Decentralized Wallet Application using Blockchain

Khetesh Choudhary[1]; Afiya Dhanse[2]; Mandavi Dubey[3]; Yash Kushwaha[4]; Prof. Anand Ingle[5]
[1,2,3,4]B. E Graduate(IV year), Department of Computer Engineering, MGMCET, Maharashtra, India

Abstract:- Decentralized applications (DApps) are gaining significant traction due to the widespread adoption and development of blockchain technology. These applications receive substantial funding through crowdfunding, reflecting the growing interest in their potential. Despite this, there remains ambiguity surrounding their definitions, architectures, and classifications. This survey seeks to address these gaps by offering a comprehensive exploration of DApps for further investigation.

Decentralized Applications, are software programs that typically include front-end interfaces, smart contracts for automation, and decentralized protocols for data storage and communication. Analyzing popular DApps reveals their varied functionalities, advantages, and challenges, showcasing the potential for decentralized technologies to reshape industries. Lastly, the survey outlines recent research problems concerning DApps, focusing on economics, security, and performance. It identifies promising avenues for future research in this domain.

Keywords:- *Blockchain, AWS, Android Studio, Flutter, React-Native.*

I. INTRODUCTION

Centralized digital wallets, which rely on traditional financial intermediaries, often fall short in terms of security. These wallets are vulnerable to hacking, fraud, and mismanagement, putting users' digital assets at risk. Additionally, they necessitate alevel of trust in third-party entities, raising concerns about control and privacy. The complexities associated with blockchain technology also hinder its widespread adoption, making it difficult for everyday users to take advantage of the benefits itoffers. Given these issues, there is a pressing need for decentralized walletapplications. These wallets can provide users with control, security, and transparency over their digital assets, reducing reliance on centralized financial institutions and addressing the trust and security concerns inherent in traditional wallets. To achieve this overarching aim, the project has set severalspecific objectives. First, the project will entail in-depth research and analysis of various blockchain platforms to determine the most suitable one for wallet development. Subsequently, the team will design and develop the decentralized wallet application, with a strong focus on creating an intuitive user interface. In terms of security, robust features, including private key management and encryption, will be implemented. Rigorous testing will be conducted to ensure the wallet's functionalityand security. User experience and feedback will be assessed to drive iterativeimprovements. Furthermore, the project will include a comparative evaluation of the decentralized wallet's performance and security in relation to traditional centralized alternatives. Ultimately, the project aims to provide recommendations for the future development and adoption of decentralized wallet applications, helping to bridge the gap between blockchain technology and mainstream financial services.

II. EXISTING SYSTEM

First and foremost, user-friendliness remains a challenge, as the intricacies of managing private keys and addresses can be intimidating, especially for non-technical users. Additionally, the lack of account recovery options poses a significant risk; if users lose their private keys or wallet access, they may face the irreversible loss of assets. Scalability issues on certain blockchain networks can affect transaction speed and cost, potentially hampering the efficiency of decentralized wallets for everyday use. While decentralized wallets offer increased security through user-controlled private keys, this also places the responsibility of safeguarding keys entirely on the users, leaving their assets vulnerable if keys are lost or stolen.

Furthermore, the level of customer support for decentralized wallet applications is generally limited, making issue resolution or assistance a challenge for users. The need for users to manage multiple wallets for different cryptocurrencies due to limited support and the lack of standardized user protections are other drawbacks.

Moreover, the irreversibility of blockchain transactions and ongoing regulatory uncertainties contribute to the limitations of decentralized wallet applications. Lastly, concerns related to user privacy and the need for extensive user education further compound the challenges in achieving mainstream adoption of these wallets. Addressing these limitations is crucial to enhance the accessibility, security, and user-friendliness of decentralized wallet applications for a wider user base.

III. LITERATURE SURVEY

The research paper provides a comprehensive overview of decentralized applications (DApps) in blockchain ecosystems. It delves into the various types of DApps, the blockchain platforms they operate on, and the challenges associated with their development and deployment. The paper explores security, privacy, and the role of smart contracts in DApps. It also offers insights into use cases and future trends. Thissurvey serves as a valuable resource for understanding the foundations and complexities of DApps, providing essential guidance for the development of a decentralized wallet application in the blockchain.

In this research paper, we can extract valuable insights to enhance the security and investigative capabilities of our wallet application. Consider integrating the data visualization techniques and investigative tools discussed in the paper to help users track and analyze their wallet transactions more effectively. This could offer users a deeper understanding of their wallet activity, enhancing transparency and security.

