web 3.0 technologies and smart contracts. The intended platform harnesses the capacity of blockchain to establish a transparent as well as secure space for cryptocurrency trading. The automation of trade executions is achieved through the implementation of smart contracts, guaranteeing the reliability and permanence of transactions.**

**A key emphasis of the project lies in crafting a user-friendly interface that enables individuals to engage in direct trading of various cryptocurrencies, eliminating the necessity for intermediaries. Furthermore, the platform integrates advanced security protocols to safeguard user funds and thwart any unauthorized access attempts.**

**Keywords:** Decentralized Exchange, Web 3.0 Technologies, Smart Contracts, Transparent Environment, Secure Crypto Trading, Trade Automation, User-Friendly Interface, Direct Cryptocurrency Trading, Intermediary Elimination, Advanced Security Measures, Unauthorized Access Prevention.

## II. INTRODUCTION

Our decentralized blockchain platform, KryptX, establishes a secure peer-to-peer network for smart contract execution and

verification, our decentralized blockchain platform, KryptX, empowers users to conduct transactions independently of a central authority. With immutable, verifiable records safely dispersed throughout the network, smart contracts enable trustless transactions and provide participants with complete ownership and insight into transaction data. User-created Ethereum accounts are used in transactions, and as a processing fee on the network, senders are required to sign transactions and spend Ether, Ethereum's native coin. Developing encrypted blockchain apps that are available to everybody with an internet connection is the main goal of this study. Clients can send and receive Ethereum over the blockchain network by using this web application. Blockchain gives cryptocurrency operations the security and infrastructure they need by organizing transactions and preventing double-spending by using proof of work. The term "blockchain" originates from the interconnected nature of each block in the chain, with each block linking to its predecessor. This technology serves as the foundational structure for cryptocurrencies like Bitcoin.

Web 3.0 technology is integral to our project, representing the third generation of Internet services designed to enhance website and app functionality. Leveraging the decentralized nature of blockchain, Web 3.0 is anticipated to offer improved security compared to its predecessors, minimizing vulnerability to hacking. Users may feel confident knowing that their data is secured because of this decentralized system's increased security measures for the Internet and websites. The

functionalities include secure Ethereum transactions between wallets and exchanges. The existing cryptocurrency exchange system operates predominantly on centralized platforms, introducing intermediaries that control the exchange infrastructure. This setup requires users to deposit their cryptocurrencies into exchange-managed wallets, relinquishing control over their funds. While centralized exchanges offer fast and user-friendly experiences, they present risks such as security breaches and hacking incidents. Furthermore, they may face challenges related to transparency, regulatory compliance, and operational downtime. This centralized model contradicts the decentralized principles of blockchain and Web 3.0, where direct ownership, control, and peer-to-peer transactions are emphasized.

A paradigm change in traditional financial services is represented by Decentralised Finance (Defi), incorporating decentralized infrastructure and smart contracts for activities such as borrowing, lending, and trading. Blockchain developers focusing on Defi must possess the necessary skills and an understanding of the problems addressed in financial services to drive meaningful innovation. Unlike the finance industry, where there is often limited incentive for improvement, Defi seeks to revolutionize the sector.

Transactions within the blockchain involve storing data, with Bitcoin tracking currency transfers in a timestamped, transparent manner. The decentralized ledger preserves on-chain transactions, viewable by anyone with a copy of the ledger. Ethereum utilizes the "TRIE DATA STRUCTURE" for efficient off-chain data storage, reducing the storage requirements for each blockchain node and minimizing blockchain traffic. Reliability is a fundamental aspect, as once data is stored on the blockchain, it cannot be altered. Consensus algorithms ensure agreement among nodes to attach new blocks to the previous chain containing various other blocks, maintaining the integrity of the system.

