B-SAFE: Blockchain Security Assessment Framework Enhanced with Machine Learning *

Ngo Thanh Trung
Troy University
Hanoi, Viet Nam
tngo220196@troy.edu

Pham Thai Duong
Troy University
Hanoi, Viet Nam
dpham220299@troy.edu

Doan Hoang Long
Troy University
Hanoi, Viet Nam
ldoan220279@troy.edu

Pham Tien Dat
Troy University
Hanoi, Viet Nam
dpham220298@troy.edu

Le Quang Huy
Troy University
Hanoi, Viet Nam
hle....@troy.edu

Abstract—**The emergence of the metaverse has initiated a paradigm shift in how individuals interact, socialize, and transact within digital environments. This study explores the evolving architecture of decentralized virtual worlds, emphasizing the integration of blockchain technologies, digital asset ownership, and immersive social experiences. Leveraging empirical data from multiple blockchain-based metaverse platforms, we investigate user engagement metrics, asset distribution patterns, and behavioral trends within gamified ecosystems. Our findings reveal that the incorporation of play-to-earn mechanics, virtual real estate, and avatar customization significantly enhances user retention and economic activity. Moreover, decentralized governance and community-driven development are shown to influence both the scalability and perceived legitimacy of these platforms. By synthesizing insights from computer science, economics, and media studies, this paper provides a multidisciplinary perspective on the dynamics shaping the future of the metaverse. Our work lays the foundation for further empirical investigation and policy formulation aimed at fostering transparent, equitable, and sustainable virtual ecosystems.**

Keywords*—*Blockchain security, machine learning, security assessment, threat detection, consensus mechanisms, smart contracts

I. Introduction

The development of civilization, along with technological advances, brings opportunities such as improved communication and access to information. The metaverse represents an evolving digital ecosystem, where virtual properties hold tangible economic value. This study analyzes Decentraland's real estate market, assessing property pricing trends and market dynamics.

The development of civilization, along with technological advances, brings opportunities such as improved communication and access to information. The metaverse represents an evolving digital ecosystem, where virtual properties hold tangible economic value. This study analyzes Decentraland's real estate market, assessing property pricing trends and market dynamics.

The development of civilization, along with technological advances, brings opportunities such as improved communication and access to information. The metaverse represents an evolving digital ecosystem, where virtual properties hold tangible economic value. This study analyzes Decentraland's real estate market, assessing property pricing trends and market dynamics.

II. Foundations and Vulnerability Landscape

A. *Consensus and Network-Layer Attack Surface*

This subsection surveys consensus-layer and peer-to-peer network vulnerabilities, including 51% attacks, selfish mining, long-range attacks (PoS), validator bribery, and Sybil/Eclipse routing manipulation. Emphasis is placed on enterprise impact, likelihood, and mitigations with citations to academic and industry sources.

B. *Key Management and Wallet Security*

Proper key management is the most important part of security for any blockchain-based system. Even the strongest protocols can fail if keys are not handled correctly [1]. In decentralized systems, private keys give users final control over their digital assets, identity, and ability to perform actions on the blockchain. This idea is often summarized by the saying, "Not your keys, not your coins," but it applies to more than

*__Cite (APA):__ Trung N., Dat P., Long D., Duong P., Huy L. (2025).

just currency [2]. The main tools users have for managing these keys are called "wallets." The security of these wallets is therefore essential for protecting user actions on the blockchain [3]. However, wallet security is not just a technical problem; it also depends on software design and, importantly, on the behavior and understanding of the users themselves [2].

To understand wallet security, it is helpful to first classify the different types of wallets. The most basic classification is between "hot wallets," which are connected to the internet, and "cold wallets," which are kept offline. Hot wallets include desktop software, mobile apps, and web browser extensions. They are easier to use for daily transactions, but their online nature makes them more vulnerable to attacks. Cold wallets, such as hardware devices or paper wallets, offer better security for long-term storage because they are not directly exposed to online threats [3]. Another important classification is based on who controls the keys. With "custodial wallets," a third party like a cryptocurrency exchange holds the keys for the user. This is simpler for beginners, as the experience is similar to online banking, but it requires trusting that the third party is competent and honest. With "non-custodial wallets," users have full control and responsibility over their own keys. These non-custodial wallets can be further divided into traditional Externally Owned Accounts (EOAs) and newer Smart Contract wallets, which allow for more complex security rules [2, 3].