This research paper is a valuable resource for our project on a decentralized blockchain wallet application. We can use insights from this paper to bolster the security and privacy aspects of our wallet application. By doing so, our wallet application can offer users an enhanced level of security and privacy for their transactions. These techniques allow for increased anonymity and strong protection of transaction details,aligning perfectly with the principles of decentralization and security within the blockchain ecosystem.

IV. PROPOSED SYSTEM

This Proposed system is designed to address the limitations of existing solutions while prioritizing user-friendliness, security, and functionality. To enhance user-friendliness, the system will feature an intuitive and accessible interface, making it user-centric to cater to both blockchain enthusiasts and those less familiar with the technology. In tackling account recovery challenges, it will implement a robust and secure mechanism, potentially utilizing multi-factor authentication or social recovery to ensure users can regain access to their wallets in the event of key loss. Scalability issues will be mitigated by supporting multiple blockchain networks and utilizing off-chain or layer-2 solutions to optimize transaction speed and cost-efficiency for a wide range of use cases. Advanced securitymeasures, such as hardware wallet integration and biometric authentication, will fortify user asset protection.

Additionally, responsive customer support, comprehensive asset support, user protections, and transaction verification mechanisms will collectively enhance user trust and satisfaction. To address transaction reversibility, the system will introduce features for transaction verification, reducing the risk of accidental or malicious transfers. Privacy concerns will be tackled with options for coin mixing and transaction obfuscation, ensuring user anonymity when needed. Moreover, the systemwill provide extensive educational resources, guides, and tools to empower users withblockchain knowledge and maximize their proficiency in utilizing the wallet.

V. METHODOLOGY

A. Gather Knowledge:

In the creation of cryptocurrency applications, blockchain technology is essential. A blockchain is a series of blockchain ledger that are connected via a cryptologic and contain digital information (data). The main goal of employing it is to make it possible to share sensitive data safely.

B. Using Open-Source Libraries:

The majority of crypto currencies are free to use. So, we don't need to get started from the bottom. We used free resources and programs that are already out there, such as the Coinbase SDK or the Bitcoin J SDK. The Java library Coinbase SDK is cross- platform. It aids in the development of Bitcoin wallets for both iOS and Android. Thislibrary also supports a wide variety of widely used languages, like Python, Java, Ruby, etc. The Bitcoin J SDK includes thorough documentation and is simple to use. Additionally, Bitcoin J is JVM-compatible and supports its language ecosystem, including C++, JavaScript, Ruby, Python, etc.

C. Using APIs:

A Bitcoin wallet software with plenty of features may be created by utilizing APIs. You can synchronize your cryptocurrency wallet with the blockchain ecosystem using a distributed ledger API. You may select from the most well-liked APIs listed here: Coinbase, Bitcore, SimpleSwap, and Factom. Your development team may quickly perform the required processes using the APIs, accelerating the development of the project.

D. Blockchain Platform Selection:

The first crucial decision was to select the appropriate blockchain platform for the wallet. Ethereum was chosen due to its widespread adoption and robust smart contract capabilities. Ethereum wallets serve as applications empowering users with control over their accounts. Analogous to a physical wallet, they encompass all essential elements to authenticate identity and manage assets. With a wallet, users can access applications, review balances, execute transactions, and verify their identities seamlessly.

E. Choosing the Right Stack:

Your app will succeed if the appropriate technological stack is used. For instance, we have used Flutter to create an application. Java or Kotlin are the two options for developing native Android apps. Swift or Objective-C are also options foriOS apps.

F. Integration with Blockchain:

A back-end system was developed to interact with the Ethereum blockchain. This included APIs for transaction processing, balance queries, and smart contract interactions.

G. Activate Security:

When developing Bitcoin wallet software, security is of the utmost importance. You should make sure your cryptocurrency app has top-notch security because of this. Consider using 2FA, which uses hardware authentication, face ID, and fingerprints, to bolster the security of the crypto wallet app. The creators are responsible for ensuring ongoing security upgrades. They must swiftly locate any bugs and other security vulnerabilities and resolve them utilizing the most recent technologies.

H. Get Started on Application Development:

Therefore, when we were ready to begin developing the crypto wallet app, we were sure to do the following steps:

- Choose all of our app's features.
- Assemble our database and write the application code.
- Create a user-friendly, straightforward interface.
- Before releasing our wallet, we will make sure to do thorough tests.

