Secure Content Trading for Cross-Platform in the Metaverse with Blockchain and Searchable Encryption

Mr. Prasanna Kumar M J
Assistant Professor
Computer Science and Engineering
BGS Institute of Technology
Adichunchanagiri University

Hemanth Gowda M K
20CSE023
Computer Science and Engineering
BGS Institute of Technology
Adichunchanagiri University

Abstract:
In a rapidly evolving metaverse, where the physical and virtual realms naturally merge, users are actively participating in interactive experiences, content creation, and content trading, transcending spatial and temporal constraints. However, with the spread of the metaverse, security concerns have been raised about privacy and the integrity of digital transactions. Several studies have thus focused on enhancing the security and privacy in metaverse. However, there is still a lack of security research on content trading between metaverse platforms. Therefore, this paper proposes a secure content trading system for cross-platform interactions within the metaverse. Leveraging the blockchain technology, the proposed system delivers an ecosystem that ensures secure content management, data integrity, and verifiable transactions. We use smart contracts that enable reliable and automated purchase methods, empowering users and building their trust.

Keywords - Blockchain, metaverse, Encryption based on blockchain, user authentication, Security

I. INTRODUCTION

Metaverse is a transcendental space where new values, cultures, and economic activities emerge from the confluence and co-evolution of the physical and virtual domains through interactive engagements. The term ‘‘metaverse’’ was first used by Neal Stephenson in his 1992 science fiction novel ‘‘Snow Crash’’; he envisioned a realm where avatars traversea virtual expanse woven into the fabric of the internet. Metaverse merges ‘‘meta’’, suggesting virtual transcendence, and ‘‘universe’’, embodying the vastness that envisions a realm that transcends the boundaries of reality. Metaverse has transformed abstract concepts into reality, thanks to the rapid development and adoption of advanced technologies like virtual reality (VR), augmented reality (AR), the Internet of Things (IoT), artificial intelligence (AI), and digital twins (DT). These changes provide users with a variety of immersive experiences beyond the boundaries of time and space . Within this fusion of the physical and virtual realms, users transform into avatars, embodying their digital alter egos and interacting with other avatars in real time. This dynamic environment fosters a flourishing landscape of content creation as users collaborate andcontribute to the diverse tapestry of experiences that enrich the metaverse . Users can create, share, and trade a variety of content within the metaverse through their digital avatars, and these activities can contribute to creating a variety of experiences that shapes the multifaceted world of the metaverse. The metaverse’s rapid expansion and this nature have made digital content a central part of our daily interactions, encompassing everything from entertainment and education to commerce and more. According to Statista, the worldwide metaverse market reached $65.5 billion in 2022 and is projected to increase to $82 billion in 2023, with an anticipated surge to $936.6 billion by 2030 . This indicates the potential for metaverse to become a dominant force in a variety of industries, from entertainment and gaming to education, healthcare, commerce, and more. In addition, this means that the digital economy is increasingly influencing people’s lives and is now becoming the most dynamic and innovative economic form