The vulnerabilities in these systems exist at multiple levels, but the most common threats are those on the user's own device [4]. A major technical risk is the improper storage of keys, such as saving them as unencrypted plaintext in the device's memory, where they can be stolen by malware. Flaws in the wallet software, such as insecure interfaces or the use of buggy code libraries, also create significant risks. This is not just a theoretical problem; real-world attacks often exploit these weaknesses. For example, weak key generation methods like "brain wallets," which use simple, memorable phrases, are a critical vulnerability. The low entropy of human-generated phrases makes them easy to guess, and one study found that most such wallets were drained of funds in less than 24 hours [4]. At the institutional level, the history of exchange hacks like the infamous Mt. Gox incident shows that even large platforms can have critical flaws [4]. More recently, the collapse of the FTX exchange served as a powerful reminder of counterparty risk—the danger that the trusted third party will fail due to mismanagement or fraud, leading to a total loss of user funds [2]. Even at an individual level, social threats are a major risk; one study documented a user who lost all their funds simply because they let a friend see their login details during the wallet setup process, highlighting the dangers of misplaced trust [2].

To protect against these threats, both technical and user-driven defense methods are used. The main technical defense is to use cold storage, such as hardware wallets, to keep keys offline and safe from online hackers [3]. More advanced solutions include multi-signature and smart contract wallets, which allow for programmable security rules like spending limits or requiring multiple people to approve a transaction [2]. However, since many attacks target the user, user-driven strategies are just as important. A common and effective strategy is "risk diversification," where users spread their assets across multiple wallets. For instance, a user might keep a small amount of "spending money" in a convenient mobile hot wallet, while keeping the majority of their savings in a more secure cold wallet [2]. They also use different wallets for different tasks, for example, using a dedicated wallet with minimal funds for interacting with new or risky dApps. For high-value transactions, many users prefer a PC setup because they can use third-party security extensions, like Fire or Revoke.cash, which simulate transactions and warn them about malicious smart contracts before they sign [2].

We can see these security trade-offs in the real-world systems that users choose. Centralized exchanges like Coinbase offer a simple user experience that is similar to online banking. This makes them popular with beginners, but it comes with significant counterparty risk, as tragically demonstrated by the failure of FTX [2]. Hardware wallets like Ledger or Trezor represent the opposite approach. They provide high security by giving users full control over their offline keys, but they can be difficult to use and require the user to be fully responsible for their own security. This trust model has also been challenged recently. For example, Ledger's controversial "Recover" service, which proposed storing shards of a user's seed phrase with third parties, caused a backlash because it went against the core reason users chose a hardware wallet: to be the sole holder of their keys [2]. As a middle ground, new systems like smart contract wallets (e.g., Argent) are emerging. They try to offer the best of both worlds: strong security features like social recovery to prevent key loss, combined with an easier user experience that often removes the need to manually manage a seed phrase. These different models show that the market is still searching for the right balance between security, usability, and trust [2].

C. *Smart Contract Vulnerabilities*

This subsection synthesizes findings on reentrancy, authorization flaws, integer over/underflow, timestamp dependence, oracle manipulation, delegatecall misuse, and upgradeability pitfalls. We contrast static, dynamic, and formal verification approaches and summarize audit checklists.

D. *DeFi Protocol Risks*

Decentralized Financial ecosystem (DeFi), is built based on blockchain platforms such as Ethereum, has emerged as an alternative to Centralized Finance due to its transparency, traceability, and decentralized nature. DeFi offers a wide range of financial services, primarily implemented through smart contracts. However, the rapid growth of DeFi has also come with serious security risks, leading to significant financial losses. While blockchain technology itself is considered secure due to its properties such as immutability and consensus mechanisms, the applications and additional layers built on top of blockchain – namely DeFi protocols – are not entirely secure and can be vulnerable.

