Hybrid Blockchain for Secure Data Sharing in Digital Twin Systems: Challenges and Opportunities

Chimeremma Sandra Amadi Md Raihan Subhan Dong-Seong Kim Taesoo Jun
Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea
chimesandra@yahoo.com, (raihan, dskim, taesoo.jun)@kumoh.ac.kr

***Abstract*—This paper examines the role of hybrid blockchain in enhancing data-sharing security for digital twin (DT) emerging applications. Traditional blockchain security methods struggle with the privacy, scalability, and interoperability needs in DT. However, by combining public and private blockchains, the hybrid blockchain system can resolve these issues, offering transparency, energy efficiency, and improved latency. Key result prove that hybrid blockchain enables fully secure and optimized data sharing in DT applications.**

***Index Terms*—Blockchain, Data Sharing, Digital Twin, Hybrid blockchain.**

I. INTRODUCTION

Collaborative data sharing has become essential for solving complex industry challenges, with the Organization for Economic Co-operation and Development (OECD) estimating a potential 2.5% gross domestic product (GDP) boost through effective data-sharing frameworks [1]. Regulatory moves like the EU's 2023 Data Act support this trend by promoting fair data access for innovation [2]. However, secure data sharing faces privacy, security, and interoperability hurdles, particularly in critical sectors [3]. The Internet of DT (IoDT) enables dynamic data exchange but requires strong security due to its complex and decentralized architecture.

Blockchain technology, known for enhancing data integrity through tamper resistance and smart contracts, has been proposed as a solution [4]. However, traditional blockchain systems often lack the scalability and flexibility required for large-scale applications [5]. This review explores hybrid blockchain as a more adaptable alternative, potentially offering secure, scalable, and efficient data sharing in DT networks. Fig 1 provides a high-level hybrid blockchain system model.

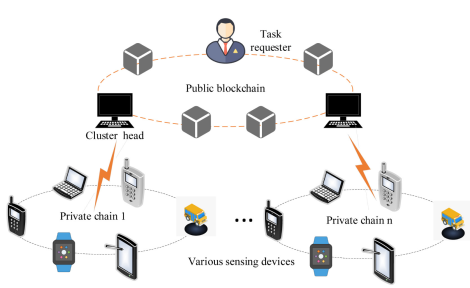

Fig. 1. High-level hybrid blockchain system model with integral components.

II. TRADITIONAL BLOCKCHAIN FOR DT DATA SHARING

Data sharing is essential in DT applications, enabling real-time synchronization between virtual models and physical entities across industries such as manufacturing, healthcare, smart cities, and aerospace [6]. DTs gather data from sensors, operational logs, and external factors, providing insights into current and predictive behaviors [7]. Table I highlights some DT data sharing applications across sectors.

TABLE I
DATA SHARING IN DT APPLICATION SECTORS

Sector	Purpose	Data Requirements
Manufacturing	Optimize production	Real-time sensor data
Healthcare	Diagnosis	Patient health data
Smart Cities	monitoring	IoT sensor data
Logistics	route optimization	Vehicle sensor data
Aerospace	Safety monitoring	Real-time telemetry data

Data sharing is integral to DT systems, and critical challenges may be introduced during the interaction of the physical and digital entities. Key concerns include data interoperability, digital twin architectural issues, latency, governance and data ownership, security and privacy problems, and secure communication [8]. Table II highlights some of these key concerns in DT data sharing.

Blockchain technology has become essential in enhancing the security of data within DT systems, overcoming limitations of traditional data security methods such as centralized access control, encryption, and firewalls [9]. Blockchain's decentralized, immutable, and transparent nature ensures data integrity and availability by preventing single points of failure, making it resilient to DDoS attacks [10]. However, conventional blockchain architectures face challenges, particularly around scalability, energy consumption, latency, privacy, and storage demands [11]. These issues hinder the ability of blockchain to manage high transaction volumes required by DT, creating conflict with the energy efficiency crucial to these applications.

III. HYBRID BLOCKCHAIN FOR DT DATA SHARING

Hybrid blockchain architectures present a solution by combining public and private blockchains to address scalability, energy, and privacy concerns [12]. Sensitive data can be managed by the private blockchain, while critical records are stored on the public blockchain for transparency. This dual-layer setup enables selective data sharing, reduces transaction load, improves latency, supports sensitive data modifications, and uses energy-efficient consensus algorithms (e.g., PoS) to

