Blockchain Driven Solutions for Preventing Cyber Threats in Online Gaming

Deepali Chaudhari[1]
Assistant Professor, School of information Technology, Indira University, Pune-411033, India.

Shweta Bhoyate[2]
Assistant Professor, School of information Technology, Indira University, Pune-411033, India.

Rajminar Navgire[3]
Assistant Professor, School of information Technology, Indira University, Pune-411033, India.

DOI: 10.29322/IJSRP.16.02.2026.p17029
https://dx.doi.org/10.29322/IJSRP.16.02.2026.p17029

Paper Received Date: 6th January 2026
Paper Acceptance Date: 5th February 2026
Paper Publication Date: 12th February 2026

Abstract

Evolution of online gaming into complex digital ecosystems supported virtual economies involving real-money transactions, real-time multiplayer interactions, and competitive environments. These rapid growth in popularity of online gaming is resulted into significant cybersecurity challenges, like digital asset theft, account compromise, financial fraud and cheating. Centralized architectures followed by most gaming platforms may cause single points of failure, limited transparency.

Decentralized architecture followed by Blockchain technology overcomes most of these limitations. Elimination of trust on single controlling authority enhance resilience and eliminate risk of systemic failure for Blockchain technologies. In addition to this, secure verification of transaction is ensured by cryptographic mechanisms and unauthorized data manipulation is prevented by immutable, transparent ledgers. Online gaming platform's security is strengthed by these promising Blockchain characteristics.

This paper focuses on how blockchain features can be selectively associated with existing online gaming platforms in order to reduce cyber threats and ensure overall security.

Keywords: Blockchain technology, Online gaming platform security, Cyber threat reduction, Smart contracts, decentralized systems.

I. INTRODUCTION

In last few years, online gaming has transformed into large scale digital ecosystems that comprises of real-money transactions, esports, and virtual marketplaces. Modern gaming platforms are more vulnerable to cyber-attacks as they produce and manage huge amounts of valuable digital assets and sensitive data. Security breaches can damage user trust, can result in long-term financial losses and can hamper rapid growth of online gaming platforms.

Even afrer technological advancements, centralized server architectures are preferred by most online gaming platforms for game logic execution, authentication and data storage. Though system management and coordination are simplified by centralized systems, it may be vulnerable to critical security threats. Platform availability and user confidence can be compromised by single points of failure, data breaches and service outages. [3][12].

Blockchain technology represents a decentralized framework operating independently of any particular authority. Secure data verification and tamper-resistant recordkeeping is well ensued by By employing consensus mechanisms and cryptographic validation in , blockchain Decentralization, immutability and transparency, blockchain features well address security challenges in online gaming environments, mostly issues related trust, fairness in gameplay, and integrity of in-game assets

Problem Statement

Online gaming platforms are vulnerable to ongoing cybersecurity risks like asset theft, data breaches, service interruptions, and account compromise due to centralized architectures. The Long-term viability and user confidence of gaming ecosystems is endangered by these imperfections. Current security measures are not up to the mark and unable to meet expected security procedures.

Contributions of This Paper

1. Security Concerns Ascertainment: Cyberthreats, affecting centralized online gaming platforms are listed down.

2. Progression of Blockchain Characteristics: These security concerns can be rectified by blockchain characteristics like decentralization, immutability, transparency and cryptographic validation..

3. Choice of curated framework: Without affecting revenue models or gameplay, current online gaming systems are incorporated witf. Blockchain-based security features

4. Security-Centric Perception: In gaming platforms, blockchain is evolved as a cybersecurity enhancement tool and not like a financial or economic innovation. The paper reveals how blockchain-based security solutions enhances integrity, trust and resilience in online gaming environments..

II. CYBERSECURITY THREATS IN ONLINE GAMING

Online gaming platforms are not very safe from people who want to hack them. These hackers can cause a lot of problems for people who use these platforms. Trust in the game can be lost by people. They can also fraud to win.