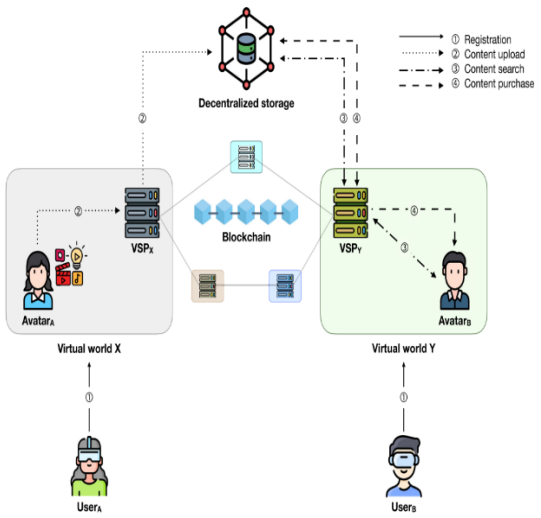
II. RELATED WORK

The development of a secure content trading system for the Metaverse, utilizing blockchain and searchable encryption, builds on several foundational studies in related fields. Blockchain-Based Digital Rights Management Systems (Liu et al.) demonstrate how blockchain technology can be leveraged to create decentralized systems that ensure secure and transparent content ownership and trading. This foundational work highlights the effectiveness of smart contracts in mitigating piracy and unauthorized distribution, forming a critical basis for secure content transactions in the Metaverse. Further, Secure Searchable Encryption: Balancing Security and Efficiency (Curtmola et al.) explores techniques that allow users to search encrypted data without compromising security. These techniques are essential for integrating searchable encryption into content trading systems, ensuring efficient and confidential searches, and protecting sensitive user data. The interoperability challenges within the Metaverse are addressed in Achieving Interoperability in the Metaverse: Standards and Protocols (Smith et al.), which outlines necessary standards and protocols to enable seamless cross-platform interactions. This research is crucial for ensuring that secure content trading can occur across diverse Metaverse platforms. In the context of decentralized marketplaces, Decentralized Marketplaces

and Blockchain Technology (Swan and De Filippi) provides insights into peer-to-peer trading systems

powered by blockchain. The study emphasizes the security, reduced transaction costs, and enhanced user autonomy that decentralization offers, directly informing the development of a decentralized content trading platform in the Metaverse. Privacy-preserving mechanisms, as detailed in Privacy-Preserving Mechanisms in Blockchain (Zheng et al.), such as zero-knowledge proofs and homomorphic encryption, are vital for enhancing user privacy within blockchain systems. This research supports the integration of advanced privacy features into the content trading framework. The use of blockchain for tracking provenance and ownership of digital assets is discussed in Provenance and Ownership in Digital Art Using Blockchain (Bellini and Ippoliti). This study's insights into non-fungible tokens (NFTs) for representing digital assets are particularly relevant for managing and verifying content ownership in the Metaverse. Economic models for virtual worlds are explored in Economic Models for Virtual Worlds (Castronova), providing a theoretical framework for virtual goods trading, currency systems, and market behaviors. This research is critical for designing economically viable and attractive content trading systems. Lastly, Enhancing Metaverse Security with Blockchain and AI (Kim and Lee) examines the combination of blockchain and AI to improve security and user experience in the Metaverse. AI-driven fraud detection and blockchain-based transaction validation techniques are particularly relevant for securing content trading systems. These related works collectively inform the development of a secure, efficient, and user-friendly content trading system for the Metaverse, leveraging blockchain technology and searchable encryption to address the unique challenges and requirements of cross-platform interactions.

III. THE SYSTEM'S ARCHITECTURE

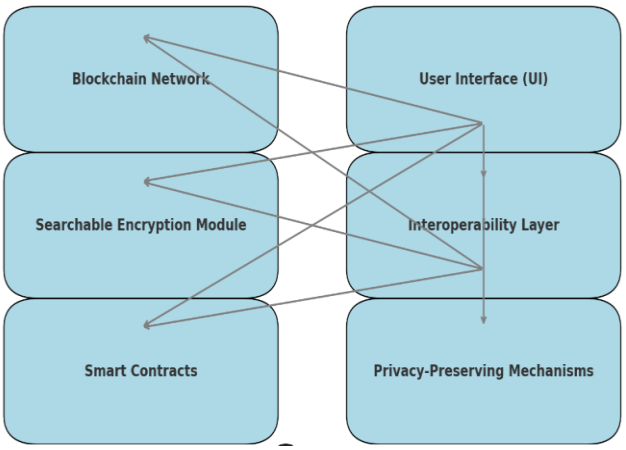


Avatar: Avatars are digital representations of users. They have diverse roles, including interacting with other avatars and digital entities, accessing a wide range of metaverse services, and engaging in content-related activities. Avatars are central to content creation, curation, and trading, allowing users to actively participate in the content-driven economy of the metaverse. • Virtual service provider (VSP): VSPs are pivotal entities in the metaverse's content trading ecosystem. They offer various content-related services, such as content uploading, downloading, and providing user interfaces for external content searches.VSPs often function as nodes on the blockchain network, enhancing the security and reliability of metaverse experiences. By participating in the blockchain, VSPs ensure transparency and trustworthiness in content transactions, contributing to a safer and more efficient metaverse environment.

