Demystify Smart Contract Vulnerabilities in Blockchain-Enabled Play-to-Earn Game Ecosystems

Srikanth Pulipeti[1,3], S.K. Manju Bargavi [2,3]

[1]Department of IT, MPSTME, SVKMs NMIMS University, Maharashtra, India.

[2]Department of Computer Science and Engineering, Jain (Deemed-to-be University), Bangalore, Karnataka, India.

[3]Postdoctoral Researcher, Lincoln University College, Malaysia.

Email ID:srikanth.1240@gmail.com

Abstract: The rapid evolution of the gaming industry has transformed from the centralized ecosystems to decentralized models owing to lack of true digital ownership of in-game assets. This transformation has led to the emergence of revenue generation opportunities while playing the games such as play to earn (P2E) gaming ecosystems powered by blockchain technology. The blockchain enabled P2E games provide the true digital ownership for their in-game assets, decentralized governance and monetization opportunities. The ecosystem provides the automation through the smart contracts (SC) that plays a governing the asset ownership, reward distribution, secure transactions, thereby providing the transparency and trust. Despite these advantages, the blockchain and SC remain vulnerable to critical security challenges that can result in economic exploitations and diminished players trust. Therefore, the study performs the critical analysis of vulnerabilities across both non-P2E and P2E ecosystems. Further, the study highlighting persistent challenges includes botting, adaptive cheating, Sybil attacks and cross-chain exploits. Moreover, the study identifies the research gaps in existing detection and mitigation mechanisms that are addressed with emerging technologies. The work outlines the future research directions including Artificial Intelligence-Large language models (AI-LLM) based monitoring, domain-specific vulnerabilities detection frameworks, advanced cryptographic techniques for player's privacy preservation. The findings emphasize the necessity for holistic security approaches that integrates the technical economic and governance dimensions to ensure resilience, fairness and sustainability in the P2E ecosystem.

Keywords: Blockchain gaming, Large Language models, Play to Earn, Privacy Preservation, Smart Contracts, Tokenomics, Vulnerabilities Detection

Introduction

The traditional gaming industry primarily relied on centralized environment and players devote their valuable time and efforts to earn the various characters, weapons and extra powers. However, once the game was end the obtained precious collections will be vanished [1]. Further, the players cannot transfer their earned collections to other gamers or exchange with third party to encash. Conversely, the traditional gaming suffering with the various security challenges includes the data breaches, cyber-attacks and fraudulent activities targeting the in game assets. The data breaches causes the theft of in-game currency, loss of personal and financial information [2]. The cyberattacks such as steals the login credentials of gamers, acquiring digital assets illegally, breaking the fairness in the gameplay and online

frauds [3]. The threats such as players accounts at risk of theft, hacking and fraud. Therefore, the gaming industry moving towards the decentralized environment such as Blockchain technology (BT) to provide transparency and security over the traditional gaming ecosystem.

Moreover, during the COVID-19 pandemic, many people were confirmed to their home resulting the number of gamers improved [4]. Hence, blockchain enabled games gain the popularity to play the online games, either competing or collaborating in player versus environment such as massively multiplayers online games (MMOG)[5]. The MMOG games the players earn the digital assets, preserved in the gamer's account that provider the true ownership of digital asset, trust less environment and decentralized governance [6], [7]. Further, the players can trade these digital assets, and earn the Non-Fungible Tokens (NFT) or cryptocurrencies. Therefore, the MMOG gaming industry rehabilitated to the blockchain enabled Play to Earn (P2E) environment [8]. The P2E environment completely associated with the digital gaming economies that both companies to receive revenue and players to trade their earned in-game assets, player-to-player trades and disbursing rewards for their gaming [9]. The rewards are obtained in the form of NFTs and converted into real money that resulting the income streams under the premise of having the fun [10], [11]. Further, the rewards disbursing enables through the smart contracts (SC) which executes automatically through the computer program when the certain condition is satisfies. Therefore, the smart contracts revolutionizes the game environment through enforce the game rules, true ownership of assets and player interaction, ensuring the trustable and automated gaming environment [12].

Although, the SC handles the all-crypto transactions automatically which is target for the hackers to exploit the security vulnerabilities and perform the various attacks on the smart contract resulting the financial losses [13], [14]. Moreover, the attacks on SC can negatively affect the players' confidence and hamper the BT adoption [15].Therefore the current work focus on the SC vulnerabilities. The major contribution of the current work as follows

- The work systematically identifies the various traditional smart contract vulnerabilities alongside P2E specific threats. Thereby bridging the gaps between blockchain research and game oriented implementations.
- The study highlights the existing research across the smart contract and P2E ecosystems vulnerabilities and mitigation strategies. The mitigation strategies in blockchain platform remain uncertain in the gaming context.
- The study structured a research direction is proposed and emphasizing domain-specific vulnerabilities detection frameworks, fair reward distribution mechanisms and sustainable governance models tailored to P2E environment.

The article structure is illustrated in Figure 1 that encompasses the section II as Background details includes the evolution of the gaming industry and BT. Section III provides state of the art as the comprehensive details of SC vulnerabilities in both P2E and non-P2E environment. Further, provides the critical analysis of the literature. Section IV describes the future research directions in blockchain enabled P2E gaming ecosystem. Section V presents the conclusion.