Due to rapid growth and vast usage online gaming platforms are facing lots of problems. This means that security problems to be dealt with by online gaming platforms all the time. Attackers are exploiting vulnerabilities in the system. The way people use the online gaming platforms. This is a task for online gaming platforms to safeguard their systems and users.

A. Account Compromise and Credential Abuse

Player accounts are at risk. They are not secured. The reason behind this is that people login credentials are not that strong. Multiple times people use their account login credentials. They try to log in to their player accounts many times.

Why does this happen to player accounts? When someone hacks into a player's account, it is not the player's account that is affected. The person who owns the player account can have their identity stolen. The hacker can also make purchases in the game using the player account that the owner of the account does not want. This can cause financial problems for the player and the people who run the game platform [7],[10].

B. Theft and Duplication of Digital Assets

Digital assets are typically handled by servers that control repositories in centralised gaming environments that are centralized. This means that bad people can do things with virtual items, like manipulate them or copy them, or even transfer them in ways that are not allowed. This is a problem because it messes with the economy of the game and makes people wonder if they really own the digital assets they have. Digital assets are what get affected by this. It is a problem for digital assets.

C. Cheating and Gameplay Manipulation

When people play games, they can get an advantage in a way. They do this by using things that're not right with the software or by using special tools that help them cheat at the games. This is unfair, to the people, playing the games.

The games don’t work properly when people keep cheating all the time at the games. This makes people loose interest in the games.

Cheating by some people results in a loss of interest in online games by authentic players. This means people will avoid the game for a time, especially when it comes to competing with others or playing esports.

D. Financial Fraud and Scams

Gaming sites that allow people spend money may have financial fraud. This can happen because of tradespeople fantasizing to be someone else and exploiting the payments methods. These things can make the market go down for the games and make people doubt the transactions.

* Data Exposure

* Privacy Violations

Gaming sites comprising the use of real money might explode in fraud. Financial fraud produced on these sites might give them a lot of trouble. Such gaming sites should trouble about this kind of financial fraud.

Centralised sensitive user information is at higher risk. The Companies that providing game services having this issue. And also dealing with privacy and the law can be truly challenging for those companies [12].

III. SECURITY-RELEVANT BLOCKCHAIN CHARACTERISTICS

In Blockchain technology a distributed ledger framework is provided in which all transactions and system events are permanently recorded and chronologically ordered. Also Blockchain networks eliminate single points of failure by distributing data storage and validation across multiple nodes, which is the drawback of centralized systems. Because of this feature, the failure or compromise of an individual node does not disrupt overall system availability or integrity.

One of the most important point is Security in blockchain systems is enforced through consensus mechanisms, with the help of this before any transaction or state change is committed to the ledger it requires agreement among participating nodes. The risk of unauthorized modifications, fraudulent transactions, and data tampering is significantly reduces by consensus-based validation. Altering of historical records would require simultaneous manipulation of a majority of nodes, as the ledger is replicated across the network.

In blockchain security cryptographic techniques play a central role .Identity verification and transaction authentication, ensuring that only authorized entities can initiate or approve actions, which will done by Public-key cryptography . Hash functions provides Data integrity which associates blocks in a security sealed mechanism, where any data modification is instantly noticeable.

Blockchain enhances auditability, transparency as well as data protection. Firstly,real-time auditing and accountability are activated, they are not dependent on trusted intermediaries,. Immutably recorded blockchain transactions are autonomously confirmed by sanctioned members. In online gaming environments, properties like transaction legitimacy, fairness, asset ownership, are critical.

The programs which are self-executing that enforce conditions and predefined rules inevitably called Smart Contracts, the are supported by blockchain platforms. It permits translucent and safe implementation of asset transfers, in-game transactions and access controls and centralized oversight and manual intervention are strictly prohibited [2][7].

Blockchain is a robust foundation for enhancing the trust, security and an spirit of online gaming systems supported by these security-relevant characteristics.

IV. BLOCKCHAIN-BASED SOLUTIONS FOR ENHANCING GAMING SECURITY

a. Distributed Player Authentication

Identity mechanisms in blockchain technology use signatures rather than stored testimonials. It indicates that blockchains can replace passwords for user verification.

