IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

Secure Storage of Crypto Wallet Seed Phrase

Farsana AJ[1], Nisha A[2], Harikrishnan S R[3]
Student, MCA, CHMM College for Advanced Studies, Trivandrum, India[1]
Assistant Professor, MCA, CHMM College for Advanced Studies, Trivandrum, India[2]
Associate Professor, MCA, CHMM College for Advanced Studies, Trivandrum, India[3]

Abstract: *The Expense Tracker Application is a user-friendly and efficient tool designed to help individuals manage their personal finances with ease. In the ever-changing landscape of daily expenses, this application offers a structured method for tracking income, categorizing expenditures, and generating insightful financial reports. Its intuitive and visually appealing interface ensures that users of all technological skill levels can navigate it effortlessly. The application features visual representations to help users understand their budgetary trends and set limits for different expense categories. It provides timely alerts and notifications when users approach or exceed these budget limits. With robust security measures in place, the application ensures the confidentiality of users' financial data, enhancing their awareness of spending habits and enabling informed financial decisions. Additionally, this system proposes a novel approach to cryptocurrency transactions. Instead of relying on complex public and private keys, it simplifies key management by binding these keys to the unique IP addresses of the nodes involved. This method minimizes the need for users to manage large cryptographic keys, offering a more secure and user-friendly alternative for cryptocurrency wallets. By addressing the limitations of traditional cryptocurrency systems, this approach enhances key management and overall security.*

Keywords: Expense Tracking, Financial Management, Budget Alerts, Cryptocurrency Security, Key Management

I. INTRODUCTION

In an era where personal finance management and secure cryptocurrency transactions are increasingly crucial, innovative solutions are essential for addressing these needs effectively. The **Expense Tracker Application** and the cryptocurrency transaction management systemrepresent two advancements aimed at simplifying and securing financial processes.The Expense Tracker Applicationis designed to help individuals manage their personal finances more efficiently. As daily expenses become more complex, having a systematic approach to track income and categorize expenditures is vital. This application offers a user-friendly interface that caters to varying levels of technological expertise, providing tools to set budget limits, receive alerts, and generate detailed financial reports. By incorporating visual aids and robust security measures, the application enhances users' ability to monitor their spending habits and make informed financial decisions. In parallel, the cryptocurrency transaction management system introduces a novel approach to handling digital currency transactions. Traditionally, managing public and private keys for cryptocurrencies has been complex and cumbersome. This system addresses this challenge by binding keys to the unique IP addresses of nodes, simplifying key management and reducing the risk associated with handling large cryptographic keys. This method enhances the security of cryptocurrency wallets while providing a more user-friendly experience.Together, these systems represent significant strides in personal finance and cryptocurrency management, aiming to simplify and secure financial activities in a rapidly evolving digital landscape.

II. LITERATURE SURVEY

The literature on personal finance and cryptocurrency management highlights significant advancements and ongoing challenges in these areas. Modern personal finance tools like Mint and YNAB have transformed financial management by integrating automated tracking, budgeting, and visual data representation to help users understand spending patterns and adhere to budget limits These tools emphasize user-friendly interfaces, real-time alerts, and robust security measures to protect financial data. In the realm of cryptocurrency, traditional wallet systems rely on complex public and

DOI: 10.48175/IJARSCT-19434

private keys, which can be cumbersome for users to manage .Recent research suggests alternatives such as hardware wallets and secure enclave technologies to simplify key management while maintaining security .An emerging approach involves binding keys to unique attributes, like IP addresses, to streamline key management and enhance security .Integrating cryptocurrency tracking with traditional personal finance management tools is gaining attention, offering a unified platform for users to manage both asset types comprehensively. This integration aligns with current trends toward holistic financial management and addresses the complexities and security concerns inherent in digital currency transactions.