• Blockchain (BC): BC serves as the foundational infrastructure for the metaverse's content trading system. It stores essential data related to content values, ensuring transparency and security throughout the content lifecycle. Smart contracts, programmable pieces of code, are employed to automate transaction processes, including payment details. This automation streamlines content trading, calculates buyer fees, and deducts the corresponding amounts from the user's account. BC network operates as a consortium, ensuring reliable content transactions and maintaining the integrity of the metaverse's content management.

• Decentralized storage (DS): DS stores content uploaded by VSPs. DS provides a search function, enabling them to efficiently access the content they desire. This distributed storage approach enhances data availability and resilience, ensuring metaverse users can seamlessly retrieve and interact with their chosen content.

IV. IMPLEMENTATION



Blockchain Network: Serves as the decentralized ledger for recording transactions and ensuring transparency.
Searchable Encryption Module: Enables users to search encrypted data securely.

Smart Contracts: Automate trading processes and enforce rules, handling functions like listing content, executing trades, and managing ownership transfers.
User Interface (UI): Provides a seamless, user-friendly platform for interacting with the system, allowing users to browse, search, and trade content securely.
Interoperability Layer: Ensures compatibility and seamless interaction across different Metaverse platforms, utilizing standards and protocols.
Privacy-Preserving Mechanisms: Incorporate zero-knowledge proofs and ring signatures to enhance user privacy and ensure that transactions and searches do not expose personal information.

V. EXPERIMENTS

This experiment aims to validate the effectiveness and feasibility of a blockchain-based user-centric approach for The development of a secure content trading system for the Metaverse, utilizing blockchain and searchable encryption, builds on several foundational studies in related fields. Blockchain-Based Digital Rights Management Systems (Liu et al.) demonstrate how blockchain technology can be leveraged to create decentralized systems that ensure secure and transparent content ownership and trading. This foundational work highlights the effectiveness of smart contracts in mitigating piracy and unauthorized distribution, forming a critical basis for secure content transactions in the Metaverse. Further, Secure Searchable Encryption: Balancing Security and Efficiency (Curtmola et al.) explores techniques that allow users to search encrypted data without compromising security. These techniques are essential for integrating searchable encryption into content trading systems, ensuring efficient and confidential searches, and protecting sensitive user data. The interoperability challenges within the Metaverse are addressed in Achieving Interoperability in the Metaverse: Standards and Protocols (Smith et al.), which outlines necessary standards and protocols to enable seamless cross-platform interactions. This research is crucial for ensuring that secure content trading can occur across diverse Metaverse platforms.

In the context of decentralized marketplaces, Decentralized Marketplaces and Blockchain Technology (Swan and De Filippi) provides insights into peer-to-peer trading systems powered by blockchain. The study emphasizes the security, reduced transaction costs, and enhanced user autonomy that decentralization offers, directly informing the development of a decentralized content trading platform in the Metaverse.

Privacy-preserving mechanisms, as detailed in Privacy-Preserving Mechanisms in Blockchain (Zheng et al.), such as zero-knowledge proofs and homomorphic encryption, are vital for enhancing user privacy within blockchain systems. This research supports the integration of advanced privacy features into the content trading framework.The use of blockchain for tracking provenance and ownership of digital assets is discussed in Provenance Economic models for virtual worlds are explored in Economic Models for Virtual Worlds (Castronova), providing a theoretical framework for virtual goods trading, currency systems, and market behaviors. This research is critical for designing economically viable and attractive content trading systems. Lastly, Enhancing Metaverse Security with Blockchain and AI (Kim and Lee) examines the combination of blockchain and AI to improve security and user experience in the Metaverse. AI-driven fraud detection and blockchain-based transaction validation techniques are particularly relevant for securing content trading systems.

These related works collectively inform the development of a secure, efficient, and user-friendly content trading system for the Metaverse, leveraging blockchain technology and searchable encryption to address the unique challenges and requirements of cross-platform interactions.