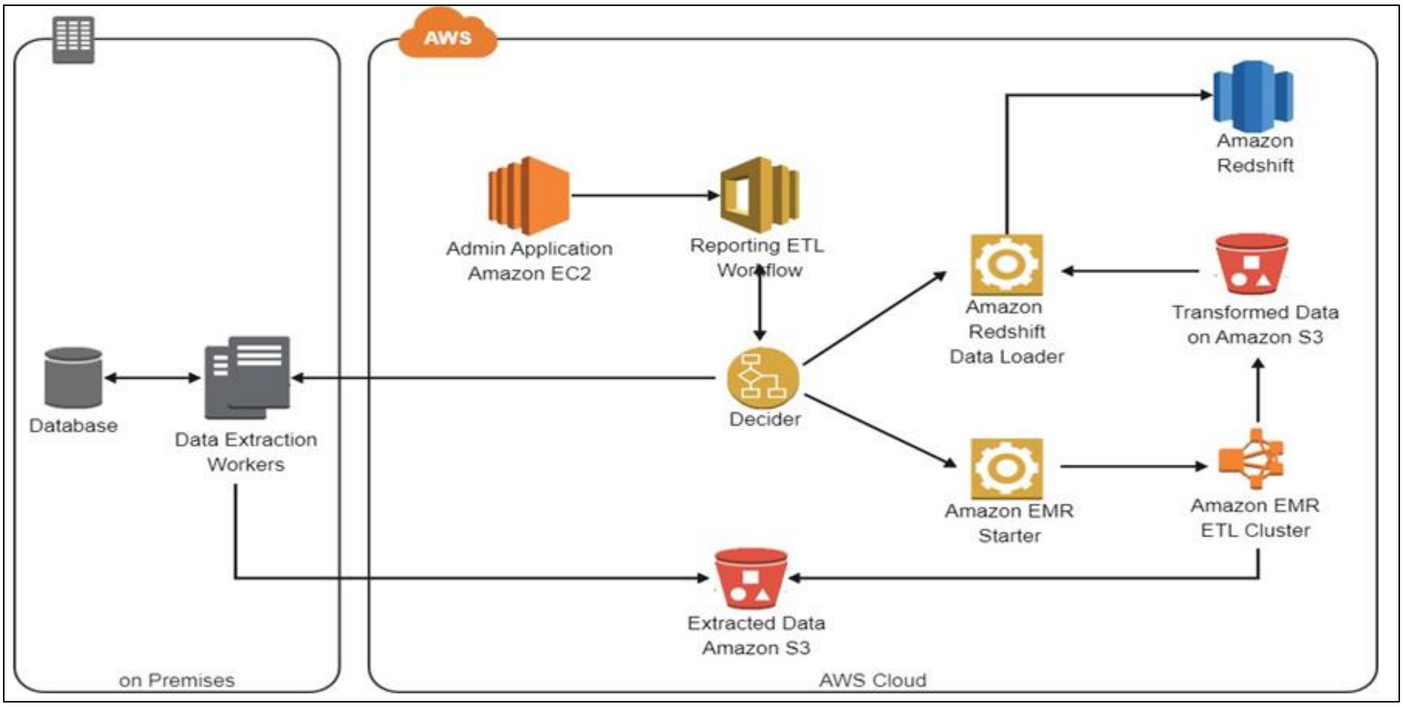


Fig 1: AWS Cloud

VI. SYSTEM DESIGNS

The system begins with a user prompt at the start, inquiring about the amount of Bitcoin stored in the wallet. This initial question serves as a means of understanding the user's current cryptocurrency holdings. Following this, the flowchart diverges intotwo paths, asking whether the user is willing to purchase a wallet.

The first path involves the choice between a mobile wallet or a web wallet. This decision primarily hinges on the user's preferred mode of access and convenience. A mobile wallet offers on-the-go access through a smartphone app, while a web wallet is accessible through a web browser on various devices.

The second path offers the option of a hardware wallet, which is known for its enhanced security features. Users can select this option if they prioritize maximum protection for their digital assets. This choice may depend on the user's risk tolerance and the overall security posture of their cryptocurrency holdings.

The system also accounts for the user's internet connection status, providing options for both online and offline storage. Online storage implies that the wallet is connected to the internet, while offline storage means the wallet operates without a constant internet connection. This choice often revolves around the user's security preferences, with offline storage considered more secure due to its reduced exposure to potential online threats.

In summary, the system facilitates a user's decision-making process when it comes to decentralized wallet applications. It tailors the wallet choice to the user's current Bitcoin holdings, willingness to purchase a wallet, preferred mode of access, and the level of security they desire based on their choice of a mobile, web, or hardware wallet, as well as their internet connection status. This comprehensive approach addresses a range of user needs and security considerations in the realm of cryptocurrency storage.