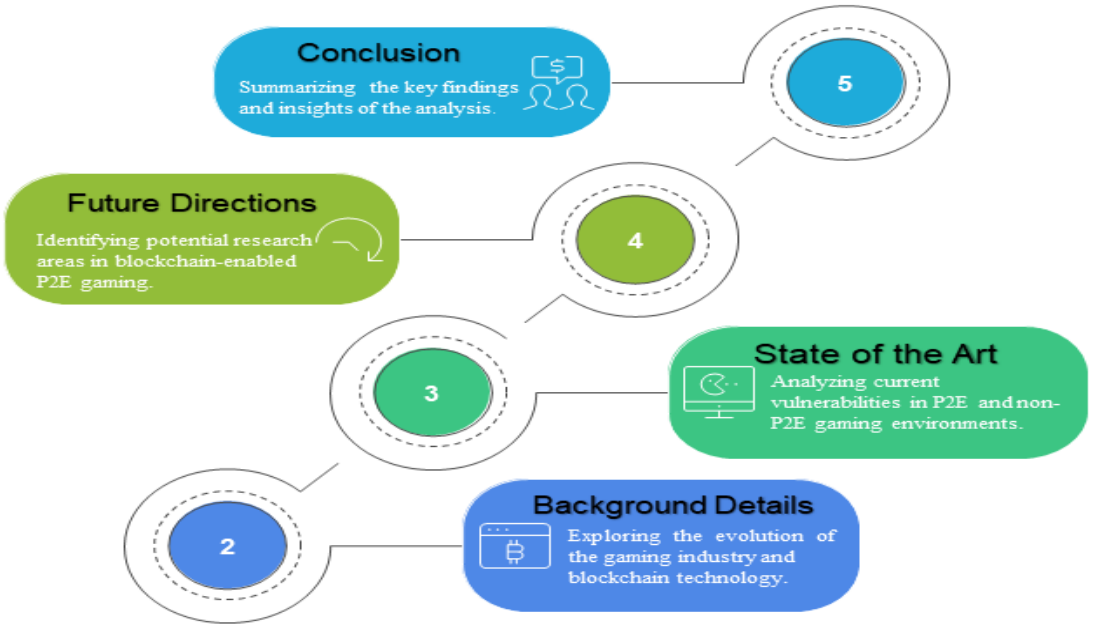

Figure 1: Work Organization

Background

The background details of the game industry and its pertained monetization models are discussed in this section. Further, it covers the blockchain technology integration with the game industry are described.

- **Monetization in Gaming models**

  The current gaming industry is enriched with distinctive features and monetization approaches. Thus, the game players are decided to select the monetization schemes for their game. The first monetization game is buy to play (B2P) where the players to buy the digital game by paying and it is available in the floppy, or Compact disk (CD). The monetization associated in this games is less and this type of these games are facing various challenges like single player is available in the game, the other players' interactions also very less and game play experience is self-contained[9]. Thus, the single player game challenges addressed with the multiplayer online games.

  The multiple players are involved and they can establish the interactions with other players through the same location or online platform i.e. different location. The players are interacting and playing the game leads to the various types include the co-operative and competitive gaming. Further, the monetization of multiplayer game is classified based the playing skills such as subscription based, free to play (F2P) and pay to play (P2P). The subscription-based games are massively multiplayer online role-play games (MMORPG) like world of war craft. The emergence of mobile devices the gaming industry adopted the rapid monetization models includes F2P games are in-game purchase like Fortnite and Candy Crush Saga. The P2P are freemium models, which are available limited however the players to acquire full access to gaming functions through the micro transaction i.e. players to make payment includes over-watch [5].

  The Cooperative Games (Co-Op) focus on the collaborative or team play to achieve the common goals over the online or locally. The monetization associated in Co-Op games with F2P or P2P. The Competitive games highlight the player versus player interaction. The competitive games depend on

the game players' skills and strategies resulting the victory of the game as team or individual. The monetization associated in competitive game includes sponsorship, sales of event tickets, telecasting of the events or media rights and advertising. The subscription based gaming completely depends on the subscription payment to access the game basic functions. This type of game is established in MMORPG and the revenue is generated through the subscription charges which is helpful for the sustain of the game development and maintaining the server. The F2P games permit the players to access some content of game without fee and revenue source is in-game purchases i.e. buying the game items or upgrades for game. Further, the F2P games generates the revenue through advertisements that appears throughout the game play. However, playing the game is free of charge and in-game transactions permits the players must pay to enhance their in-game experience. The P2P games permit the players to pay the initial amount to gain the access of the basic game play without extra cost. The monetization of P2P associated with diverse ways like advancement of the game, downloadable content. Moreover, these models generates the revenue such as funds from players, advertising, telecasting of events, sales of the tickets however, in-game asset trading is not supported above-mentioned games[16].

The play to earn (P2E) gaming model revolutionize the monetization models by adopting the decentralized environment. In decentralization gaming environment permits the players earn the cryptocurrencies by trading their in-game assets and rewards for their game play as well as the companies receives the revenue. The P2E gaming model provides the true ownership for players' in-game assets, and secure transactions. Therefore, the comparison of the various monetization models is illustrated in Table 1 and the sub sequent section deals with the integration of BT with P2E.