Many recent works have systematized DeFi into layers (network, consensus, smart-contract, protocol, auxiliary services) and emphasized that many incidents arise from unsafe dependencies between protocols and off-chain services (oracles, centralized relays, bridges) [5]. Among them, vulnerabilities in the DeFi protocol layer (PRO Layer) are often related to design flaws or financial market manipulation. For instance, pricing mechanisms, slippage, liquidation mechanisms, rebases… or invalid assumptions about token standards can be catastrophic when contracts are composed together; in particular, external dependencies are called directly without consistency checks are the source of many real-world failures. [5]

A key economic risk is flash loans, uncollateralized lending mechanisms in an atomic transaction. Flash loans have opened a new attack vector where an attacker can temporarily borrow large amounts of capital to manipulate the market or price feed, performing a series of profit and debt repayment operations in the same transaction. Attacks like Harvest, PancakeBunny, Beanstalk... [5, 6] show that flash loans lower the cost barrier to attack and make small design issues become financial catastrophic. Another risk directly related to off-chain backends is that when price data sources are manipulated – through source changes, on-chain update attacks, or updater compromises – key parameters such as liquidation prices or collateralization ratios can become distorted, leading to mass liquidations or systemic profiteering [6]. There are mitigations such as multiple source aggregation, medianizers, or latency mechanisms that exist but carry trade-offs in latency, centralization and fault tolerance [5, 6].

In addition, transaction ordering and MEV (Miner/Maximal Extractable Value) issues allow sequencers or miners to order, insert or remove transactions to maximize profits – this mechanism gives rise to front-running, sandwiching and other mining strategies, which directly impact the stability of the protocol's financial invariants [5]. Expanding the functional space with cross-chain bridges also creates a new attack surface: many bridges rely on centralized signing/organizations, and bridge crashes have led to large scale asset losses, demonstrating a clear trade-off between cross-chain utility and security risk [6]. Finally, operational and human risks – including private key, mismanagement (privileged keys, weak multisig...), compromised front ends, and implement flaws (not pure protocol design flaws) have a direct impact on asset security and are often present in real-world incidents [7].

To mitigate these risks, incident studies and analysis have proposed a multilayer set of measures: protocol design that considers both economic attack scenarios (game-theoretic stress testing) and defense mechanisms such as circuit breakers [5]; oracle enhancements using aggregations, delayed updates or reputation-based models [6]; MEV mitigations using transparent sequencers or close-chain relay [5]; along with audit, formal verification and real-time monitoring (e.g., oracle mutation detection) with response options as emergency halts [5, 6]. Each approach carries trade-offs in performance, latency, and decentralization, so the choice of solution should be based on the specific application context.

Finally, the systematic analysis revealed important research gaps: the lack of a comprehensive quantitative framework for protocol economic risk (incorporating TVL, liquidity depth, oracle latency, and flash loan capabilities), the lack of a common fault tolerant architectural pattern for trustless backends, and the lack of dependency analysis tools for complex composability environments – these gaps share the research direction needed to improve the robustness of DeFi protocols in the broader blockchain landscape.

E. *Exchange and Infrastructure Attacks*

This subsection covers centralized exchange compromise patterns, API key abuse, withdrawal bypasses, hot/cold wallet segregation failures, and infrastructure supply-chain risks. We incorporate regulatory and compliance impacts for enterprises.

III. Methodology

This section outlines the methodology employed in this study to analyze Decentraland's real estate market. The approach includes data collection, analysis techniques, and the frameworks used to interpret the findings.