### III. LITERATURE SURVEY

This research explores the advancements in Bitcoin technology beyond traditional blockchain, addressing existing weaknesses and unresolved issues. It highlights that

existing cryptocurrency blockchain standards fail to meet the security and privacy requirements of FinTech, emphasizing the need for solutions in areas such as transaction throughput and primitives. The study delves into the protection of distributed databases and proposes a blockchain-based approach to address information secrecy challenges. The authors argue that it would significantly disturb the conventional methods of having the confidentiality and the legitimacy of financial transactions if we do not focus on mining [1].

Another paper in the literature addresses the cryptographic consensus issue using blockchain technology, focusing on ensuring financial activities and transactions are securely stored in a specific database without reliance on a central authority. The document explores potential applications of blockchain and investigates crucial technological issues. It suggests that by incorporating blockchain technology, the banking sector can undergo transformative changes to achieve more efficient methods, ultimately promoting sustainable growth. The paper presents a systemic upgradation paradigm that may be used to better analyze innovation growth cycles and market-provided techniques in the banking industry. Empirical data suggest that several banks have not changed their existing systems to new blockchain technology. [2]. Blockchain technology has garnered significant interest because of its peer-to-peer, decentralized, and anonymous properties. The paper discusses technical challenges and regulatory concerns associated with blockchain technology. It introduces smart contracts as self-executing and uncrackable computer programs, highlighting their ability to facilitate real-time transactions with reduced costs and enhanced security. The paper provides an in-depth exploration of the various elements and smart contract characteristics [3].

Despite widespread acceptance of the technology of blockchain, its long-term applications and potential are still largely unknown. The paper reviews the current state of blockchain technology, its applications in enhancing privacy protection, and identifies design flaws leading to additional issues. It examines prevalent blockchain security applications, discusses key issues, and highlights obstacles for future research to

address [4].

For optimal configuration, durability, and strategy, the paper suggests simulating an open-source blockchain project using Block SIM. This simulation mimics the behavior of the blockchain system, allowing developers to predict network behavior and choose the most effective settings. The paper emphasizes the importance of considering parallels and simulation findings to ensure the development of scalable, extensible, stable, and robust blockchain networks [5].

Another approach described in a paper builds on the Ethereum principle, advocating that software systems should only be present in the utilized layer at a given time. The extension of this idea involves incorporating the relevant section into a new transaction, eliminating the requirement to transmit the complete system initially. This innovation permits different participants to view incoming transactions, contributing in the development of scalable blockchain technology for use cases not requiring an exhaustive history of group activities [6].

The construction, validation, and maintenance of a trustworthy knowledge source using blockchain as a platform are explored in another study. The paper introduces smart contracts and an open cradle concept to effectively record an immutable knowledge path in the developed system. It demonstrates that, under honest participation, the proposed method securely collects, verifies, and authenticates knowledge while safeguarding against detrimental modifications. This approach facilitates easier auditing and evaluation of the knowledge source's history and integrity over time [7].

TABLE I: EXISTING WORK AND THEIR CONCEPTS

| S<br>N<br>o. | Paper Title                                                                | General idea                                                                               |
|--------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1            | A survey on the security of blockchain systems [2017]                      | A thorough examination of the protection, vulnerabilities in current and available system. |
| 2            | Blockchain and Cryptocurrencies Model, Techniques, and Applications [2018] | A summary of current cryptocurrencies to better understand blockchain and its many forms.  |
| 3            | A Brief Survey of Cryptocurrency Systems[2017]                             | It assesses all main mining strategies' strengths, weaknesses, and potential dangers       |
| 4            | Bitcoin: A Peer-to-Peer Electronic Cash System[2008]                       | A system that operates within the blockchain architecture.                                 |

#### IV. EXISTING SYSTEM

The current framework for cryptocurrency exchange is predominantly centralized, operating on platforms where users engage in the trading of digital assets through intermediaries overseeing the exchange infrastructure. This involves trading through order books managed by the exchange, matching buy and sell orders. While these centralized exchanges offer relatively speedy and user-friendly trading experiences, they inherently expose users to risks such as potential security breaches, hacking incidents, and vulnerabilities that could compromise user data and funds. Moreover, issues related to transparency, regulatory compliance, and operational downtime can also arise.

