

Decentralized Crypto Wallet Tracker

Prof. Abhijeet More
dept. Master of Computer
Application
Pillai HOC College Of
Engineering And
Technology, (Mumbai University)
Rasayani
Maharashtra, India
abhijeetdmore242@gmail.com

Prof. Tejashree Patil
dept. Master of Computer
Application
Pillai HOC College Of
Engineering And Technology,
(Mumbai University) Rasayani
Maharashtra, India
ptejashree2024@gmail.com

Deep Kharate
dept. Master of Computer
Application
Pillai HOC College Of
Engineering And Technology,
(Mumbai University) Rasayani
Maharashtra, India
deepkharate36@gmail.com

M P Akhil
dept. Master of Computer
Application
Pillai HOC College Of
Engineering And Technology,
(Mumbai University) Rasayani
Maharashtra, India
akhilunni335@gmail.com.

Somanath Pratapure
dept. Master of Computer
Application
Pillai HOC College Of Engineering
And Technology, (Mumbai
University) Rasayani
Maharashtra, India
pratapuresomnath20@gmail.com.

Abstract— As the multi-chain digital assets, decentralized finance (DeFi) and non-fungible tokens (NFTs) seeing rapid development, cryptocurrency portfolio management is causing strong pain among users. With the growing number of blockchain networks like Ethereum and a variety of chains, users commonly have assets across multiple wallets, protocols and dApps. Classic portfolio tracking services often require the constant relationship between client and server, with centralized servers, offering heavy privacy issues and security implications. Manual and account based access Many of these systems require data to be manually entered or employees to sign in with their accounts, which opens up the possibility for data leaks, inaccurate reporting, and divulgence of sensitive financial information. More centralized trackers unfortunately have a very poor understanding of more advanced DeFi functions such as staking, joining liquidity pools, and yield farming positions, total or just plain token approval permissions leading to either incomplete or worse yet misleading asset summaries. To solve the above issues, this system suggests a completely decentralized cryptocurrency portfolio tracker on client-side. The code utilizes APIs like Alchemy, Zapper and CoinGecko to read real-time token balances, NFTs creatures or positions (for DeFi), and allowances from the current network directly off-chain. Being exclusively client side, the tracker does not rely on centralized databases and it is designed to minimize privacy compromises. The built-in on-chain security module is its most noticeable feature, as it detects any potentially malicious or extremely large token approvals given to smart contracts. Suspicious approvals can be detected, and then revoked in a timely manner through signed wallet transactions without needing to reveal any private keys. The results show that this decentralized tracker would provide significantly better user privacy, data accuracy and overall security. As a serverless applications service, that bypasses central authentication, as well as database storage, it offers a transparency, user-centric and scalable way to manage digital assets securely.

Keywords— Cryptocurrency, Blockchain, Portfolio Tracking, Wallet Security.

I. INTRODUCTION

Blockchain technology has evolved digital banking by facilitating distributed, trust less and transparent transactions

through distributed ledger systems [7]. They have been staking, lending, providing liquidity trading NFTs and participating in governance in multiple decentralized applications as the DeFi world has exploded rapidly. While such advances make blockchain networks more practical, they also complicate the management of diverse digital assets and introduce new security challenges, most notably in connection with malicious smart contracts and token approvals [10].

Traditional BTC portfolio trackers run on centralized systems and involve manual input of records as they were designed way back when the concept of blockchain technology was new into popular lexicons. Especially in scenarios which demand the real-time DeFi analysis, works including Yadav et al. [1] and Patil et al. [3] proved that centralized trackers induce privacy attack, preserves outdated information, and it is not automated. React-based market analysis tools in [4], [6] provide global markets overview, but do not support monitoring for multi-assets or searching for on-chain wallets, which hinders the portfolio visibility for users.

Previous studies have 3 decentralized ecosystems. According to Conti et al. [7], looked closely at security in bitcoin wallets are vulnerable to signature exploits, phishing assaults, and authentication threats. Chen et al. [10] investigate DeFi protocol vulnerabilities in further detail, particularly those related to token approvals, where users unintentionally give smart contracts authorization to move money. Attackers can empty wallets even in the absence of user activity because these approvals are perpetually active unless specifically cancelled.



Figure 1. Decentralized crypto wallet

However, due to the above security concerns, automated approval tracking and revoke facilities are left out in most of today's systems. In addition, most trackers break blockchain privacy rules by storing sensitive information on the central server: user profiles, wallet addresses and portfolio (balances) [1], [7]. The lack of decentralized and privacy-preserving answers to aggregate tokens, NFTs, or DeFi positions are a significant research gap.