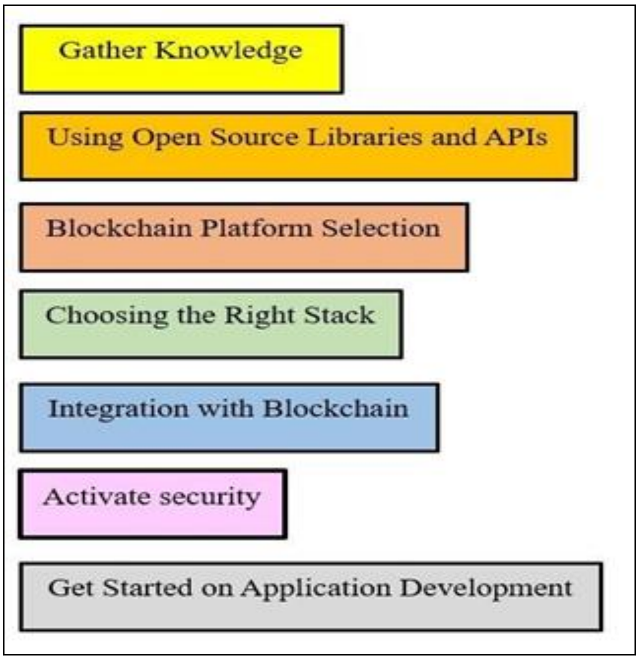

Gather Knowledge
Using Open Source Libraries and APIs
Blockchain Platform Selection
Choosing the Right Stack
Integration with Blockchain
Activate security
Get Started on Application Development

Fig 2: Methodology for the Project

VII. DATABASE

Every application necessitates a repository for storing data gathered from users, devices, and the application itself. Databases serve as critical backend systems, facilitating the storage, management, updating, and analysis of data across various applications, ranging from small-scale back-office systems to large-scale mobile and consumer web applications with global reach. To construct an application enabling users to monitor their digital asset balances across multiple blockchains, it's imperative to host a web application that is publicly accessible and capable of accommodating users connecting their digital asset wallets to the application. Figure 4 depicts the architecture diagram, showcasing the core AWS services and components constituting the digital asset portfolio tracker sample application.