In gaming, the blockchain identity method is quite supportive. The management of private keys and consumption of secure access is for smoother operation. Blockchain identification systems noticeably diminishes the threat of credential theft and database hacking.

b. Blockchain-Safe Digital Asset Ownership

In-game items and collectibles are comparable by unique tokens and. Token creation is performed by ERC-721 technology we can more easily keep an unchanging record of who owns something thanks to this. It also helps guarantee that people claiming ownership of something are who they say they are.

This is good because without permission it does not let people just make copies of things. It can also make it more expensive to buy and sell these tokens. Sometimes it can take a while for the transaction to go through. So we have to be careful when we set up the system for buying and selling these game items and collectables.

c. Smart Contract–Controlled Transactions

Setting up in-game transactions to take place automatically makes things easier. This is due to the game's ability to act independently in specific situations. Additionally, it implies that you don't require assistance with the transactions. This makes it harder for people to cheat.

The benefit of smart contracts is that they clarify transactions. Games can be quite challenging. The game must therefore occasionally verify information on the blockchain. It must occasionally perform tasks on its own computer server. This makes the game function. It all comes down to ensuring that the game and smart contracts are compatible. For the game to function properly, smart contracts and the game must cooperate.

d. Game Integrity and Anti-Cheating Enforcement

Events and game outcomes can be recorded using unchangeable blockchain ledgers, which can make competitions more equitable by preventing people from altering the results after the game is ended and ensuring that scores are not altered without consent.

A combination of blockchain verification and other methods of tracking and analyzing events outside of the blockchain is typically required to detect cheating in real time. A lot of people act in this way.

e. Decentralized Gaming Infrastructure

Many nodes in gaming designs are assigned additional tasks to verify things. As a result, the system is more resilient against server and service-stopping threats. These kinds of nodes contribute to the smooth operation of the system. Multiple nodes are responsible for verification, which makes decentralized game infrastructures superior. Attacks such as denial-of-service and server-level attacks are less likely to occur.

V. THREAT-TO-MITIGATION ALIGNMENT

Cybersecurity Threat	Impact on Gaming Platforms	Blockchain-Based Mitigation Technique
Account	Identity theft,	Decentralized identity management

compromise	unauthorized purchases	using cryptographic signatures[7]
Digital asset theft / duplication	Economic imbalance, loss of ownership trust	Tokenized assets (NFTs) with immutable ownership records[6][8]
Cheating and score manipulation	Loss of fair competition	Immutable ledgers for recording game outcomes[1][5]
Financial fraud	Monetary loss, transaction disputes	Smart contract–based transaction enforcement[2][4]
Data tampering	Integrity loss, trust erosion	Cryptographic hash-linked ledger immutability[9][11]
DDoS and server outages	Service unavailability	Decentralized validation and distributed infrastructure

VI. LITERATURE REVIEW

Ref. No.	Research Focus	Application Domain	Key Contributions	Limitations / Research Gaps
[1]	Cryptocurrency systems	Blockchain foundations	Introduced blockchain as a decentralized, trustless ledger for digital currency transactions	Limited to financial use cases; no consideration of non-currency applications
[2], [3]	Decentralized computation and smart contracts	Distributed systems	Expanded blockchain usage beyond cryptocurrency through programmable smart contracts	Security threats and domain-specific constraints not deeply analyzed
[8]	Blockchain adoption in gaming	Online gaming platforms	Highlighted benefits such as digital asset ownership, transparency, and decentralization	Focuses mainly on feature descriptions; lacks security threat mitigation analysis
[7]	Blockchain-based Identity authentication	Gaming and digital identity	Proposed decentralized Authentication mechanisms to prevent identity fraud	Overlooks real-time performance and latency constraints in gaming environments
[6]	NFT-based asset ownership	Game asset management	Addresses asset duplication and ownership verification using NFTs	Does not address broader security threats such as cheating, DDoS attacks, or service disruption
Proposed Work	Threat-driven Blockchain Security framework	Online Gaming cybersecurity	Systematically maps cybersecurity threats to suitable blockchain mechanisms while considering integration feasibility	Addresses gaps identified in prior work

VII. FUTURE RESEARCH OPPORTUNITIES

For handling games that need to work in time and for applications that use both artificial intelligence and blockchain to stop cheating layer 2 scalability solutions are really important.