Currently we have client side only, decentralized crypto wallet tracker which can fetch real time blockchain data through APIs such as Alchemy API, Zapper API, CoinGecko in left panel to solve this type of issue. The proposal includes a powerful security query module to identify and revoke dangerous grants, irrelevant back-end databases are eliminated, and full client-side computing ensures the user's right to privacy. The platform provides a secure, scalable and accurate solution for current digital asset management due to its on-chain analytics service and decentralized design.

II. BACKGROUND

The rising difficulty in tracking bitcoin assets using various types of, wallets, protocols, and asset classes is increasingly becoming difficult with the evolving technology of blockchain and decentralized finance. There were problems in the early stages of portfolio management too. concerning accuracy, privacy, and scalability, which were the result of being developed on top of web applications in a centralized manner. This called for manual entry by some level of discipline to keep the information updated [1], [2], [3], storing the login credentials for access to the third-party server. Some research studies have been done on the API-based crawling of the cryptocurrency market, such as CoinGecko [4], [5], [6], which have been presented however, they lacked wallet integration and crawling by price. The focus in the design of the aforementioned works was on authentication and access security aspects; thus, it did not consider attacks like malicious contracts and dangerous token approvals etc., post-authentication in our study as well as in some other researches on decentralized applications and wallet architectures [7], [8]. Even though, few recent DeFi security works have surfaced analyzing attack vectors and protocol-level vulnerabilities. These did not come with any tools that had a user interface that let users aggregate assets and check wallet risks in real-time [9], [10]. This makes a

need for an entirely decentralized, client-side wallet tracking system, which will help the end-user keep active security controls along with DeFi and NFT exposure while also ensuring on-chain data retrieval with autopiloted assistance.

III. MOTIVATION

The general motivation of the study is that present-day cryptocurrency portfolio management systems (system) are centralized and require manual entry of assets users are finally presented with a half up-to-date, incomplete view at their portfolio, which comprised privacy [1], [2], [3]. With the expansion of DeFi systems, users commonly interact with smart contracts, liquidity pools and NFT platforms; however most current monitoring systems fail to provide full visibility across these assets [4], [5], and [6]. Moreover, recent studies find that substantial number of DeFi losses can be attributed to malicious or excessive token approvals behind wallet login rather than private key compromise [7], [8]. However, There isn't enough of practicable and user centred solutions to help users continually be aware about on-chain assets at stake or the post-authentication real-time change for security despite wide-ranging research with respect to wallet structures and DeFi vulnerabilities [9], [10]. The gap presented here is addressed by implementing a decentralized, client-side wallet tracker ensuring privacy, automatization of asset aggregation and allowing end users for active security controls.

IV. LITERATURE SURVEY

1) *Tracking and Managing of Cryptocurrency Wallet*

Rajesh Kumar Yadav et al. proposed a MERN stack-based cryptocurrency wallet tracking and managing tool which incorporates MongoDB, Express, ReactJS and NodeJS. js in monitoring the portfolios on the web [1]. The platform enables users to monitor their crypto holdings and visualize market trends with an up-to-the-second price feed fetched from the coin-gecko API. Through melding frontend interactive tools and backend data processing, the platform offers a more structured setup for people to manage their digital assets. The app also makes it very easy to keep track of your participation in a simple web interface with token balances, price changes and valuation summary. This work is advantageous in practical utility of full-stack web technologies for crypto tracking, and is current and simple to deploy. The work provides an example of the possibility to exploit web software frameworks for effective cryptocurrencies e-management. It also helps to clarify how API integration facilitates real-time financial tracking. It is a basic use case for how portfolio tracking apps can design and implement in popular DevOps tools.

2) *CryptoDomains: Building a Decentralized Domain Marketplace*

Sheetal Phatangare et al. launched the CryptoDomains DApp which allows users to purchase and sell domain names stored on a blockchain using NFT (non-fungible token) standards [2]. Smart contracts and MetaMask integration enables

transparent transfers of ownership without intermediaries. The platform provides on-chain secure and verifiable domain ownership using ERC-721 token standards. This work demonstrates the potential of DApps for handling DID assets with utilizing blockchain. One of the main advantages of this study is proving fully decentralized execution environment for smart contracts with wallet-based authentication. This research demonstrates the capability of network technology such as blockchain to take over traditional domain management systems making direct peer-to-peer ownership transfer possible. Also, it enriches the understanding of NFT-asset management in decentralized applications. The project demonstrates applied use of Ethereum based development and is a practical reference for safe and transparent digital ownership.