Table 1: Comparison of Monetization Game models on various parameters

Playing Mode	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**Application**
Single Player	▲	●	●	○	○	●	▲	◐	○	○	◐	●	○	▲	●	◐	Narrative-driven RPGs	Piracy, cheat codes, corruption.
Multiplayer Online	◆	●	●	○	○	●	◐	●	◐	○	◐	◐	◐	●	◐	●	MMOs, casual/ competitive	DDoS, phishing, hijacking.
Co-op Mode	▲	◐	●	○	○	●	○	●	●	○	◐	◐	○	●	◐	◐	Shared narrative / team play	Voice chat exploits, sniffing.
Battle Royale (F2P)	▲	●	●	○	○	●	●	●	●	○	◐	◐	◐	●	◐	●	Fortnite, PUBG	Cheating via bots, server overload.
Sandbox / Open World (P2P)	◆	●	●	◐	○	●	●	●	◐	○	◐	◐	◐	◆	●	◐	Minecraft, GTA	Modding risks, theft, fake assets.

VR / AR Games (P2P)	●	◐	◐	○	○	●	▲	◐	○	○	●	◐	◐	◆	●	◐	VRChat, AR apps	Sensor spoofing, privacy leaks.
Esports (Subscription/Hybrid)	◆	●	●	○	○	●	●	●	●	○	◐	◐	●	●	●	◐	DOTA, CS:GO, LoL	DDoS, fraud, match manipulation.
Play-to-Earn (P2E)	●	●	◐	●	●	●	●	●	●	●	◐	◐	●	●	◐	●	Axie, Decentraland	Smart contract exploits, rug pulls

X: A: Access Cost, B: Monetization, C: Accessibility, D: Ownership Rights, E: Blockchain Integration, F: Game Experience, G: Economic Model, Y: H: Cross-Platform, I: Community / Guild, J: P2E Incentives, K: Device Dependency, L: Scalability, M: Legal / Regulatory Risks, N: Social Interaction, O: Immersion, P: Data Privacy, Q: Sustainability, ▲ = Low, ◆ = Medium, ● = High, ○ = Not Supported, ◐ = Partial, ● = Supported

- **Integration of Blockchain Technology(BT) to Gaming Ecosystem**

The gaming ecosystem initially manages through the central server and game related information stored in database by the publishers and game developers. The central game ecosystem is suffering with various critical challenges such as transparency, security, trust and lack of the true ownership of in-game assets [17]. Further, the players are depending the developers for experiences, integrity and availability of assets [17]. Therefore, the emerging technology like BT address the various challenges of the centralized gaming ecosystem. The BT enables the decentralization to govern the game assets, true ownership for in-game assets and transactions. Further, the BT enhances the security through the immutable ledger, transparency for in-game economies, ensures the fairness in game play and innovation to drive the gaming eco-system towards player centric. The ledger preserves the transaction information in the blocks through validating the transactions by leveraging the consensus mechanisms without using third party. Moreover, BT provides the automation through SC, which is computer program that executes when the condition satisfies, based on the agreement. Therefore, the benefits of the BT include the distributed ledger, consensus mechanism and SS provides the robust security which revolutions the gaming industry.

The integration of BT with gaming industry provides the various benefits like enhances the security, establishes the true ownership of in-game assets, develop the in-game economics and technical challenges as shown in Figure 2.

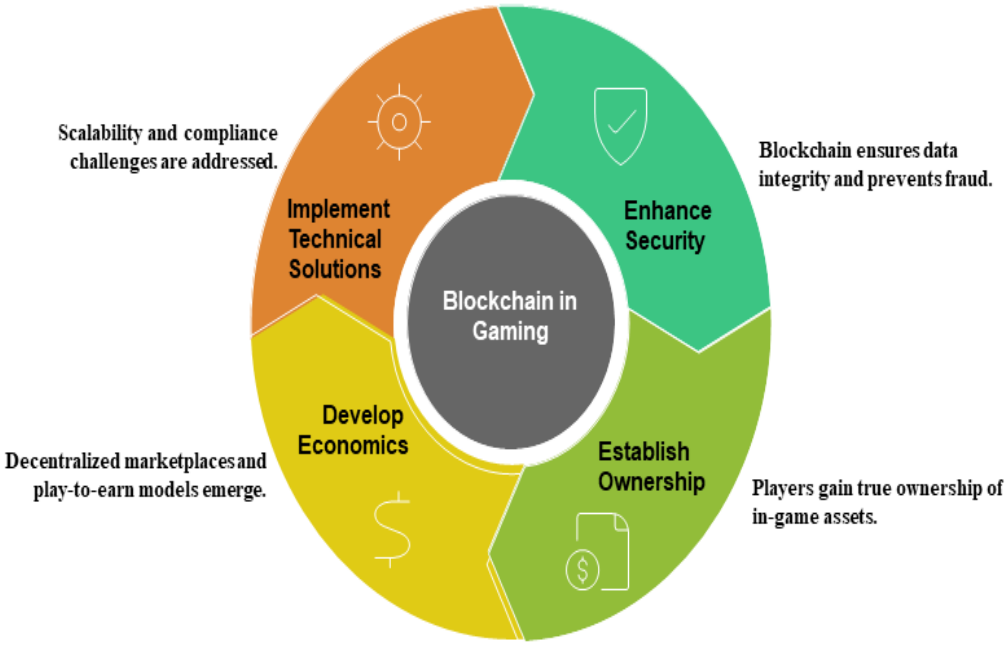

Figure 2: Blockchain in Gaming ecosystem

According to Figure 2 by integrating the BT with gaming, industry following benefits are associated