III. WORKING OF PROPOSED SYSTEM

This system introduces a novel approach to cryptocurrency transactions by eliminating the need for complex public and private keys. Instead, it utilizes a minimal additional layer by binding these keys to the unique IP addresses of the nodes involved. This innovation allows nodes to perform transactions without the need to remember intricate cryptographic keys, enhancing security and simplifying key management. The new system addresses the limitations of traditional cryptocurrency wallets, which rely heavily on the secure handling of keysan essential aspect for preventing the loss or theft of transaction details and assets. By providing a more secure and manageable key management scheme, this system aims to protect users' cryptocurrencies from potential loss.In a separate yet relevant development, the Expense Tracker application offers individuals a robust tool for managing their finances. With its user-friendly interface, the application facilitates the easy input of transaction details, including amount, date, and category. It supports comprehensive expense categorizationsuch as groceries, entertainment, and billsproviding users with a detailed breakdown of their spending habits and a holistic view of their financial status. The app allows users to track daily expenses and build a thorough financial history, enhanced by insightful visualizations like charts and graphs that clarify spending patterns and trends. By fostering greater financial awareness, the Expense Tracker empowers users to make informed budgeting decisions, identify areas for improvement, and optimize their spending behaviour. Overall, it serves as a valuable tool for effective financial management, guiding users towards better financial well-being through improved decision-making and budget optimization.

IV. TECHNOLOGY USED

Visual studio 2019

Visual Studio 2019 is a robust integrated development environment (IDE) created by Microsoft to streamline the software development process. It offers a comprehensive set of tools and features that support a variety of programming languages and development tasks, making it a favored choice among developers. A notable feature of Visual Studio 2019 is its advanced IntelliSense, which provides enhanced code completion, parameter information, quick info, and member lists. The IDE also includes a powerful debugging environment that facilitates the easy identification and resolution of code issues, supporting techniques such as live debugging, snapshot debugging, and variable inspection through breakpoints.Compared to previous versions, Visual Studio 2019 delivers improved performance and a more intuitive user interface. It features a customizable start window for quick access to recent projects and development tools. The new version also enhances code navigation with features like code maps and advanced search functionalities, simplifying the management and understanding of complex codebases. Additionally, Visual Studio 2019 supports modern development practices, including integration with Azure DevOps and GitHub for version control and continuous integration/continuous deployment (CI/CD) pipelines. Overall, Visual Studio 2019 is a versatile and feature-rich IDE that serves both individual developers and large teams, offering advanced capabilities, enhanced performance, and support for contemporary development workflows.

Cascading Style Sheet (CSS)

CSS, or Cascading Style Sheets, is a crucial technology for styling web pages and applications. It controls how HTML elements are displayed on the screen, managing their appearance, layout, and formatting. CSS empowers developers and designers to adjust various aspects, including colors, fonts, spacing, positioning, and responsiveness of web content. CSS operates using a rule-based approach, where selectors identify specific HTML elements or groups, and declarations within curly braces define the styles to be applied. Styles can be added directly within HTML elements, included internally via a `<style>` tag in the document's head, or linked externally through separate .css files. This modular design allows developers to craft visually appealing and user-friendly interfaces that adjust seamlessly to different screen sizes and devices, improving the overall user experience across various platforms.

C#.net

C# is known for its strong type checking, which helps prevent common programming errors and enhances the reliability of code. The language includes automatic garbage collection, which simplifies memory management and reduces the risk of memory leaks. Its syntax is clean and expressive, making it accessible to both beginners and seasoned programmers. C# adheres to core object-oriented programming principles, including encapsulation, inheritance, and polymorphism, which support the creation of reusable, modular code and improve maintainability.A significant advantage of C# is its seamless integration with the .NET framework. This framework provides a comprehensive library of pre-built components and a Common Language Runtime (CLR) that manages program execution, thereby simplifying the development process and enhancing application performance. Additionally, C# supports asynchronous programming via the `async` and `await` keywords, which streamlines the development of applications that require responsiveness and scalability, such as web applications and services.Developers working with C# benefit from powerful tools provided by Visual Studio, Microsoft's advanced integrated development environment (IDE). Visual Studio offers an array of features, including code completion, debugging, and performance profiling, which aid in writing efficient and error-free code. These tools contribute to a more streamlined development process and boost overall productivity, making C# a favored choice for a wide range of programming tasks.Overall, C# combines the strengths of its predecessors with modern programming practices, providing a robust, flexible, and efficient language for building high-quality applications. Its integration with the .NET framework, support for advanced programming techniques, and the powerful development environment offered by Visual Studio make it an essential tool for developers seeking to create reliable and scalable software solutions.