#### V. PROPOSED SYSTEM

The envisioned application will be constructed based on Web 3.0 principles, emphasizing user empowerment, data ownership, and a decentralized architecture. The primary features and components of the proposed application include:

**Decentralized Trading Platform:** At the core of the application will be a decentralized trading platform, enabling users to securely trade a diverse range of cryptocurrencies.

**User-Controlled Wallets:** Users will have full control over their cryptocurrency holdings through personalized wallets.

**Smart Contract Integration:** Smart contracts will be incorporated to automate and enforce the execution of trades.

**Security Measures:** It contains various multi-factor protocols for complete security and complete authentication. Regular security audits, will be implemented to protect user data and assets from potential threats.

**Interesting Interface:** The interface will be attractive and completely user-friendly. It will ensure that both novice and experienced traders can easily navigate and utilize the platform's features.

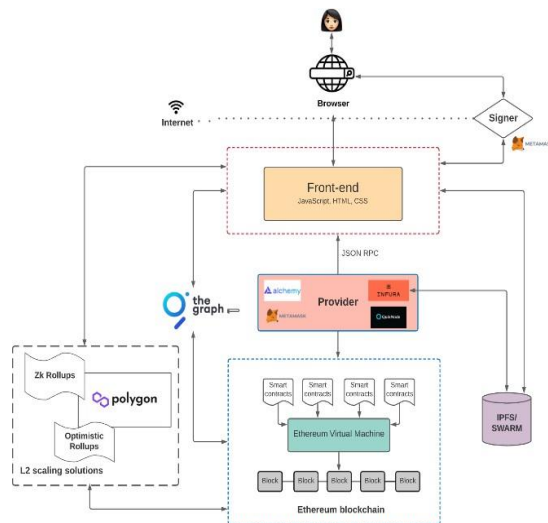


Fig.1. Architecture of Proposed System

The institution plans to establish a completely new certificate ID for its students using their MetaMask wallet addresses, considering factors such as the Merkle hash value, asking for permissions, and that new certificate ID for distribution across the network. In Uniswap, the smart contract can be interacted with to create a front end for a decentralized application using JavaScript. Other decentralized exchange applications, such as Ether Delta, also exist, featuring an element known as the Order book, which compiles details of buyer and seller orders. Uniswap, however, operates differently, utilizing liquidity pools for each asset instead of an order book.

Algorithms:

SHA-2: The Secure Hashing Algorithm version 2, including SHA-256, operates on 32-bit words and offers various output-bit input lengths.

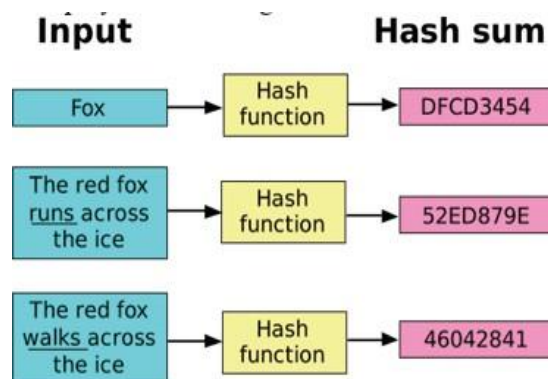


Fig.2 Jobs display tab

Consensus Protocols: These protocols aim to achieve only one result in a distributed system.

The system employs a hybrid algorithm, requiring computational challenges to be solved by guesswork. Proof-of-authority, using identification as a stake, facilitates relatively fast transactions.



Fig 3: Consensus Protocol.

Smart Contract: The smart contract creation represents the contract for the DeFi project, interacting with Uniswap protocols. Uniswap's smart contract is created in the Vyper, and an interface of Solidity is used to interface with Uniswap.