- *Enhance Security*: in BT, each transaction or data is preserved in the block and the blocks are interlinked with next block using the cryptographic algorithms such as Hashing techniques. The alteration of the hash value reflecting on the subsequent blocks thereby the data remains not changed i.e. consistent and provides the tamper-proof. In the context of gaming eco system the player's activities, transactions and in-game assets are preserved and not permits the modification or deletion of in-game assets related information. Therefore, BT provides the immutability, transparency and trust among the players and developers. Further, in decentralized gaming environment the transparency is essential to ensure the fair game play resulting the enhanced the security [18]. The players' interaction and game logic is encoded into automatically executed computer program based on the condition satisfactory such as the SC resulting the cheating prevention [19]. Furthermore, each transaction recorded in the block using the timestamp and in linked with previous transactions that ensures the traceable and unaltered transaction history. Therefore, the traceability prevents the fraud for in-game assets trading and provides the confidentiality to the players by preserving the buyer, seller, trading information secretly. Therefore, the integration leads the enhanced surety over the traditional security system for game ecosystem [20].
- *Establishes the ownership:* In gaming context, the players earn the various game components such as weapons, characters and many more. These components are stored on the decentralized blockchain and players have the full ownership and governance on their earned items. Further, players can buy and sell their earned components over the various platforms using the gaming infrastructure. Therefore, the decentralized gaming eco system ensures that if the gaming server is down or failed also the players retains their items, which offers the accessibility. Further, assets of various games seamlessly transfer one game to another game based on the players' true

ownership that offers through the SC and blockchain protocol. For instance, the fantasy game the player obtains the sword weapon that can be transferred to another game as metaverse. Thus, this cross platform asset usage provides the interoperability among the gaming ecosystems, encourages the players engagement and revenue generation through collaborations[21].The governance in the decentralized game ecosystem the decision-making process takes place across the game developers and players by leveraging the distributed autonomous organizations (DAO). The game developers are closely associated with the players' interests and desires towards the democratic environment. Further, the decentralized governance ensures the transparency and accessibility across the participants in the network[17].

- *Develop Economics:* BT enables the decentralized in-game currencies and assets to transfer and verifiable over the network. The verification process avoids the replication of in-game assets and enhances their value. Moreover, the players trade their in-game assets leads to the dynamic and robust game economies. The SC enables the automate and secure interactions of economic such as auctions, lending and staking assets [17]. The P2E models, the players earn the rewards as NFTs or cryptocurrencies for their in-games and distributed through SC [17].
- *Implement Technical Solutions:* the BT based games handles the high volume of transactions and interactions among the characteristics over the online games without compromising the speed of the transaction. Further, the transaction congestion is reduced and throughput is enhanced through layer-2 solutions. The network capacity is enhanced through sharding, which divides the blockchain into small fragments that are manageable easily and performs the parallel processing of its transactions [17].

Literature Review

The current study provides the state-of the art details of the blockchain enable P2E gaming eco systems challenges are described in two categories such as non-P2E gaming and P2E gaming ecosystem challenges.

- **Non-P2E gaming ecosystem**

Iuliano and Di Nucci [22] provides a comprehensive and systematic review of vulnerabilities and detection tools related to smart contract security. The authors conducted rigorous review to identify the 101 distinct vulnerabilities and 144 automated detection tools underlying the code-transformation techniques. However, the study is limited by its exclusion of non-Ethereum platforms, vulnerabilities and tools relevant to other blockchain ecosystems. Further, authors emphasize the automation in detection tools for future research directions. Shaikh [23] assess the effectiveness of various smart contract vulnerability detection techniques and deployment of Ethereum platforms with identifying the performance profiles and practical applicability. The framework leveraged s the static analysis, dynamic code analysis, symbolic execution and machine learning as detection techniques. Further, the static analysis provides the high accuracy and fast detection, machine learning provides the scalability. However, the models lack the empirical evaluations of real-world contract. Kissoon and Bekaroo [24] presented detection of vulnerabilities in smart contract using security analysis and pen-testing in decentralized environment. The author leveraged various detection tools such as fuzz testing and AI-driven models thereby applying the pen-testing quality model assessing each method with various metrics. However, the article not focus on the empirical testing on real smart contract datasets.