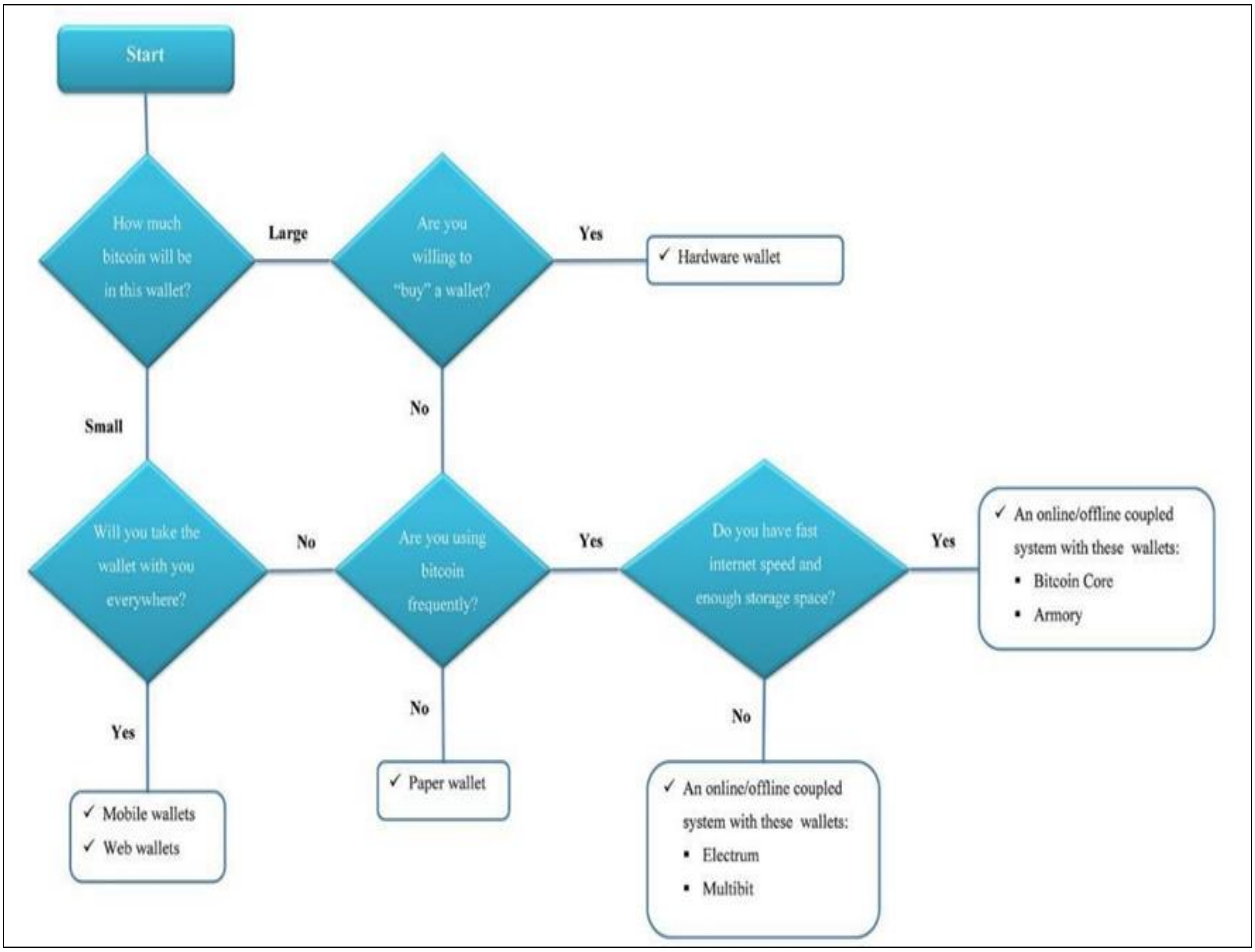
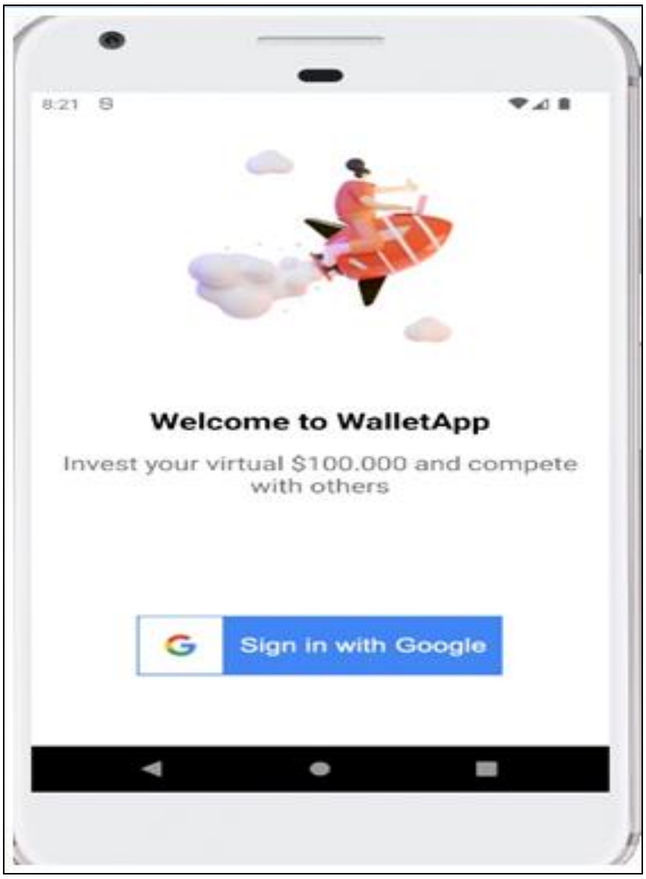

Start
How much bitcoin will be in this wallet?
Large
Are you willing to "buy" a wallet?
Yes
✓ Hardware wallet
Small
No
Will you take the wallet with you everywhere?
No
Are you using bitcoin frequently?
Yes
Do you have fast internet speed and enough storage space?
Yes
✓ An online/offline coupled system with these wallets:
▪ Bitcoin Core
▪ Armory
Yes
✓ Mobile wallets
✓ Web wallets
No
✓ Paper wallet
No
✓ An online/offline coupled system with these wallets:
▪ Electrum
▪ Multibit