Blockchain technology

Blockchain technology is a groundbreaking approach to data management that utilizes a decentralized and distributed ledger system. Unlike traditional centralized databases, blockchain operates on a peer-to-peer network where each participant, or node, holds a complete copy of the ledger. This structure ensures data security and integrity by making it highly resistant to tampering and fraud.In a blockchain, data is organized into blocks, which are linked together in a chronological sequence. Each block contains a cryptographic hash of the previous block, along with a timestamp and transaction details. This chaining makes the data immutable, as altering any block would require altering all subsequent blocks, a process that demands significant computational power.Blockchain's transparency is a major advantage, as all network participants can access the same ledger, allowing for easy verification of transactions. The technology also employs consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) to validate and agree on transactions, ensuring network security and preventing double-spending.Beyond cryptocurrencies, blockchain has diverse applications, including supply chain management, financial transactions, voting systems, and smart contracts. Its decentralized, transparent, and secure nature positions it as a transformative tool for various industries.

Open cv

OpenCV (Open-Source Computer Vision Library) is a widely utilized open-source library designed for real-time computer vision and image processing. Originally developed by Intel and now maintained by the OpenCV community, it offers a comprehensive array of tools and algorithms for managing various visual data tasks. OpenCV supports multiple programming languages, including C++, Python, and Java, making it adaptable and accessible across different development environments.The library encompasses functionalities for image and video analysis, object detection, feature extraction, and machine learning. It enables tasks such as facial recognition, motion tracking, and image enhancement, and it integrates seamlessly with other machine learning frameworks and deep learning libraries, such as TensorFlow and PyTorch.OpenCV is widely adopted in academic research, industry applications, and hobbyist projects, thanks to its extensive capabilities and active community support. It provides a robust set of functions for image manipulation, geometric transformations, and data visualization, equipping developers with the necessary tools to build advanced computer vision applications. Its efficiency and flexibility make OpenCV a valuable resource for anyone involved in computer vision and image processing.

V. DATABASE DESIGN

Database design is a fundamental aspect of software development, serving as the cornerstone for effective data management. At its core, a database is a collection of interrelated files designed for real-time processing, containing vital data for problem-solving and enabling concurrent access by multiple users. The primary goal of database design is to facilitate easy, cost-efficient, and flexible data access for users.The design process involves defining and specifying the structure needed for the client/server system. Business objects, which represent information visible to system users, must be accurately modelled. A well-designed database should be normalized to ensure data integrity and efficiency.A Database Management System (DBMS) is essential for protecting and organizing data separately from other resources such as hardware and software. It provides features that distinguish it from other data management tools, notably the separation between logical data (how data is presented to programs)and physical data (how it is stored on storage devices).