IV. Results and Analysis

This section presents the findings from the analysis of Decentraland's real estate market. The data collected includes property prices, transaction volumes, and market trends over a specified period. The results are categorized into several key areas:

V. Discussion

This section discusses the implications of the findings from the analysis of Decentraland's real estate market. The trends observed in property pricing and market dynamics provide insights into the evolving nature of virtual economies. The study highlights how virtual properties can mirror real-world economic principles, influencing investment strategies and market behavior. The findings suggest that as the metaverse continues to grow, understanding these dynamics will be crucial for stakeholders, including investors, developers, and users. The analysis indicates that factors such as location, property features, and market demand play significant roles in determining property values. Additionally, the impact of external events and technological advancements on the virtual real estate market is discussed. The discussion also addresses the limitations of the study, such as the reliance on available data and the challenges of analyzing a rapidly evolving market. Future research directions are proposed to enhance the understanding of virtual real estate markets, including the integration of more sophisticated analytical tools and broader data sources. The discussion concludes with a reflection on the potential of virtual real estate markets to shape future economic landscapes, emphasizing the need for ongoing research and analysis in this emerging field.

VI. Future Work

This is future work section. It outlines potential directions for further research and development in the field, building on the findings of this study. Future work may include exploring additional metaverse platforms, enhancing data collection methods, or integrating advanced analytical techniques to gain deeper insights into virtual real estate markets. Future work may also involve the application of machine learning algorithms to predict market trends or the development of new frameworks for assessing the economic impact of virtual properties. Additionally, expanding the scope to include user behavior analysis and its influence on property values could provide a more comprehensive understanding of the metaverse real estate landscape.

VII. Conclusion

Donec eget elit id risus iaculis tristique. Maecenas justo mauris, sagittis id ipsum vitae, elementum consectetur neque. Nam pharetra ultrices sapien, vel semper odio bibendum non. Proin mi quam, mollis a posuere vitae, facilisis pharetra urna. Pellentesque tincidunt mauris et sagittis vestibulum. Curabitur semper suscipit metus, eget cursus lacus faucibus quis. Aliquam fermentum cursus pulvinar. Curabitur posuere felis nisl, a condimentum enim molestie non. Vivamus accumsan porta felis, a hendrerit erat malesuada in. Aliquam aliquam rhoncus mauris in feugiat.

Nullam ligula nisl, interdum id libero ut, aliquam placerat erat. Proin ut lectus vel tellus ornare ultricies. Suspendisse potenti. Sed at dolor bibendum, feugiat turpis accumsan, interdum erat. Sed posuere turpis vel blandit convallis. Fusce ac elit velit. Ut sodales vulputate maximus. Nunc nec nibh in arcu luctus cursus. Sed vulputate accumsan fermentum. Curabitur maximus nec lacus nec posuere. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris congue est nec quam auctor blandit. Proin sit amet maximus nibh. In pharetra sem dolor, eget pharetra mi porttitor in. Suspendisse ac neque lacus.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras finibus ante ut metus vehicula vehicula. Cras justo lacus, efficitur quis odio quis, interdum efficitur libero. Donec sodales lectus vitae libero consectetur, vitae ornare lorem placerat. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Integer a aliquam risus, ullamcorper aliquet velit. Cras vulputate magna augue. Vestibulum bibendum est vel interdum euismod. Fusce finibus nulla ex, non rhoncus lectus malesuada mattis. Duis venenatis nunc vel lacinia rutrum. Proin faucibus sapien nisl, vitae fringilla orci hendrerit a. Quisque condimentum condimentum felis vel ullamcorper. Quisque pharetra tortor quis nisl bibendum accumsan.

Duis auctor semper turpis, vel mollis purus. Proin orci quam, pellentesque tincidunt ultricies eget, dignissim id orci. Maecenas sed fermentum ligula. Mauris facilisis sed dolor sed finibus. Curabitur luctus ultrices tempus. Etiam venenatis feugiat congue. Curabitur id purus purus. Curabitur nec enim tempus, volutpat erat in, auctor ligula. Phasellus rutrum tellus lectus. Aenean imperdiet pharetra nisl quis sodales. Praesent facilisis gravida pretium. Nam eget aliquet risus, nec dictum turpis.