3) *Cryptocurrency Portfolio Management (Altfolio)*

Dr. S. T. Patil et al. built Altfolio, a web application for cryptocurrency portfolio management that utilises React as the frontend framework and Firebase for backend [3]. It allows them to track in real-time their cryptocurrency holdings with current price information and historical performance graphs. The app dynamically links to market APIs for instantaneous value updates and portfolio summaries. This work makes puzzles to user-friendly crypto management concentrating explicit visualization and asset arrangement. A structured dashboard and graphical representation make investment monitoring easy on the platform. Another key point in the work is that it focuses on usability and interactive data visualization serving to make users more involved at cryptocurrency managing. The research also discusses how cloud-based backend-services can facilitate portfolio applications. It shows a practical way to combine frontend frameworks with real-time data APIs to create useful financial trackers.

4) *Cryptocurrency Tracker Using ReactJS*

P. Nandini et al. presented a cryptocurrency tracking app written with ReactJS. This also aims to display the real-time market information such as; prices rankings and chart [4]. The application collects data from public APIs to report recent cryptocurrency market trends for users. "The application will increase user awareness by the means of interactive charts and search features. This study can prove that lightweight web technology is able to well process real-time data visualization. One of the main achievements of this work is showing large scale cryptocurrency data naturally and interactively. The site enhances user visibility toward price changes and market cap variations. It also demonstrates how API-oriented applications may be used for financial analysis without a bulky infrastructure plate. This paper helps to improve transparency and accessibility of crypto markets information.

5) *Cryptocurrency Tracker for Real-Time Market Analysis*

S. Rajesh et al. presented a technology to analyze cryptocurrency markets in real-time by observing market trends and price fluctuations with ReactJS and external APIs

[5]. The software application analyzes short and long-term market activity to identify volatility and price momentum. With the use of images and graphic techniques, informed trading is fostered. This study emphasizes the need for real-time monitoring in digital markets. One significant thing we'd like to mention about this research paper is allowing us to provide a real-time market data in a 24/7 basis due to the responsive web-design. The software is interactive and users can process data easily. It's an example of how sophisticated web frameworks can manage high frequency financial data feeds. The paper contributes to better understanding of real-time financial analytics in cryptocurrency.

6) *Crypto-Currency App Using React*

A. Sharma et al. presented Coin Track, another cryptocurrency tracking system based on React and Redux for real-time price analysis [6]. It is a state managed environment combined with tools to organize the manipulation of data and user interaction. It now has structures for application architecture so it can perform well when the market changes. This study emphasizes the significance of frontend optimization for financial applications. Another contribution of this work is the ability to demonstrate effective state management in cryptocurrency monitoring applications. Using Redux has several benefits in terms of application stability and data consistency. The application is responsive and user-friendly. This work helps remembering scalable frontend patterns in crypto monitoring apps.

7) *SoK: Cryptocurrency Wallets—Security Review*

M. Conti et al. introduced a Systematization of Knowledge on secure cryptocurrency wallet, providing taxonomies for wallets architecture and authentication methods [7]. We classify wallets by storage type, access form and security model, offering a systematic view of wallet security design. The research explores the threats and defensive measures for digital wallets. One of the important contributions of this paper is to provide a comprehensive theoretical framework in which previous knowledge can be classified and synthesized. It is a fundamental reference for the study of wallet security models. The study backs future explorations of secure wallet based applications, and contributes in their architecture pattern definition. It also makes an important contribution to academic literature on security of cryptocurrency wallets.

8) *A Survey on Blockchain Wallet Systems*

V. Singh et al. studied the design of blockchain wallets, including different types of wallet, methods for key management and related security concerns [8]. The paper offers an in-depth comparison between the three most common types of wallets: hardware, software, and web-based wallets. The study provides insights to the understanding of wallet traits and risk factors in block-chain affiliated asset storage. The primary novelty of this work lies in its comparison across different types of wallets and how they operate. The questionnaire can help researchers and developers to sample suitable wallet forms for various purposes. It contributes to theoretical background of

blockchain wallet infrastructures. The research also highlights best practices in digital asset management.

9) Security Checklist for DeFi Projects

J. Kumar et al. proposed a systematic security checklist for DeFi projects, with an emphasis on smart contract vulnerabilities and approval management [9]. The study also explores the common security threats of DeFi to offer insight into practical assessment standards. The research draws a focus on governance concerns, contract verification mechanisms and permission settings to promote safer DeFi development. One of the main advantages of this paper is its structured way for determining and classifying risks. Developers can consider network protocol safety in terms of a checklist. It is helpful to improve security awareness in the design of decentralized application.