Login

Field Name	Data Type	Size	Constraint	Description
Username	Varchar	12	Primary key	Username
Password	Varchar	12	Not null	Password of user
userid	int	4	Not Null	User identification
address	varchar	50	Not Null	Public key of user
status	int	4	Not Null	Status of user

Wregister

Field Name	Data Type	Size	Constraint	Description
wid	int	4	Primary key	wallet Identification
wuname	Varchar	30	Not Null	Wallet username
wpass	varchar	30	Not Null	Wallet password
Mobile	varchar	30	Not Null	Mobile number
wdate	varchar	30	Not Null	Path of fingerprint
email	varchar	30	Not Null	Email ID
phrase	varchar	50	Not Null	Phrase of wallet
Waddress	varchar	30	Not Null	Public key
Status	int	4	Not Null	Status of wallet
cstatus	varchar	10	Not Null	Security status

Bank

Field Name	Data Type	Size	Constraint	Description
sid	int	4	Primary key	Bank Identification
Bwname	Varchar	30	Not Null	Wallet username
accno	varchar	30	Not Null	Account no
bname	varchar	30	Not Null	Bank Name
branchname	varchar	30	Not Null	Bank branch name
Bisfc	varchar	10	Not Null	Bank ISFC code
Name	varchar	30	Not Null	Name of bank user
sdate	varchar	30	Not Null	Sending date
amount	decimal	10	Not Null	Bank amount

DOI: 10.48175/IJARSCT-19434

wamount	decimal	10	Not Null	Wallet amount
Wcoin	int	4	Not Null	Wallet balance coin
scoin	int	4	Not Null	Selling coin

Transcation

Field Name	Data Type	Size	Constraint	Description
transid	int	4	Primary key	Transaction identification
suname	varchar	30	Foreign key	Sender username
senderpublic	varchar	30	Not Null	Sender public key
senderprivate	varchar	30	Not Null	Sender private key
runame	varchar	30	Foreign key	Receiver username
recieverpublic	varchar	30	Not Null	Receiver public key
amount	decimal	10	Not Null	Transaction Amount
mfee	int	4	Not Null	Miner fee
Status	int	4	Not Null	Transaction status
tdate	varchar	10	Not Null	Transaction date
blockid	int	4	Not Null	Block Identification

usertable

Field Name	Data Type	Size	Constraint	Description
userid	int	4	Primary key	User identification
name	varchar	30	Not Null	Name
phone	varchar	30	Not Null	Phone
mailid	varchar	30	Not Null	MailID
address	varchar	30	Not Null	Address
username	varchar	30	Foreign key	Username
password	varchar	15	Not Null	Password

accounts

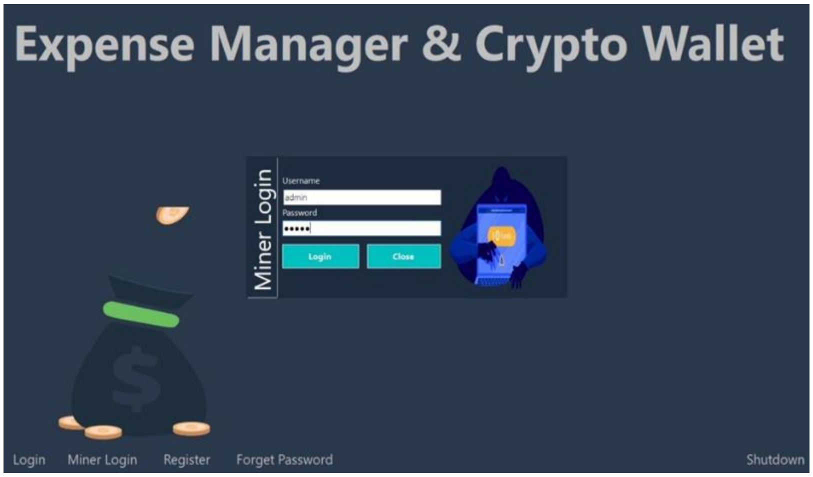
Field Name	Data Type	Size	Constraint	Description
tid	int	4	Primary key	Transcation identification
userid	varchar	30	Foreign key	User Identification
date	varchar	30	Not Null	Date
month	varchar	30	Not Null	Month
category	varchar	30	Not Null	Category
amount	decimal	30	Not Null	Amount
concernperson	varchar	30	Not Null	Concern Person
comments	varchar	100	Not Null	Comments
type	varchar	30	Not Null	Type

VI. FUTURE WORK

The privacy and smart contract based distributed ledger management system is proposed in future. The future approach will be deployed in a Hyperledger based payment portal and the steps followed in the deployment are discussed. The business network was developed with the REST APIs and the angular JS based application. The results would show the improved and effective payment management with the blockchain based cryptocurrency management.