Proin vitae malesuada lectus. Aliquam erat volutpat. Aenean tincidunt consectetur pulvinar. Proin sed dolor magna. Donec in ornare tortor, in lacinia massa. Cras mollis, mi vel facilisis dictum, nisl ipsum egestas urna, sit amet dignissim turpis felis quis massa. Sed vel euismod turpis. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas.

Vestibulum ullamcorper ipsum sit amet mi molestie, vel convallis ipsum malesuada. Pellentesque sed lacinia metus. Pellentesque posuere tempor diam eu pretium. Duis aliquam eget felis ac imperdiet. Quisque viverra erat turpis, vel venenatis tortor porttitor quis. Integer tincidunt vel purus a blandit. Mauris sit amet quam vel leo ultrices vulputate a at ante. Maecenas hendrerit maximus orci, eu euismod odio laoreet et. Donec in interdum elit. Praesent sed sollicitudin risus. Donec accumsan purus ut justo accumsan euismod. Sed tincidunt vehicula suscipit. Vestibulum dignissim ultricies dictum. Praesent vel nisi dolor. In at scelerisque mi. Nam malesuada nunc vel tellus convallis, ultrices facilisis dui gravida.

Acknowledgement

We thank AGH University of Krakow for their support.

References

[1] W. Fumy and P. Landrock, "Principles of key management," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 785–793, 1993.

[2] Y. Yu, T. Sharma, S. Das, and Y. Wang, ""don't put all your eggs in one basket": How cryptocurrency users choose and secure their wallets," in *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*, (New York, NY, USA), Association for Computing Machinery, 2024.

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

[4] S. Houy, P. Schmid, and A. Bartel, "Security aspects of cryptocurrency wallets—a systematic literature review," *ACM Computing Surveys*, vol. 56, no. 1, pp. 1–31, 2023.

[5] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, "SoK: Decentralized Finance (DeFi) Attacks," in *2023 IEEE Symposium on Security and Privacy (SP)*, pp. 2444–2461, IEEE, 2023.

[6] W. Li, J. Bu, X. Li, and X. Chen, "Security analysis of defi: Vulnerabilities, attacks and advances," in *Proceedings of the IEEE International Conference on Blockchain (Blockchain 2022)*, pp. 488–493, IEEE, 2022.

[7] M. Liu, J. H. Huh, H. Han, J. Lee, J. Ahn, F. Li, H. Kim, and T. Kim, "I experienced more than 10 defi scams: On defi users' perception of security breaches and countermeasures," in *Proceedings of the 33rd USENIX Security Symposium*, pp. 6039–6055, USENIX Association, 2024.

[8] C. Chen and M. Z. Yao, "Strategic use of immersive media and narrative message in virtual marketing: Understanding the roles of telepresence and transportation," *Psychology and Marketing*, vol. 39, no. 3, pp. 524–542, 2022.

[9] Deloitte, "The evolving european model of professional sports finance," *Journal of Sports Economics*, vol. 1, no. 3, pp. 257–276, 2000.

[10] Scribbr, "Develop a theoretical framework in three steps." YouTube video, 2020. Video.

[11] B. Slat and C. Worp, "Whales likely impacted by great pacific garbage patch." The Ocean Cleanup, 2019.

[12] B. Slat, C. Worp, and L. Holierhoek, "Whales likely impacted by great pacific garbage patch." The Ocean Cleanup. Retrieved February 12, 2025.

[13] P. Launiainen, *A brief history of everything wireless: How invisible waves have changed the world.* Cham: Springer, 2018.

[14] E. Karatas, B. Adali, O. Aydin, and G. Dalkilic, “Mobile application that detects covid-19 from cough and image using smartphone recordings and machine learning,” in *2021 Innovations in Intelligent Systems and Applications Conference (ASYU)*, pp. 1–6, IEEE, 2021.

[15] H. Marah and M. Challenger, “An architecture for intelligent agent-based digital twin for cyber-physical systems,” in *Digital Twin Driven Intelligent Systems and Emerging Metaverse* (E. Karaarslan, O. Aydin, U. Cali, and M. Challenger, eds.), Singapore: Springer, 2023.