Chen et.al [25] assess the performance of ChatGPT as a smart contract vulnerability detection tool to identify the known vulnerabilities. The study reveals that the ChatGPT achieves the high recall, moderate precision resulting the false positives across various vulnerabilities. The model outperforms over the

traditional tool and finds the root causes of the false positives outputs. This analysis provides the high recall rate however, lack of precision, variability across vulnerabilities types used for smart contract security. Gorton and Abiona [26] investigate the cheat codes and game bots used for cheating in modern online games. The authors focused on sports and puzzles to complex multiplayer frameworks to examine cheat-related mechanisms. The study reveals that the vulnerabilities exploited by cheat tools and bots thereby undermining the integrity and diminishing the gaming experiences for honest players. However, the article lack of gameplay case studies requires the updated frameworks for understanding modern cheating dynamics and security implications. Zaazaa and El Bakkali [27] developed a framework named as smartLLMSentry to enhance the smart contract vulnerabilities detection using large language models(LLM). The smartLLMSentry leverages in-context learning with ChatGPT to dynamically generate and integrate vulnerability detection rules to ensure a diverse and unbiased evaluation. The model provides the 91.1% accuracy for exact matching detection rules. Further, the framework demonstrated enhanced speed and precision in integrating the new vulnerabilities rules. However, the framework lacking the full automation to validate and refine the generated rules. Further, the evaluation is limited to fewer vulnerabilities types. Hu et.al [28] is explore the vulnerabilities of the smart contracts using LLMs for automated detection framework to enhance the security. The authors employed the prompting paradigms like binary, multi-class and open-ended. Further, two-staged adversarial framework named as GPTLens that splits the detection into auditor and critic stages. The results demonstrated the enhanced detection of true positives substantially raises the false positives. However, high false positive rate inherent in naive LLM prompting, the randomness of generation and in-depth validation is essential in large-scale real world contract audits.

- **P2E gaming ecosystem**

Traithipthomrongchoke et al. [29] proposed a data driven strategy to analyze the user behavior in P2E games and its pertained challenges to user retention, engagement and monetization. The primary aim to enhance the retention and economic stability in the game design. The proposed model uses the players behavior segmentation, optimizes the privilege assignment timing with personalized rewards and predictive modelling to examine the players' actions include redemption of asset and risk management. The model integrates the various techniques such as the recency frequency and monetary (RFM) to analyze the players' segmentation and optimization, Isolation Forest (IS) employed to detect player behavior such as bot from high-dimension data. Further, principle component analysis (PCA) employs to reduce the dimensionality and k-means clustering to group the players into clusters. However, IS method effectively detecting the anomalies in static nature for dynamic nature incorporates the graph-based techniques through profiling normal patterns. The XGBoost leveraged for predictive modeling that enables the precise prediction of redemption behavior. However, the redemption events are imbalanced nature due to that the Synthetic Minority Oversampling Techniques (SMOTE) was used to balance the dataset. However, the model lack to provide the comprehensive details of player retention and challenges associated in bots' detection. Tan [4] presents P2E games transformation towards economic rentiership in digital environment using blockchain technology. This work provides qualitative and conceptual methodology on critical economic and digital labor to analyses the in-game trading activities. The model finds the boundaries between work and play, players positioning as consumers and digital labors to contribute the creation and rent extraction value. Further, the theoretical model emphasizes the assetization ownership and labor digital economies. However, the study is limited to providing the player

experiences in the P2E games, and in-depth investigation is essential for ownership models, economic inequality and sustainability of rent driven platforms in volatile crypto markets. Duguleana et al. [9] developed a consumer decision making in web3 P2E decentralized gaming paradigm that combines the entertainment with economic incentives. The proposed model examines the various types of micro – economics developed in five P2E games. The study provides the consumer behavior in cryptocurrency based games and their dynamics resulting the development of in-game economics and individual player engagement. Moreover, the study compares the traditional online games with the web3 games and assessing the P2E revenues aspects for the consumers. However, the study is considered small game samples, limited stakeholder's perspective and the comparison with traditional gaming models. Delic et al.[30] presents the P2E gaming profile risks focus on Axie infinity blockchain enabled game. The model uses the qualitative data in the form of online chat threads through thematic analysis scheme. The data is collected from various platforms such as Reddit, twitter and game specific forms. However, the game players receive rewards for their game play and accompanied negative assessment of game quality. Therefore, the study emphasizes the economic and social benefits are associated with revenue generation opportunities and community establishment. However, the model raises the various concerns such as limited sustainability of scholarship models, financial stress, consumer protection. The qualitative analysis validation leaves gaps in understanding widespread of various P2E communities. Rishiwal et al. [16] presented a blockchain enabled secure gaming environment literature to protect the in-game transactions, reducing the fraud and ensuring the digital asset integrity. The work emphasizes the decentralized ledgers, smart contracts and immutability that enhances the secure transaction, transparency and trust in gaming ecosystems. Further, the survey identifies the potential game rules and asset ownership thereby cheating prevention and manipulation. However, the survey was lack of cross-platform standards, scalability challenges and performance constrains in the real-world deployment. Lai et al [8] investigates the market instability that affects the player behavior in P2E games and examine the viability potentials of government regulations. The authors employed the non-probability snowball sampling through SPSS to generate descriptive statistics of the player behaviour. The results of the methodology identify the player financial instability to volatile markets and expressed trusts challenges pertained to price manipulation, privacy and usability. However, the model limited to on-chain behaviour analysis and token governance effectiveness remains untested. The summary of literature is illustrated based on numerous parameters and shown in Table 2.