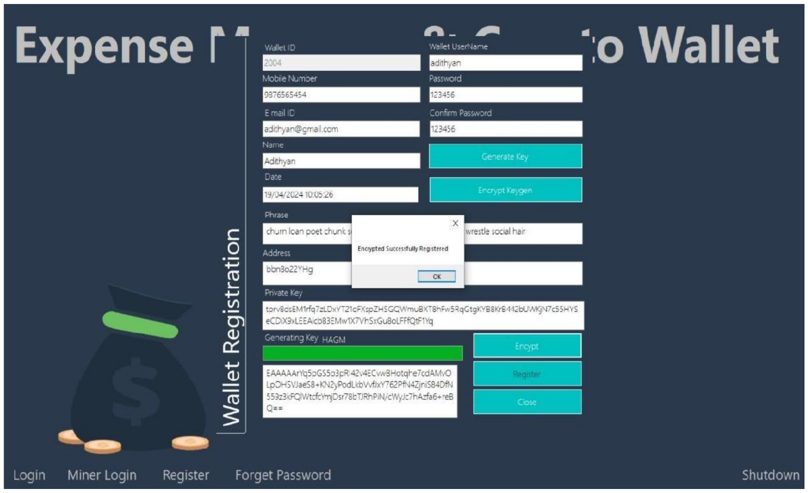
VII. RESULT

Miner Login



Username: admin
Password: •••••

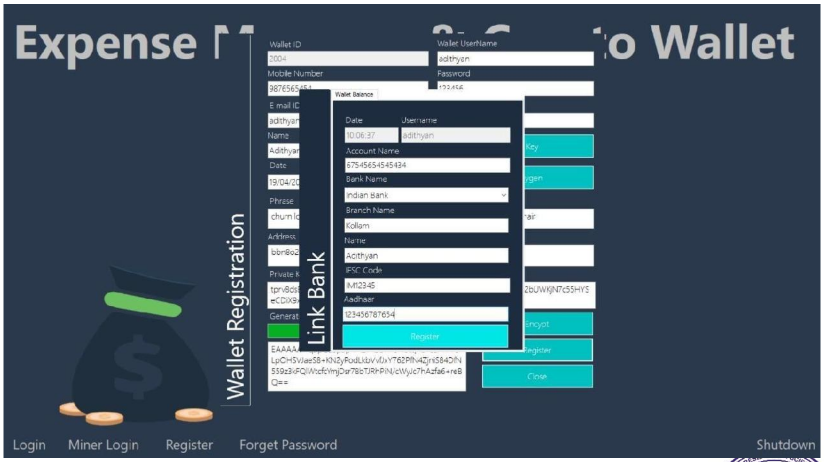
Wallet Registration



Wallet ID: 2004
Wallet UserName: adithyan
Mobile Number: 9876565454
Password: 123456
E mail ID: adithyan@gmail.com
Confirm Password: 123456
Name: Adithyan
Date: 19/04/2024 10:05:26
Phrase: churn loan poet chunk s … wrestle social hair
Address: bbn8o22YHg
Private Key: tprv8dsEM1rfq7zLDxYT21cFXspZHSGQWmuBXT8hFw5RqGtgKYB8KrB442bUWKjN7c55HYS eCDiX9xLEEAicb83EMw1X7VhSxGu8oLFFfQtF1Yq
Generating Key HAGM
EAAAAArYq5pGS5p3pRi42v4ECvwBHotqhe7cdAMvO LpOHSVJaeS8+KN2yPodLkbVvfJxY762PfN4ZjniS84DfN 559z3kFQlWtcfcYmjDsr78bTJRhPiN/cWyJc7hAzfa6+reB Q==