10) Attack Vectors in Decentralized Finance

L. Chen et al. studied the different attack surfaces in decentralized finance like flash loan attacks and oracle attacks [10]. The work includes detailed discussions on how these attacks are launched and vulnerabilities are abused in smart contract ecosystems. Analysing real-life incidents, the analysis provides key learnings on emerging DeFi threat vectors. One important feat of this work is that it includes a realistic analysis of real attack situations. The research is instrumental in bettering the understanding about protocol-level vulnerabilities. It provides the stronger design strategy for decentralized system security, and promotes financial risk awareness in blockchain ecology.

11) SoK: DeFi Attacks

L. Zhou et al. presented a detailed SoK study of the attacks in decentralized finance (DeFi), and studied several real-world security incidents where large amount of financial losses were caused [11]. The paper classifies types of DeFi attacks as smart contract vulnerability, governance attack, oracle exploit, and liquidity-based. Through a systematic organization of practical case studies and historical exploit data, authors deliver an organized taxonomy on how decentralized financial systems are attacked and help researchers and developers make sense of these attacks. The paper unveils shared aspects within attack strategies and reveals vulnerabilities in protocol design and implementation. A key benefit of this work is its extensive empirical study performed at a large-scale using real-life incidents and not theoretical considerations. The taxonomy provided by our structured classification model can be utilized to identify risk layers in DApps. It also deepens academic understanding as well as practical insights on DeFi security issues. What's next? The study also offers a solid stepping stone towards improving the security of decentralized financial markets by defining how and where such bugs ultimately surface. This fact turns this paper into high value resource for researchers and developers in the field of blockchain security.

12) Security Aspects of Cryptocurrency Wallets

A. Bartel et al. ceEvenhagesystematically surveyed the security aspects related to cryptocurrency wallets including threat models, attack surfaces and protection mechanisms of digital assets storage[2]. The work considers various categories of wallets such as Hardware Wallet, Software wallet and Web Wallet; it analyses the security features in different scenarios. The work offers a comprehensive view of wallet security threats by considering technical vulnerabilities and user-triggered (risk). The authors outline the common ways of attacking: phishing, malware, key leakage and unauthorized usage, as well as prevention measures and defense technologies. One important strength is that the scope of wallet-related threats is covered along a range of dimensions. The study structures complex security topics in such a way that it is straightforward to see how wallet systems can be improved. It also points out the research vacancy and future confrontation in protecting a wallet in order to encourage innovation with secure management of digital asset. This work is a fundamental work for the wallet security design improvement and user protection enhancement in blockchain systems.

V. EXISTING SYSTEM

People can currently display their crypto assets and monitor all profits they generate. It would be tiring and tedious work manually listing all your crypto assets. Creating an account with the intention of storing your wallet information on distant servers raises significant security and safety worries. These tools are great for being able to see the cryptocurrency market and track changes, however, they don't let you see an accurate and real time price value of your portfolio. This is because there is an aggregate value that is usually pulled from public APIs. The existing tools, as we found through previous works, tend to sacrifice decentralization in favor of convenience and fails to keep pace with the dynamic nature of blockchain-based assets [1], [3]. As they don't query directly on the blockchain, current trackers cannot sense for user holding changes (or positions / nfts / risks) on Post Execute on behalf of users. So, users are lead to make poor investment decisions due to discrepancies in their true on-chain asset allocation and the summary provided by centralized platforms.

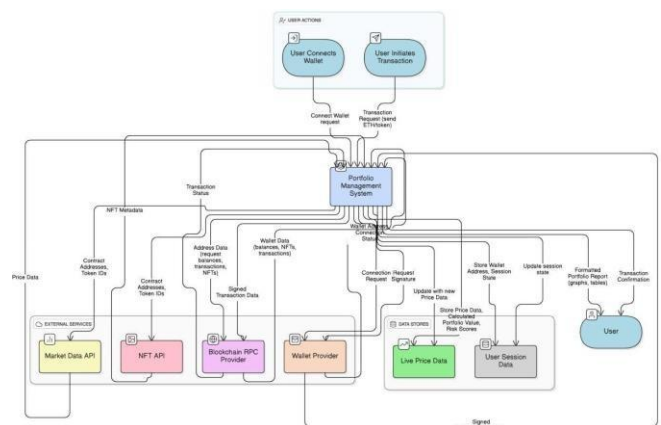


Figure 2. System Architecture

The existing trackers are incapable of automatically recognizing user activity changes. The downsides caused by centralization impact not just usability but also the security and privacy of users. These will be talked about in detail below: Usability costs in most applications, either detection or classification is not in real time; periodic adaptation steps are required, which in some cases may be manual or automatic. These approaches contradict the very foundation of the blockchain technology, since they claim to be decentralized with the capability to manage user information but retain wallet addresses and user information on centralized servers [8],[12]. Moreover, despite the fact that there is research that has already discovered that token approvals and how smart contracts interact with one another is fundamentally the core source of losses for the DeFi markets [9],[11], [14], these platforms provide almost no information with regard to such matters. Traditional trackers lack any way to tell the difference between malicious allowance permissions, oil slick smart contract phishing scams, or malicious tokens. These mentioned drawbacks are enough to assert that the current approaches had developmentally failed to encompass the demands of a bitcoin user with considerable expansion into DeFi, NFTs, multi-chains, etc.