Table 2: Comparative summary for various vulnerabilities

Article	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Iuliano & Di Nucci (2024)[22]	●	●	◐	●	●	◐	◐	○	○	○	○	○	○	○
Shaikh (2024)[23]	●	●	◐	●	●	●	◐	○	○	○	○	○	○	○
Kissoon & Bekaroo (2022)[24]	◐	◐	○	◐	●	●	◐	○	○	○	○	○	○	○
Chen et al. (2023)[25]	●	●	◐	◐	○	●	◐	○	○	○	○	○	○	○
Gorton & Abiona (2022)[26]	○	○	◐	○	○	○	●	○	○	●	●	○	○	○
Zaazaa & El Bakkali (2024)[27]	◐	◐	○	◐	○	●	◐	○	○	○	○	○	○	○
Hu et al. (2023)[28]	◐	◐	◐	◐	○	●	◐	○	○	○	○	○	○	○
Traithipthomrongchoke et al. (2023)[29]	○	○	○	○	○	●	●	○	○	○	●	○	○	○

Tan (2022)[4]	○	○	○	○	○	○	●	●	○	○	○	○	○	○
Duguleana et al. (2022)[9]	○	○	○	○	○	○	●	◐	○	○	○	○	○	○
Delic et al. (2023)[30]	○	○	○	○	○	○	●	○	○	○	○	○	○	●
Rishiwal et al. (2023)[16]	◐	◐	○	◐	○	○	●	○	○	○	○	○	○	○
Lai et al. (2023)[8]	○	○	○	○	○	○	●	◐	●	○	○	◐	●	○

A: Re-entrancy / Technical Bugs, B: DoS / Gas / Overflow, C: Time / Oracle / RNG Issues, D: Access Control / Logic Flaws, E: Symbolic / Fuzzing, F: ML / AI Detection, G: Econ Exploit / Rentiership, H: Ponzi-like Tokenomics, I: Governance Exploits, J: Gambling / Addiction, K: Botting / Sybil Attacks, L: Privacy / Data Risks, M: Market Instability, N: Consumer Protection, ● Fully supported, ◐ Partially supported, ○ Not supported

Critical analysis:

- The classical smart contract vulnerabilities like access control, logic flaws and integer overflow and underflows are most consistently addressed in Ethereum blockchain. However, the P2E gaming ecosystem still suffering with these vulnerabilities when distributing the rewards through smart contracts.
- The timestamp dependence and denial of rewards obtain only partial attention however these are critical in P2E ecosystems yet no study addressed comprehensively.
- The oracle challenges are high risk and important in pricing and randomness feeds for P2E tokens.
- The critical P2E vulnerabilities such as botting, reward denial. Sybil attacks, bridge exploits, Ponzi tokenomics and governance manipulation remain open challenges because of inadequate academic solutions.
- The adoption of on-chain analytics, wallet tracking and NFT based identity, player privacy and data leakage risks in P2E decentralized gaming ecosystems.
- The emerging technologies like LLMs, AI detection, interoperability protocols and advanced cryptography are underutilized in the P2E context.
- The studies are lacking to address the scalability-security trade off in the P2E due to the high transaction of data, micro-payments and asset transfers in the P2E prone the performance bottlenecks
- The P2E gaming ecosystem is pertains to security, economics and social dynamics however most of the studies focused on the single dimension approach. Thus, it requires the holistic framework that provides both technical exploits and economic manipulations.

Future Direction

The literature emphasizes the critical research challenges remain in the P2E specific risks, cross-chain challenges and economic sustain abilities. Therefore, this section provides future research in the P2E gaming ecosystem as follows

- Advanced vulnerability detection frameworks: Develop domain specific vulnerability detection tools to detect and mitigate the vulnerabilities like access control flaws, logic flows and arithmetic vulnerabilities in reward distribution over P2E smart contracts [22], [23].
- Fair and Transparent Reward Mechanisms: Establish the protocols that prevent the timestamp manipulation, reward denial and ensuring equitable distribution of in-game incentives for their game play [24], [25].
- Robust Oracle and security: Decentralized oracles and cross-chain with cryptographic proofs and formal verification to protect the pricing, and multi-chain assets [24], [25]

- LLM based threat detection: Employ the AI and LLM models to detect the botting, Sybil attacks and automated exploits while monitoring player behaviour and smart contract vulnerabilities [27], [28].
- Privacy preserving player protection: Incorporate the zero-knowledge proofs, zk-SNARKS and privacy preserving analytics to protect the wallet data identities and gaming activity from the acquaintance [15], [30].
- Sustainable Tokenomics and governance: Design adaptive token models and DAO governance mechanisms that resist the Ponzi-like structures, vote manipulation and economic instability [15], [16].
- Multidisciplinary security architectures: The holistic frameworks that integrates the technical, economic, governance and privacy layers to ensure the sustainable resilience of P2E ecosystems [26], [30].
- Dynamic Bot and Cheat detection systems: The current approaches detect anomalies at static that are failed against the adaptive cheating. Therefore, graph-based anomaly detection, and real-time cheat detection is essential for P2E exploits [23], [26].