Fig 3: Database

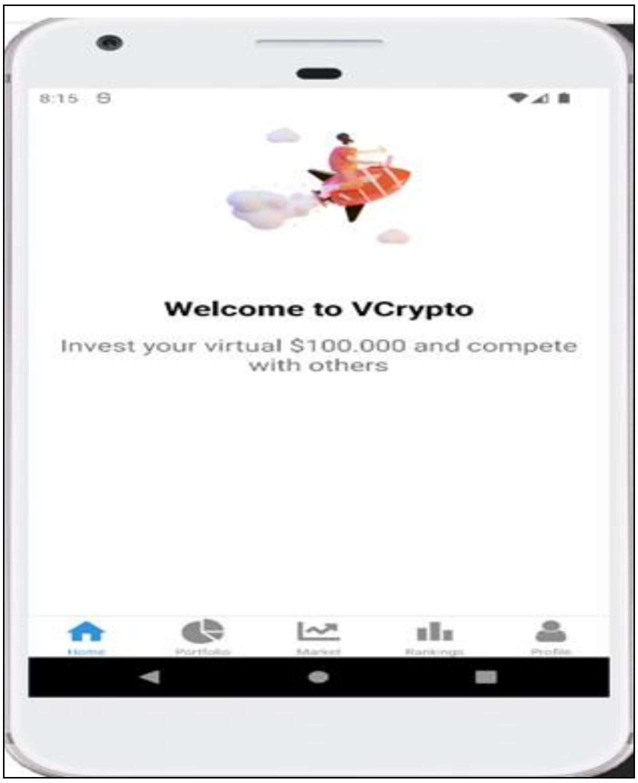
VIII. RESULT



Welcome to WalletApp

Invest your virtual $100.000 and compete with others

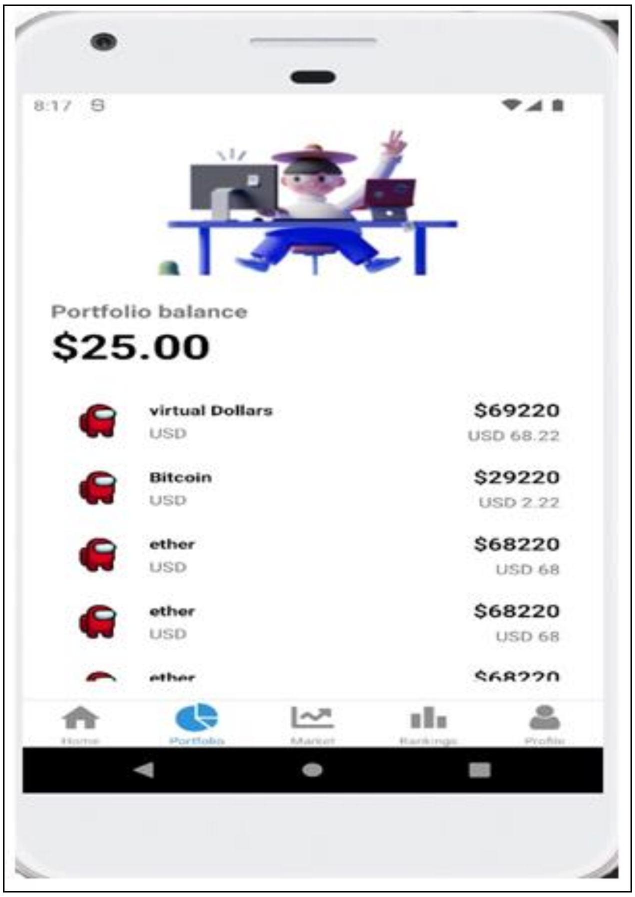
Fig 4: Welcome Page



Welcome to VCrypto

Invest your virtual $100.000 and compete with others

Fig 5: After Login

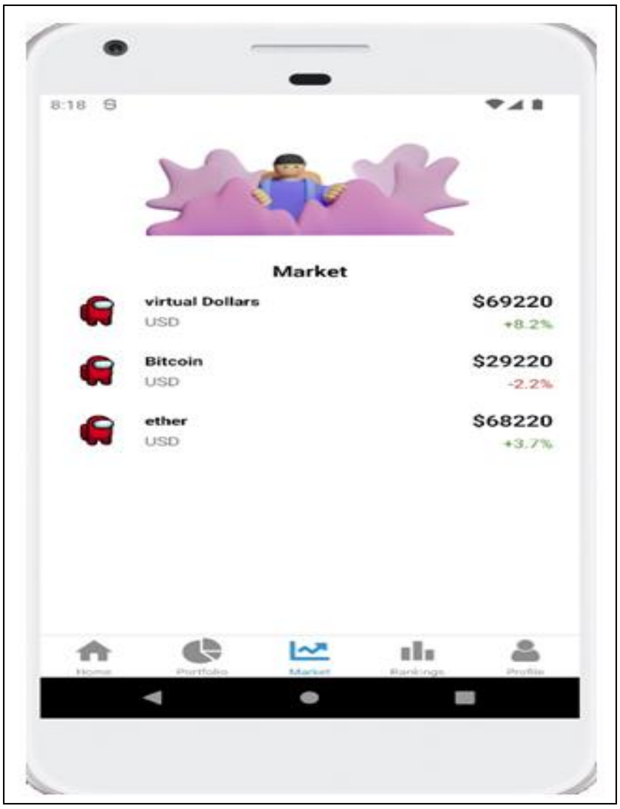


Portfolio balance

$25.00

virtual Dollars USD	$69220 USD 68.22
Bitcoin USD	$29220 USD 2.22
ether USD	$68220 USD 68
ether USD	$68220 USD 68
ether	$68220