Encrypted Successfully Registered

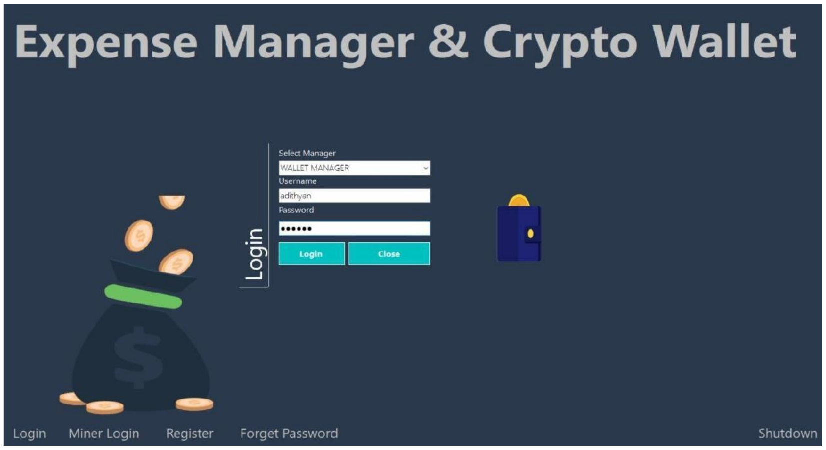
Link Bank



Date: 10:06:37
Username: adithyan
Account Name: 67545654545434
Bank Name: Indian Bank
Branch Name: Kollam
Name: Adithyan
IFSC Code: IM12345
Aadhaar: 123456787654

DOI: 10.48175/IJARSCT-19434

Wallet Manager Login



Expense Manager & Crypto Wallet

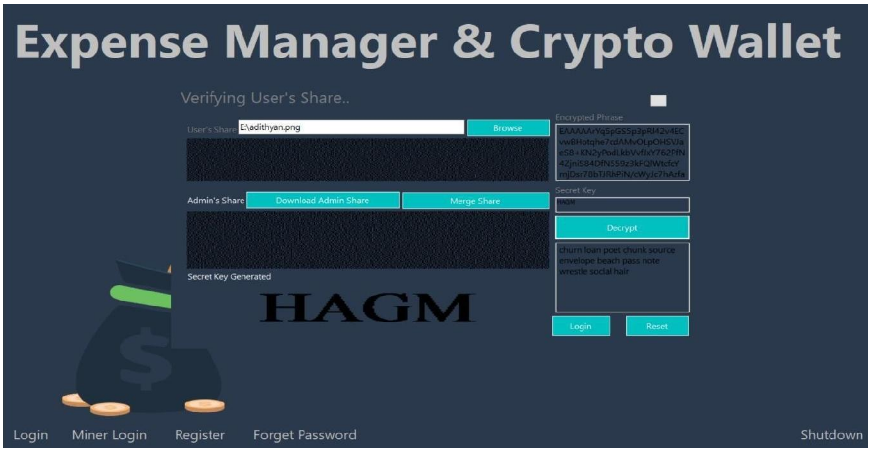
Login

Select Manager: WALLET MANAGER

Username: adithyan

Password: ••••••

Second Level Security



Expense Manager & Crypto Wallet

Verifying User's Share..