Conclusion

The study examines the smart contract vulnerabilities inherent in blockchain enabled P2E ecosystems that emphasizes the reward distribution, economic stability and player trust. While the traditional vulnerabilities like access control flaws, logic errors and arithmetic overflows poses the system risks. The P2E ecosystem also suffering with various threats like botting, Sybil attacks, oracle manipulation and unsustainable tokenomics. Therefore, the literature reveals that the existing challenges are partially addressed still there is a significant research gaps exist in both academic and real world. Additionally, the work outlines the future research directions that integrate the adaptive vulnerability detection frameworks, AI-LLM driven monitoring, sustainable governance models. The multidisciplinary approaches that integrates the technical, economic and social dimensions is essential to ensure long-term resilience of decentralized gaming ecosystems. Finally, the P2E ecosystems requires transformation towards holistic, adaptive and scalable security frameworks that not only mitigate vulnerabilities but also enhances the fairness, transparency and player experience in decentralized gaming environment.

Funding Information

This research not received funding

Data Availability Statement

The data or material that support the findings of this article are not available

Conflicts Of Interest

Declare conflicts of interest or state “The authors declare that they have no conflicts of interest to this work. Authors are required to disclose any personal circumstances or interests that could potentially influence the way research results are presented or interpreted. Additionally, "The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript.

References

[1] J. Yu, M. Zhang, X. Chen, and Z. Fang, “SoK: Play-to-Earn Projects,” Nov. 02, 2022, arXiv: arXiv:2211.01000. doi: 10.48550/arXiv.2211.01000.

[2] U. Agarwal et al., “Exploring Blockchain and Supply Chain Integration: State-of-the-Art, Security Issues, and Emerging Directions,” IEEE Access, vol. 12, pp. 143945–143974, 2024, doi: 10.1109/ACCESS.2024.3471340.
[3] H. Palivela et al., “Optimization of Deep Learning-Based Model for Identification of Credit Card Frauds,” IEEE Access, vol. 12, pp. 125629–125642, 2024, doi: 10.1109/ACCESS.2024.3440637.
[4] G. K. S. Tan, “Assetizing the video game: Play-to-earn (P2E) games and blockchain rentiership,” Progress in Economic Geography, vol. 3, no. 1, p. 100036, Jun. 2025, doi: 10.1016/j.peg.2025.100036.
[5] P. Delfabbro, A. Delic, and D. L. King, “Understanding the mechanics and consumer risks associated with play-to-earn (P2E) gaming,” J Behav Addict, vol. 11, no. 3, pp. 716–726, Sep. 2022, doi: 10.1556/2006.2022.00066.
[6] T. Shivani, “Gaming and Asset Tokenization: The Rise of Play-to-Earn Models.” Accessed: Sep. 08, 2025. [Online]. Available: https://www.linkedin.com/pulse/gaming-asset-tokenization-rise-play-to-earn-models-spydra-qu1gc
[7] D. Stamatakis, D. G. Kogias, P. Papadopoulos, P. A. Karkazis, and H. C. Leligou, “Blockchain-Powered Gaming: Bridging Entertainment with Serious Game Objectives,” Computers, vol. 13, no. 1, p. 14, Jan. 2024, doi: 10.3390/computers13010014.
[8] Y. Lai, S. Fan, and W. Cai, “Quantitative Analysis of Play-to-Earn Blockchain Games: A Case Study of Axie Infinity,” in 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), Kyoto, Japan: IEEE, Jun. 2023, pp. 250–257. doi: 10.1109/MetaCom57706.2023.00054.
[9] A. R. Duguleană, C. R. Tănăsescu, and M. Duguleană, “Emerging Trends in Play-to-Earn (P2E) Games,” Journal of Theoretical and Applied Electronic Commerce Research, vol. 19, no. 1, pp. 486–506, Mar. 2024, doi: 10.3390/jtaer19010026.
[10] K. SHIN, H. E. Kwon, A. Ghose, and C. Suh, “Play, Earn, and Engage: The Motivational Influence of Crypto-Economic Models on Mobile Game Engagement,” ICIS 2024 Proceedings, p. 1980, Dec. 2024.
[11] M. Davis, “‘Serfing’ the Web; Play-to-Earn, Blockchain, and the Workification of Online Games,” Apr. 13, 2025, Social Science Research Network, Rochester, NY: 5211964. doi: 10.2139/ssrn.5211964.
[12] M. Xevgenis, D. G. Kogias, P. A. Karkazis, and H. C. Leligou, “Addressing ZSM Security Issues with Blockchain Technology,” Future Internet, vol. 15, no. 4, p. 129, Mar. 2023, doi: 10.3390/fi15040129.
[13] ZebPay, “How Smart Contracts Are Revolutionizing Gaming Experiences | ZebPay,” How Smart Contracts Are Revolutionizing Gaming Experiences. Accessed: Sep. 08, 2025. [Online]. Available: https://zebpay.com/in/blog/how-smart-contracts-are-revolutionizing-gaming-experiences
[14] S. HajiHosseinKhani, A. H. Lashkari, and A. Mizani Oskui, “Unveiling vulnerable smart contracts: Toward profiling vulnerable smart contracts using genetic algorithm and generating benchmark dataset,” Blockchain: Research and Applications, vol. 5, no. 1, p. 100171, Mar. 2024, doi: 10.1016/j.bcra.2023.100171.
[15] M. Mnasri, A. J. Maâlej, and M. Jmaiel, “A systematic literature review on security testing of Ethereum smart contracts,” Blockchain: Research and Applications, p. 100314, Jun. 2025, doi: 10.1016/j.bcra.2025.100314.
[16] V. Rishiwal, U. Agarwal, M. Yadav, A. Alotaibi, P. Yadav, and S. Tanwar, “Blockchain-Secure Gaming Environments: A Comprehensive Survey,” IEEE Access, vol. 12, pp. 183466–183488, 2024, doi: 10.1109/ACCESS.2024.3510467.
[17] K. Macwan, “Integrating Blockchain Technology in Online Gaming Ecosystems,” Computer, vol. 57, no. 10, pp. 104–111, Oct. 2024, doi: 10.1109/MC.2024.3431908.
[18] G. Manasa, K. Rajesh, E. L. Goud, G. Shriya, and K. Srijani, “Block Chain Technology with Centralized Database For Conventional Data Integrity Verification schemes,” IJARST, vol. 14, pp. 825–833, 2024.