Fig 6: Portfolio Balance of the Logged-in User

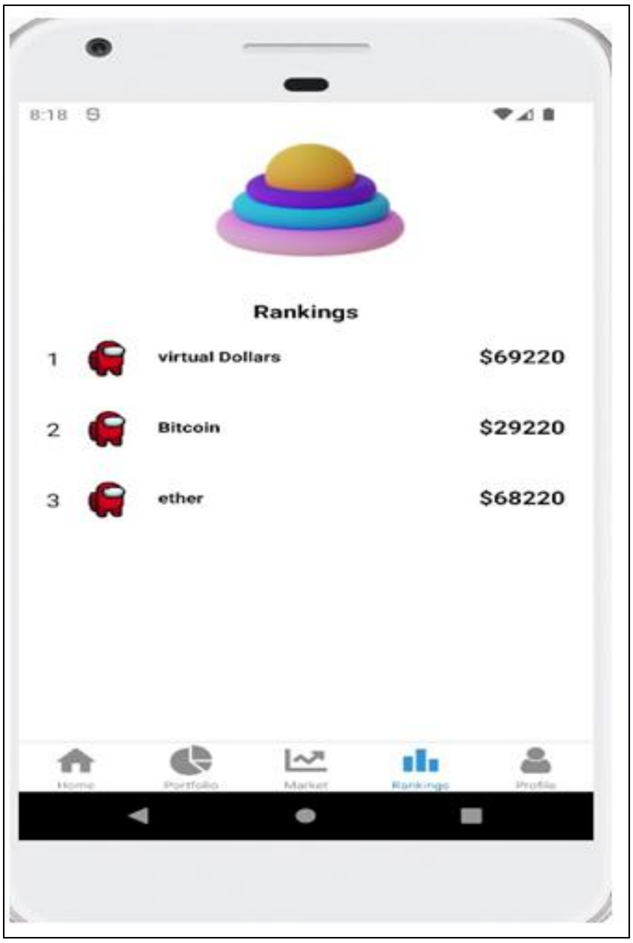


Market

virtual Dollars USD	$69220 +8.2%
Bitcoin USD	$29220 -2.2%
ether USD	$68220 +3.7%

Fig 7: Market Value

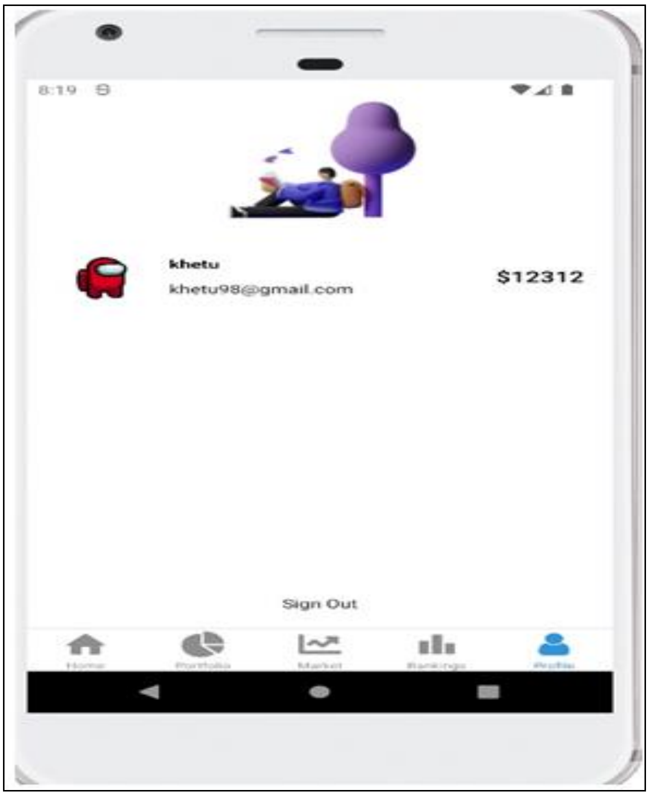
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2082



Rankings

1	virtual Dollars	$69220
2	Bitcoin	$29220
3	ether	$68220

Fig 8: Rankings



khetu
khetu98@gmail.com
$12312

Fig 9: Profile of Logged-in User

IX. FUTURE SCOPE

In the future we will implement an android application that will provide the users to access trading features of the cryptocurrency that has been added. Security of the app will also be checked and more security will be provided. Furthermore, the user interface will also be improved so if there exists any complication that will be solved. Latest conversion rates that calculate transaction fees based on ever-changing conversion rates. A payment gateway integrated for users to buy or sell the assets efficiently.