#### SOFTWARE SPECIFICATION

|                  |                                               |
|------------------|-----------------------------------------------|
| <b>Ganache</b>   | – Creates a Local Ethereum test environment.  |
| <b>Truffle</b>   | – Initialise basic setup for Ethereum Dapp    |
| <b>React js</b>  | – for frontend implementation                 |
| <b>Web3.js</b>   | – for interacting with Smart Contracts        |
| <b>IPFS</b>      | – for decentralized file storage              |
| <b>Meta Mask</b> | – Wallet for connecting with Ethereum Network |
| <b>Vscode</b>    | – code editor                                 |

The use of regulated transaction tokens or money is crucial for successful transactions. We developed an e-wallet which can handle different types of cryptocurrencies, along with an API for constructing further blockchain-related applications. A new hashing function was created to give the output containing the length which is predefined. The cryptocurrency implemented a hybrid consensus process to check as well as validate transactions. Implementing an effective data purification and detection method improved the execution performance of blockchain systems. The e-wallet is very accessible, rapid, and secure, allowing users to engage with and handle Bitcoin or other currencies.

## VII. ACKNOWLEDGMENT

Gratitude is extended to all the members of our college for their support throughout the project and to whoever has assisted us in completing this paper.

## REFERENCES

- [1] Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.
- [2] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin.
- [3] Buterin, V. (2013). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. [White paper]. Ethereum Project. Retrieved from <https://github.com/ethereum/wiki/wiki/White-Paper>
- [4] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from <https://bitcoin.org/bitcoin.pdf>
- [5] Wood, G. (2014). *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. [White paper]. Ethereum Project. Retrieved from <https://ethereum.org/en/whitepaper/>
- [6] Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2017). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, 13(4), 352–375. <https://doi.org/10.1504/IJWGS.2017.10006689>
- [7] Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.
- [8] Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media.
- [9] Zohar, A. (2015). Bitcoin: Under the Hood. *Communications of the ACM*, 58(9), 104–113. <https://doi.org/10.1145/2818993>
- [10] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303. <https://doi.org/10.1109/ACCESS.2016.2566339>
- [11] Dai, J., Vasarhelyi, M. A., & Kogan, A. (2019). Accounting for the Blockchain Information Risk in Audit and Assurance Services. *Journal of Emerging Technologies in Accounting*, 16(1), 59–74. <https://doi.org/10.2308/jeta-52223>
- [12] Zheng, Z., Xie, S., Dai, H.-N., Wang, H., & Pan, Y. (2016). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In *2016 IEEE International Congress on Big Data* (pp. 557–564). <https://doi.org/10.1109/BigDataCongress.2016.85>
- [13] Grigg, I. (2019). Triple-Entry Accounting. Available at: [http://iang.org/papers/triple\\_entry.html](http://iang.org/papers/triple_entry.html)
- [14] Mullan, M., & Reitz, K. (2018). Blockchain: Opportunities and Challenges for Accounting and Financial Reporting. *Journal of Information Systems*, 32(3), 81–93. <https://doi.org/10.2308/isys-52188>
- [15] Yermack, D. (2017). Corporate Governance and Blockchains. *Review of Finance*, 21(1), 7–31. <https://doi.org/10.1093/rof/rfw074>
- [16] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.
- [17] Consensys. (2019). *Understanding Ethereum: A Complete Guide*. Available at: <https://consensys.net/ethereum-guide/>
- [18] Clark, J., Dorri, A., & Tucker, R. (2019). A Survey of Blockchain Enabled Applications: Challenges, Solutions, and Future Trends. *IEEE Access*, 7, 159160–159191. <https://doi.org/10.1109/ACCESS.2019.2948577>
- [19] Szabo, N. (1996). *Smart Contracts: Building Blocks for Digital Markets*. Available at: [http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\\_contracts\\_2.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html)
- [20] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials*, 18(3), 2084–2123. <https://doi.org/10.1109/COMST.2016.2535718>

## D. CERTIFICATE



Certificate :Karan Mahto