[19] A. Ibrahim, “Guarding the Future of Gaming: The Imperative of Cybersecurity,” in 2024 2nd International Conference on Cyber Resilience (ICCR), Feb. 2024, pp. 1–9. doi: 10.1109/ICCR61006.2024.10532843.
[20] G. Rosario, “Regulation of Cryptocurrencies and Blockchain Technologies: National and International Perspectives | SpringerLink.” Accessed: Sep. 08, 2025. [Online]. Available: https://link.springer.com/book/10.1007/978-3-319-78509-7
[21] R. Sarode, Y. Watanobe, and S. Bhalla, “From Silos to Unity: Seamless Cross-Platform Gaming by Leveraging Blockchain Technology,” in Big Data Analytics in Astronomy, Science, and Engineering, in Lecture Notes in Computer Science. , Springer, Cham, 2024, pp. 213–223. doi: 10.1007/978-3-031-58502-9_15.
[22] G. Iuliano and D. D. Nucci, “Smart Contract Vulnerabilities, Tools, and Benchmarks: An Updated Systematic Literature Review,” May 26, 2025, arXiv: arXiv:2412.01719. doi: 10.48550/arXiv.2412.01719.
[23] S. M. A. Shaikh, “Mathematical Analysis of Existing Techniques for Ethereum Smart Contract Vulnerability Detection,” Communications on Applied Nonlinear Analysis, vol. 31, no. 3s, pp. 127–139, Jun. 2024, doi: 10.52783/cana.v31.737.
[24] Y. Kissoon and G. Bekaroo, “Detecting Vulnerabilities in Smart Contract within Blockchain: A Review and Comparative Analysis of Key Approaches,” in 2022 3rd International Conference on Next Generation Computing Applications (NextComp), Oct. 2022, pp. 1–6. doi: 10.1109/NextComp55567.2022.9932169.
[25] C. Chen et al., “When ChatGPT Meets Smart Contract Vulnerability Detection: How Far Are We?,” ACM Trans. Softw. Eng. Methodol., vol. 34, no. 4, pp. 1–30, May 2025, doi: 10.1145/3702973.
[26] S. Gorton and O. Abiona, “The Confidentiality of Coding Video Games with Cheat Code and Bots for Cheating in a Virtual World,” International Journal of Communications, Network and System Sciences, vol. 16, no. 6, pp. 105–114, Jun. 2023, doi: 10.4236/ijcns.2023.166008.
[27] O. Zaazaa and H. E. Bakkali, “SmartLLMSentry: A Comprehensive LLM Based Smart Contract Vulnerability Detection Framework,” Journal of Metaverse, vol. 4, no. 2, pp. 126–137, Dec. 2024, doi: 10.57019/jmv.1489060.
[28] S. Hu, T. Huang, F. İlhan, S. F. Tekin, and L. Liu, “Large Language Model-Powered Smart Contract Vulnerability Detection: New Perspectives,” in 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Nov. 2023, pp. 297–306. doi: 10.1109/TPS-ISA58951.2023.00044.
[29] W. Traithipthomrongchoke, A. Aeksari, P. Boonrawd, and S. Nuchitprasitchai, “Data-Driven Strategies for Enhancing User Engagement in Play-to-Earn Games: Segmentation, Privilege Assignment Optimization, and Redemption Behavior Prediction,” in 2025 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), Nan, Thailand: IEEE, Jan. 2025, pp. 264–269. doi: 10.1109/ECTIDAMTNCON64748.2025.10962047.
[30] A. J. Delic and P. H. Delfabbro, “Profiling the Potential Risks and Benefits of Emerging ‘Play to Earn’ Games: a Qualitative Analysis of Players’ Experiences with Axie Infinity,” Int J Ment Health Addiction, vol. 22, no. 1, pp. 634–647, Feb. 2024, doi: 10.1007/s11469-022-00894-y.