VI. PROBLEM STATEMENT

The original design of the classic portfolio trackers is not capable of dealing with the spread of decentralised finance, NFTs, as well as inter-wallet interactions. A vast number of portfolios are reliant on human processing and the central systems that produce gaps, outdated, and incorrect data of a portfolio [1], [4]. Usually, a person manages dozens of assets on multiple dApps, lending protocols, as well as liquidity pools. It is a pressing problem to have a solution that can pull on-chain data in real time from user wallets - without relying on third-party databases- as the static and centralised nature of legacy tracking tools no longer suits the decentralized, thrustless reality of blockchain technology. It's even harder to manage assets because it's NOT automated; The user has to note token balance, NFT ownership, DeFi yield and Monitor deals manually. This is not a viable option as blockchain ecosystems grow in complexity and scale.

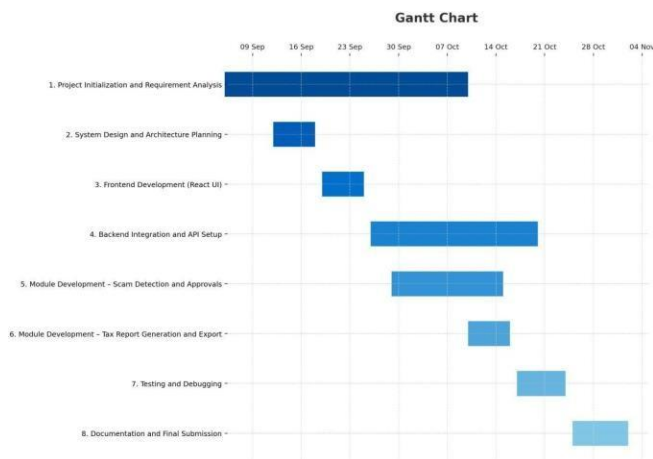


Figure 3. Gantt chart

The shortcomings evident in current systems are serious security vulnerabilities and functionality limitations. Unsecured token approvals and interacting with smart contracts in a way that is not clear is among the attacks at the level of wallets that these people who use cryptocurrencies have suffered serious financial losses because of [9], [11], [14]. But traditional portfolio trackers don't try to evaluate and alert us about why approval might be dangerous. Also, without on-chain security auditing, customers still don't know about the risks that come with their own wallets. Moreover, core blockchain characteristics, including user control and decentralization, are disrupted due to centralized wallet meta-data storage, which, apart from undermining data privacy [7] and aside from the data leaches violations of [12], [16], weakly sensitive data. As there isn't an overall security solution feasible and appropriate to protect these people within a perspective decentralization due to loss of practicability for assets tracking, something more was required.

VII. PROPOSED SYSTEM

To overcome the fails of the current centralized portfolio management derivatives, a non-custodial client-based approach called Decentralized Crypto Wallet Tracker is introduced. The proposed approach leverages the Web3 stack to track wallets and retrieve token balances, DeFi positions and NFT ownership in real time from the blockchain itself measured against legacy system that are account-based on top of centralized databases. Since no sensitive information is stored off-chain, this design ensures full decentralization, privacy and data integrity. It allows everyday users to invest across any number of protocols without a need for human input, by using the API integration to source on chain data and real time market prices. Such decentralized automation approach is congruent with the guidelines of previous works that emphasize on the need of real-time engagement over blockchain and better usability features in bitcoin tools. [3], [8], [15].