User's Share: E:\adithyan.png

Encrypted Phrase: EAAAAArYq5pGS5p3pRJ42v4EC vwBHstqhe7cdAMvOLpOHSVJa eS8+KN2yPodLkbVvfIxY762PfN 4Zjni584DfN559z3kFQlWtcfcY mjDsr78bTJRhPiN/cWyJc7hAzfa

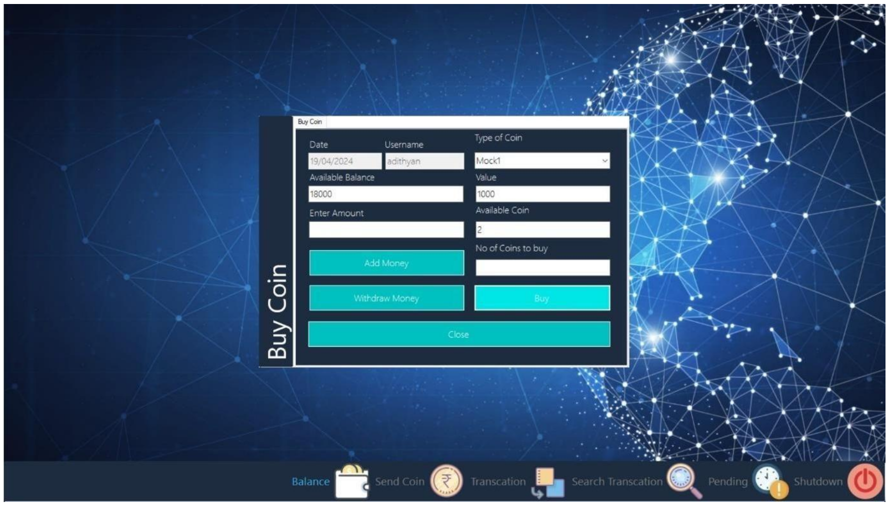
Secret Key: HAGM

churn loan poet chunk source envelope beach pass note wrestle social hair

Secret Key Generated

HAGM

Buy Coin



Buy Coin

Date: 19/04/2024

Username: adithyan

Type of Coin: Mock1

Available Balance: 18000

Value: 1000

Enter Amount:

Available Coin: 2

No of Coins to buy:

DOI: 10.48175/IJARSCT-19434

VIII. SUMMARY

With the rapid increase in the value of cryptocurrencies, there is an urgent need for a tool that can provide a means of using cryptocurrencies securely and efficiently. The main challenge is the gap between the limited memory of human beings and the complex key structures of cryptocurrencies. We propose an effective, usable and secure cryptocurrency wallet management system based on a semi-trusteed social network, herein implementing a HIKE scheme, a secret sharing scheme, a signature scheme and a symmetric encryption scheme as building blocks. We present five protocols under our system, which imply that the system enjoys the properties of security-enhanced storage, portable login on different devices, no- password authentication, flexible key delegation, blind wallet recovery, etc The blockchain based payment wallet management exhibited the anonymity of transactions while maintaining the authenticity of the user with the distributed ledger management system

REFERENCES

[1] Hyperledger Composer - Create business networks https://hyperledger.github.io/composer

[2] Creating Cryptocurrency - https://medium.com/coinmonks/create-your-own-cryptocurre ncy-in-ethereum-blockchain-40865db8a29f

[3] Confidential Transactions by Gregory Maxwell-https://people.xiph.org/~greg/confidential_values.txt

[4] Digital Currencies by Bank of International Settlements, Committee on Payments and Market Infrastructures - https://www.bis.org/cpmi/publ/d174.pdf

[5] Mahdi H. Miraz and Maaruf Ali, "Blockchain Enabled Enhanced IoT Ecosystem

[6] Security,"proceeded in First International Conference on Emerging Technologies in Computing 2018 (iCETiC '18), London.

[7] Pilkington, Marc, Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and MajlindaZhegu. Edward Elgar, 2016. Available at SSRN: https://ssrn.com/abstract=2662660.

[8] K.Christidis and M.Devetsikiotis, ―Blockchains and smart contracts for the internet of things, IEEE Access, vol. 4, 2016, pp. 2292–2303.

[9] V. Buterin, ―On Public and Private Blockchains, 2015, Available: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains.

DOI: 10.48175/IJARSCT-19434