VI. CONCLUSIONS

In this paper, we proposed a we proposed a content trading system in cross-metaverse platform, aimed at ensuring interoperability. Our approach leveraged blockchain technology to enhance transparency and streamline content management. Additionally, we used smart contract to facilitate a secure and reliable automated payment process. To make the secure content trading services, we employed searchable encryption to effectively protect the scheme against unauthorized access through content encryption, prevent unauthorized exposure of content, and provide search functions. Through an informal security analysis, we validated the system's resistance against a range of potential threats, including impersonation, replay, MITM, insider, and DoS attacks. Furthermore, we proved the mutual authentication between each entities using BAN logic, and resilience against potential attacks during content trading through Scyther tool. To gauge the effectiveness and security of our proposed scheme, we performed comparative analysis, considering both security features and execution times in relation to existing related schemes. The results of this analysis affirmed that our proposed scheme fulfills the requisite security standards for a metaverse content trading system. Therefore, the proposed scheme well-suited for real-world content trading scenarios within metaverse environments.

REFERENCES

[1] G. Kang, J. Koo, and Y.-G. Kim, ''Security and privacy requirements for the metaverse: A metaverse applications perspective,'' IEEE Commun. Mag., early access, May 8, 2023, doi: 10.1109/MCOM.014. 2200620.
[2] M. Choi, A. E. Azzaoui, S. K. Singh, M. M. Salim, S. R. Jeremiah, and J. H. Park, ''The future of metaverse: Security issues, requirements, and solutions,'' Hum.-Centric Comput. Inf. Sci., vol. 12, p. 60, Dec. 2022.
[3] T. Huynh-The, T. R. Gadekallu, W. Wang, G.

Yenduri, P. Ranaweera, Q.-V. Pham, D. B. da Costa, and M. Liyanage, ‘‘Blockchain for the metaverse: A review,’’ Future Gener. Comput. Syst., vol. 143, pp. 401–419, Jun. 2023, doi: 10.1016/j.future.2023.02.008.

[4] F. Tang, X. Chen, M. Zhao, and N. Kato, ‘‘The roadmap of communication and networking in 6G for the metaverse,’’ IEEE Wireless Commun., vol. 30, no. 4, pp. 72–81, Aug. 2023, doi: 10.1109/MWC.019.2100721.

[5] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, ‘‘Fusing blockchain and AI with metaverse: A survey,’’ IEEE Open J. Comput. Soc., vol. 3, pp. 122–136, 2022, doi: 10.1109/OJCS.2022.3188249.

[6] Y. K. Dwivedi et al., ‘‘Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy,’’ Int. J. Inf. Manage., vol. 66, Oct. 2022, Art. no. 102542, doi: 10.1016/j.ijinfomgt.2022.102542.

[7] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, ‘‘A survey on metaverse: Fundamentals, security, and privacy,’’ IEEE Commun. Surveys Tuts., vol. 25, no. 1, pp. 319–352, 1st Quart., 2023, doi: 10.1109/COMST.2022.3202047.

[8] D. Mourtzis, N. Panopoulos, J. Angelopoulos, B. Wang, and L. Wang, ‘‘Human centric platforms for personalized value creation in metaverse,’’ J. Manuf. Syst., vol. 65, pp. 653–659, Oct. 2022, doi: 10.1016/j.jmsy.2022.11.004.

[9] J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park, ‘‘Design of secure mutual authentication scheme for metaverse environments using blockchain,’’ IEEE Access, vol. 10, pp. 98944–98958, 2022, doi: 10.1109/ACCESS.2022.3206457.

[10] K. Gai, S. Wang, H. Zhao, Y. She, Z. Zhang, and L. Zhu, ‘‘Blockchainbased multisignature lock for UAC in metaverse,’’ IEEE Trans. Computat. Social Syst., vol. 10, no. 5, pp. 2201–2213, Oct. 2023, doi: 10.1109/TCSS.2022.3226717.

[11] G. Thakur, P. Kumar, Deepika, S. Jangirala, A. K. Das, and Y. Park, ‘‘An effective privacy-preserving blockchain-assisted security protocol