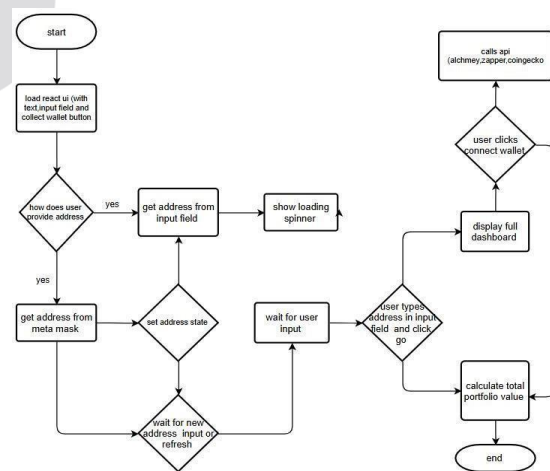


Figure 4. Control Flow of System

The proposed solution does not stop only at asset aggregation but introduces powerful wallet-level security, including identifying and assessing token approvals made to smart contracts. It has been shown in Prior research that one of the most common causes of irregular asset transfers in DeFi systems are malicious, or unnecessary approvals [9],[11], [14]. My proposed solution would alert people to such potentially damaging permissions, and pull in approval data from the blockchain itself to throw of that fear. Furthermore, it provides a valuable protection against the unknowns risks by giving users the power to revoke such approvals with no effective and secure blockchain mechanism. To help better inform trading decisions, it also includes visual analytics, retrieving transactions history and scam token identification mechanism. The proposed system is a comprehensive solution that capture real time characteristics of blockchain network, suit today's requirements of transparency, security and user empowerment by combining the decentralized conception with automatic exploring and integrated computer security analysis.

VIII. METHODOLOGY

To mitigate the limitations of currently available centralized cryptocurrency portfolio trackers discussed in related work so far [1], [2], [3], [4], [5], [6], we base our approach on a decentralized, client-side run process. Through a Web3-based interface via ethers.js, and a user can conveniently link their crypto wallet, like MetaMask It is also useful for privacy purposes, as no account or logging is required. Once connected, data is retrieved independently from user-submitted information on asset value. Alchemy API accesses balances for tokens, access to transaction history and asset or property information, while Zapper API provides information about DeFi-associated data like staking information, liquidity pools, or borrowing. Track Market Price Based on CoinGecko API, Real-time Portfolio Value Dynamic exchange rate tracking and portfolio value computation are implemented through a remote query for CoinGecko exchange rate information for offering pertinent and current information on digital assets for users.

The solution includes an added component of security analysis to find and fix any security problems that may be present and which are encountered through Bitcoin wallet and DeFi security research [7],[8],[9],[10]. Once your wallet is connected this module will search it for approved tokens for smart contracts, which are a common gambling reason to dumb money. With the application of blockchain transaction signature, users can conveniently revoke their dangerous or infinite permissions without needing any intermediary. It has been developed with a React based interface and all data processing, security control, and visualization is done directly in the user's browser. The underlying principle to the vision of decentralization and transparency allows better privacy, improved security and full user control since it does not rely on centralized server or database.

IX. DISCUSSION ANS RESULT

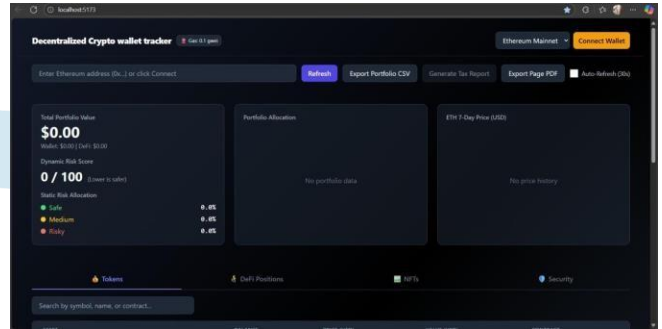


Figure 5. Home Dashboard

This is what the interface looks like when launched, and it gives users an overview of how the dashboard would look like, as well as some of its staple features. It enables you understand how our platform is structured and how it works without any interaction or the necessity to connect with a wallet.

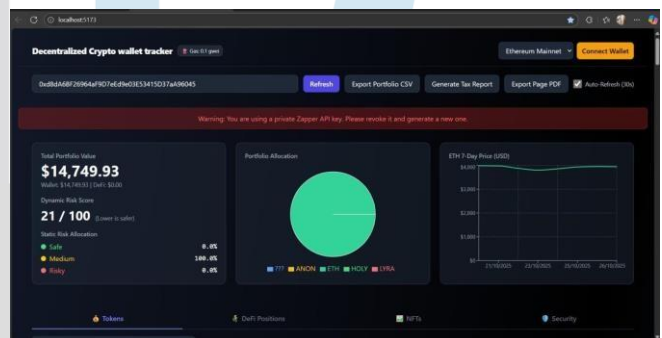


Figure 6. Dashboard Analysis

The image shows the system dashboard, where users link their blockchain related wallet to access account and real-time overview over cryptocurrency portfolio. It offers an extensive overview of token balances, digital assets and on-chain activity in a convenient and intuitive manner.