In the current landscape, cryptocurrency exchange platforms emerge as prime hubs for initiating cryptocurrency trading, offering a rich resource for cryptocurrency enthusiasts and traders. These platforms provide the convenience of trading various cryptocurrencies within a single interface and have the capability to integrate numerous cryptocurrencies seamlessly.

While the crypto-world boasts millions of crypto coins, around 700+ are actively traded globally. Among these, prominent options like Bitcoin, Ethereum, Litecoin, NEM, and others present lucrative investment prospects. For traders, especially early adopters and supporters of Bitcoin, venturing into the cryptocurrency exchange platform realm can serve as a promising startup opportunity, facilitating access to a diverse range of investment options and potential growth avenues.

X. CONCLUSION

It is anticipated that the utilization of digital wallets for cryptocurrencies will surge, leading to a significant decline in the reliance on physical wallets. Notably, Bitcoin and Ethereum, the frontrunners in the crypto sphere, are achieving unprecedented profit records, gradually cementing their status as legitimate currencies. Research findings suggest that these wallets not only offer robust security but also entail minimal additional costs compared to traditional physical currency transactions.

Transactions conducted via cryptocurrencies incur minimal expenses due to the direct interaction between the two executing nodes, bypassing the need for intermediary involvement. The only associated cost pertains to the payment to the network facilitating the transaction, such as the Bitcoin network. While transaction fees vary based on the transaction speed, they are substantially lower than those in conventional payment systems.

Furthermore, it's evident that each exchange platform presents distinct advantages and disadvantages. Some prioritize user-friendliness, while others emphasize advanced trading features. Presently, there's a burgeoning interest in commencing cryptocurrency businesses, driven by the allure and profitability of crypto coins. Individuals are increasingly drawn to cryptocurrency trading and exchange platforms, recognizing the potential for lucrative returns. Forecasts indicate that the cryptocurrency trading and exchange marketplace could outpace the growth witnessed in 2018, with the trading volumes of major cryptocurrencies poised for exponential expansion in the future.

REFERENCES

[1]. Blockchain-Based Decentralized Application : A Survey, IEEE 13 March 2023.

[2]. Secure Deterministic Wallet and Stealth Address, IEEE 5 September 2022.

[3]. A Visualization System for Bitcoin Wallet Investigation, IEEE March/April 2023.

[4]. Analysis of Cryptocurrency Wallet 03 September 2019.

[5]. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, Accessed: Apr.15, 2023. [Online].Available: https://bitcoin.org/ bitcoin.pdf

[6]. MetaMask, "MetaMask browser extension,"Accessed:Apr.15,2023.[Online]. Available:https://github.com/MetaMask/metamask extension

[7]. Li et al., "A survey on the security of blockchain systems," Future Gener. Comput. Syst., vol. 107, pp. 841–853 2017.

[8]. DAppRadar, DApp Industry Report, Aug. 2022. [Online]. Available: https://dappradar.com/blog/dappradar-blockchain-industry-reportaugust-2022

[9]. Wikipedia, "Initial Coin Offering," Accessed: Apr. 15, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Initial_coin_offering.

[10]. D. Mingxiao et al., "A review on consensus algorithm of blockchain," in Proc. IEEE Int. Conf. Syst., Man, Cybern., 2017, pp. 2567–2572.

[11]. G. Foroglou and A. L. Tsilidou, "Further applications of the blockchain," 2015, Accessed: Apr. 15, 2023. [Online]. Available: https://www.researchgate.net/publication/276304492_ Further_applications_of_the_blockchain

[12]. C. Sillaber and B. Waltl, "Life cycle of smart contracts in blockchain ecosystems," Datenschutz und Datensicherheit-DuD, vol. 41, no. 8, pp. 497–500, 2017.

[13]. V. Buterin, "Ethereum white paper," 2013. [Online]. Available: https://ethereum.org/whitepaper/

[14]. Binance Smart Chain, "Binance Smart Chain." Accessed: Apr. 15, 2023. [Online]. Available: https://github.com/binance-chain/bsc

[15]. EOSIO, "Technical White Paper v2," Accessed: Apr. 15, 2023. [Online]. Available: https://github.com/EOSIO/Documentation/blob/ master/Technical

[16]. TRON, TRON Website, Accessed: Apr. 15, 2023. [Online]. Available: https://tron.network/

[17]. Fantom, Fantom Website, Accessed: Apr. 15, 2023. [Online]. Available: https://fantom.foundation/ [18] Polygon, Polygon Website, Accessed: Apr. 15, 2023. [Online]. Available: https://polygon.technology.