At the same time these layer 2 scalability solutions need to be able to work with games and artificial intelligence, and blockchain applications.

Also we need to learn more about how to keep people's information private when they are playing games online, like using codes that do not give away any secrets and also how to make sure that games can work on different platforms.

This will help many peoples to start using these Layer 2 scalability solutions, intelligence and blockchain applications for their games.

VIII. CONCLUSION

This study shows that serious limitations of integrated system designs are overcome by blockchain technology which offers vital security advantages for online gaming platforms. Through diverse techniques like cryptographic verification, transparent transaction validation, immutable recordkeeping, and. Decentralization. Common cyber security threats such as asset theft, account manipulation, unauthorized, and digital data modification are significantly reduced by blockchain features. These technical properties improves accountability,trust, and ownership assurance within gaming ecosystems.

The online gaming platforms must be integrated with blockchain and with selective approach only. While blockchain improves security and auditability, its inherent latency, scalability constraints, and computational overhead limit its suitability for real-time gameplay operations. Subsequently, blockchain is best applied to security-sensitive components such as identity management, asset ownership, transaction verification, and audit logging, rather than core gameplay mechanics that demand low-latency processing.

This study's main contribution is to provide a security-focused assessment of blockchain for online gaming, highlighting its function as an additional security layer rather than a stand-alone fix. This paper promotes hybrid security architectures that combine blockchain with traditional high-performance systems to achieve both robustness and real-time responsiveness by highlighting the advantages and disadvantages of blockchain-based security mechanisms. In order to protect next-generation online gaming platforms from changing cyber threats, such adaptive and layered security models offer a practical and efficient approach.

REFERENCES

1. Nakamoto S, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
2. Buterin V, A Next-Generation Smart Contract and Decentralized Application Platform, Ethereum White Paper, 2014.
3. P. Pattanayak, M. Crosby, V. Kalyanaraman, S. Verma, “Blockchain technology: Beyond bitcoin,” Applied Innovation Review, no. 2, pp. 6–19, 2016.
4. M. Devetsikiotis and K. Christidis, “Blockchains and smart contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
5. D. He, Q. Feng, K. Liang, S. Zeadally, “A survey on privacy protection in blockchain systems,” IEEE Internet Computing, vol. 23, no. 5, pp. 36–45, Sep.–Oct. 2019.
6. D. Shirley, J. Evans, W. Entriken , N. Sachs, “ERC-721 non-fungible token standard,” Ethereum Foundation, 2018.
7. Z. Gao, L. Xu, L. Chen, “A secure identity authentication mechanism based on blockchain technology,” IEEE Access, vol. 7, pp. 115–123, 2019.
8. A. Zhang, J. Zhang, Y. Wang, “A survey on blockchain-based gaming,” IEEE Access, vol. 8, pp. 215–234, 2020.
9. S. S. Kanhere, R. Jurdak , A. Dorri, “Blockchain in Internet of Things: Challenges and solutions,” IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 173–201, 2017.
10. A. Narayanan, A. Miller, J. Bonneau, J. Clark, J. Kroll, and E. Felten, “SoK: Research perspectives and challenges for bitcoin and cryptocurrencies,” in Proc. IEEE Symp. on Security and Privacy, 2015, pp. 104–121.
11. M. Al-Bassam, “Scalable and decentralized online games using blockchain,” in Proc. IEEE Int. Conf. on Blockchain, 2018, pp. 1–8.
12. N. Kumar, K. R. Choo, S. Singh, “Blockchain-based secure data storage for online applications,” IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2333–2342, Apr. 2019.