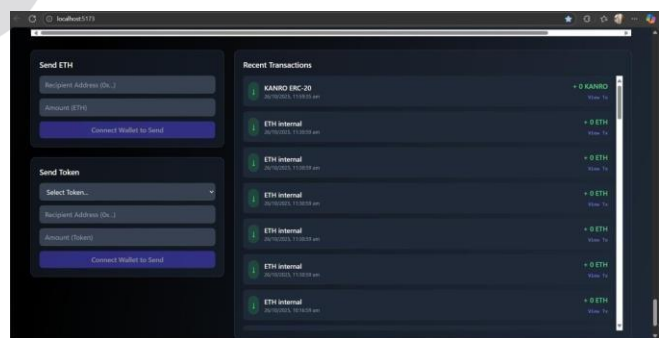


Figure 7. Transaction History Page

This sends cryptocurrency or tokens directly from your connected wallet. It also allows users to trace their transfer history on the chain, providing some good information with high outgoing transaction volumes.

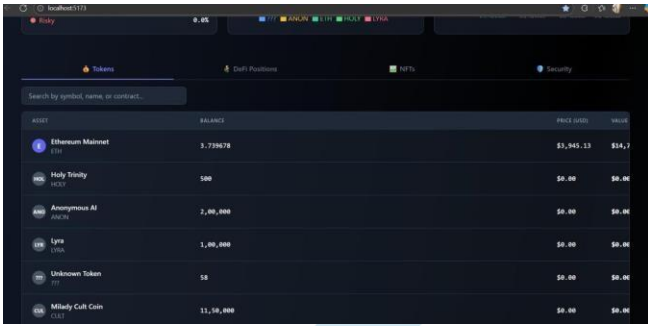


Figure 8. Token Portfolio

This interface also provides a full list of all crypto tokens that are available in the linked wallet. It shows the status of your token in real time (token quantity, market price and total value) so users can be aware of their portfolio at a glance in a simple, clear and organized way.

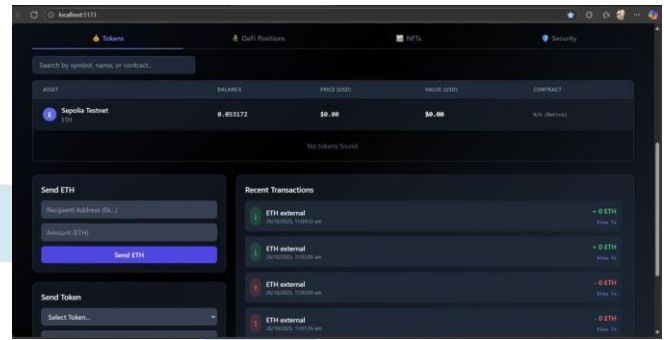


Figure 11. MetaMask Connected Account

Once the user connects their wallet, our application pulls live on-chain data from the Sepolia Ethereum test network in real-time via private API integration. It makes sure the information shown is all current and up to date.

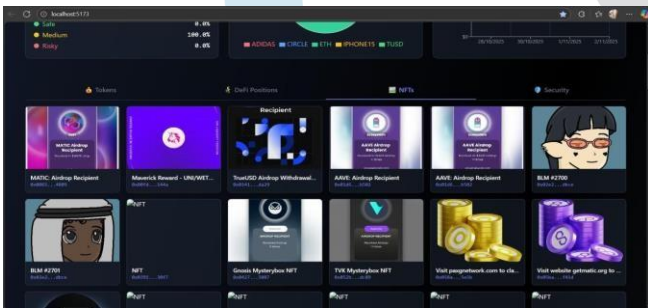


Figure 9. NFT Portfolio

The users can see and manage the NFTs listed in his connected wallet, all neatly laid in a grid layout. Because NFTs are unique digital creations, banked on the blockchain, this screen serves as users' single place to easily check and organize their assets.

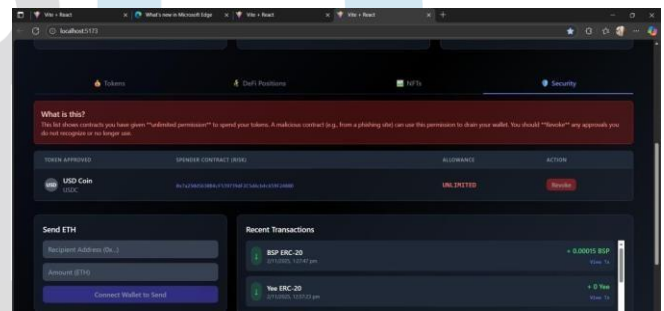


Figure 12. Security and Token Approval and Revocation

This setting looks for token approvals in the wallet to allow 3rd party smart contracts spend without limits. Considering unlimited approvals are often a security risk in DApps, these function should stop that from happening.

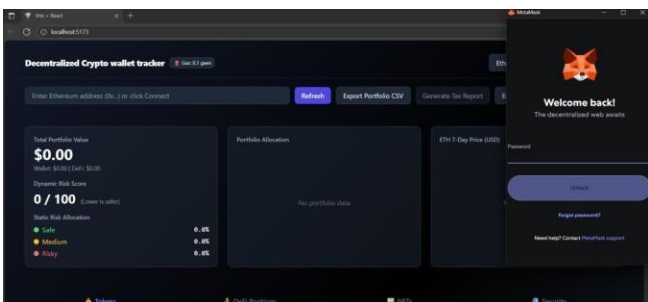


Figure 10. Connection With MetaMask

This is the vital point of connecting my wallet to your dApp securely in this stage. This link also enables the system to monitor users' cryptocurrency holdings and respective on-chains transactions in real time.

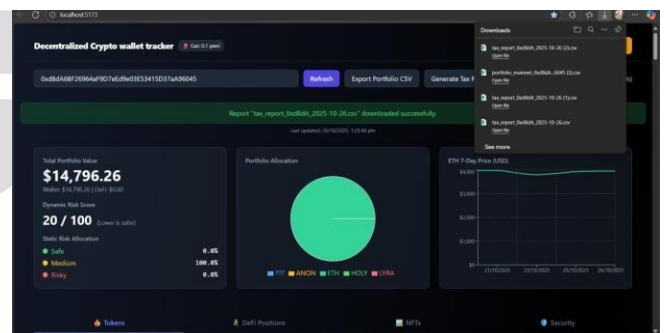


Figure 13. Tax report Generation

This function enables you to create and download a tax report which contains the summary of your cryptocurrency transactions, balances at the current moment, and overall performance of your investments over certain period. It enables the users to review and keep track of their records easily.

X. FUTURE SCOPE

The system can be further augmented by protection using wallet-level advanced security analytics and integration of machine learning based risk prediction and early threat detection. It is also a fully checked multi-chain platform and enhanced in a user-friendly way, which provides intelligent analysis and alerting system for further security and convenience.

XI. CONCLUSION

In this work, we propose a decentralized system to manage blockchain based cryptocurrency portfolios. The system to be provided has been designed to offer better accuracy, privacy, and security than the present reliance on single centralized service providers. It enables users to follow their assets on the blockchain with full custody over their data. With the real-time information and integrated security, the system make user digital assets transparent, secured and easy to handle. As the use of blockchain becomes more widespread, decentralized portfolio trackers with integrated secure features are going to be fundamental in facilitating secure and reliable digital asset management.

REFERENCES

- [1] R. K. Yadav et al., "Tracking and Managing of Cryptocurrency Wallet," IEEE, 2024.
- [2] S. Phatangare et al., "CryptoDomains: Building a Decentralized Domain Marketplace," IEEE, 2024.
- [3] S. T. Patil et al., "Cryptocurrency Portfolio Management (Altfolio)," IJERMCA, 2022.
- [4] P. Nandini et al., "Cryptocurrency Tracker Using ReactJS," IJARST, 2023.
- [5] S. Rajesh et al., "Cryptocurrency Tracker for Real-Time Market Analysis," IJEAST, 2023.
- [6] A. Sharma et al., "Crypto-Currency App Using React," IJPRP, 2023.
- [7] M. Conti et al., "SoK: Cryptocurrency Wallets—Security Review," IEEE Access, 2023.
- [8] V. Singh et al., "A Survey on Blockchain Wallet Systems," SpringerLink, 2022.
- [9] J. Kumar et al., "Security Checklist for DeFi Projects," ACM Digital Library, 2023.
- [10] L. Chen et al., "Attack Vectors in Decentralized Finance," IEEE Transactions on Blockchain, 2023.
- [11] L. Zhou et al., "SoK: DeFi Attacks," IEEE Symposium on Security and Privacy, 2023.
- [12] A. Bartel et al., "Security Aspects of Cryptocurrency Wallets," ACM Computing Surveys, 2023.
- [13] H. J. Lim et al., "Comparative Analysis of Security Features in Digital Asset Wallets," Electronics (MDPI), 2025.
- [14] A. R. Kirobo et al., "Security Vulnerabilities of Cryptocurrency Wallets," FUOYE Journal of Engineering and Technology, 2024.
- [15] K. Biernacki et al., "Comparative Analysis of Cryptocurrency Wallet Management Tools," Journal of Computer Sciences Institute, 2021.
- [16] H. Albayati et al., "A Study on the Use of Cryptocurrency Wallets from a UX Perspective," Wiley, 2021.