TABLE II
DT TECHNOLOGY AND DATA SHARING CHALLENGES

Aspect	Description	Challenges
DT Architecture	DTs replicate physical entities through data-driven and simulation models to enable real-time monitoring and optimization.	- Managing complex communication between physical and virtual entities. - Achieving real-time synchronization.
Data Interoperability	Integration of heterogeneous data sources, including sensors, IoT devices, and external systems.	- Inconsistent data formats (JSON, XML, OPC-UA). - Lack of standardized APIs and protocols across platforms.
Security and Privacy	Continuous exchange of sensitive operational and personal data introduces cybersecurity risks.	- Unauthorized access, MitM attacks, and insider threats. - Compliance with GDPR, HIPAA, and privacy laws.
Latency and Real-Time Data Exchange	Ensures low-latency communication between physical assets and DTs to maintain accurate simulations.	- Network congestion and bandwidth limitations. - Time synchronization issues across distributed systems.
Scalability	Managing large volumes of real-time data as the number of connected devices and data streams increases.	- Performance bottlenecks in centralized models. - Consistency challenges in distributed architectures.
Governance and Data Ownership	Establishes rules for data access, ownership, and usage across multi-stakeholder ecosystems.	- Ambiguous ownership across entities. - Difficulties in defining access control policies and governance frameworks.
Reliability and Fault Tolerance	DTs must maintain continuous synchronization and system integrity under all conditions.	- Single points of failure in centralized systems. - Network disruptions causing data loss or delays.

further reduce costs. Hybrid blockchains enable fine-grained access control, fostering secure collaboration among multiple stakeholders.

TABLE III
HYBRID BLOCKCHAIN ARCHITECTURE FOR DIGITAL TWIN SYSTEMS

Key Aspect	Description
Scalability	Selective data sharing
Energy Efficiency	Energy-saving consensus (e.g., PoS, PBFT).
Reduced Latency	Private chain handles real-time data, ensuring quick response, while the public chain maintains secure, immutable records.
Privacy and Transparency	Stores sensitive data on private chain for restricted access; public chain handles non-sensitive, hashed data for auditability.
Enhanced Trust and Access Control	Provides fine-grained access control for secure collaboration; public chain offers a trusted record.

IV. Open Issues

Open issues in hybrid blockchain applications include ensuring interoperability between public and private blockchains, as differing data structures complicate synchronization, hence leading to integration complexity. Additionally, hybrid blockchain is resource-intensive, posing cost and scalability barriers, especially for large-scale DT ecosystems.

V. Conclusion

This paper highlights hybrid blockchain as a robust solution to secure data sharing in DT systems, addressing the limitations of traditional security methods. By leveraging both public and private chains, hybrid architectures enhance scalability, privacy, and energy efficiency, crucial for real-time DT applications. The result prove that hybrid blockchain enables fully secure and optimized data sharing in DT ecosystems.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korea government(MSIT) (IITP-2024-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program(IITP-2024-RS-2024-00438430, 34%) supervised by the IITP.

References

[1] S. G. Team, "Data sharing — challenges and opportunities," Data sharing — Challenges and Opportunities, 2024.

[2] C. François, S. d. B. Guillaume, Z. M. David, C. S. Harsha, and M. Aguiar, "The benefits of data sharing now outweigh the risks," /2024/the-benefits-of-data-sharing-now-outweigh-the-risks, 2024, accessed: 2024-09-16.

[3] R. Abraham, N. Dougal, and D. Patrick, "Sharing of military veterans' mental health data across canada: A scoping review," *The Journal of Military, Veteran and Family Health*, vol. 8, pp. 7–17, 2022.

[4] I. S. Igboanusi, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Vlc-uwb hybrid (vuh) network for indoor industrial robots at military warehouses / distribution centers," in *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, 2019, pp. 762–766.

[5] S. O. Ajakwe, I. I. Saviour, V. U. Ihekoronye, O. U. Nwankwo, M. A. Dini, I. U. Uchechi, D.-S. Kim, and J. M. Lee, "Medical iot record security and blockchain: Systematic review of milieu, milestones, and momentum," *Big Data and Cognitive Computing*, vol. 8, no. 9, p. 121, 2024.

[6] A. Rasheed, O. San, and T. Kvamsdal, "Digital twin: Values, challenges and enablers from a modeling perspective," *IEEE access*, vol. 8, pp. 21 980–22 012, 2020.

[7] W. Hu, T. Zhang, X. Deng, Z. Liu, and J. Tan, "Digital twin: A state-of-the-art review of its enabling technologies, applications and challenges," *Journal of Intelligent Manufacturing and Special Equipment*, vol. 2, no. 1, pp. 1–34, 2021.

[8] C. Alcaraz and J. Lopez, "Digital twin: A comprehensive survey of security threats," *IEEE Communications Surveys Tutorials*, vol. 24, no. 3, pp. 1475–1503, 2022.

[9] A. F. Mendi, T. Erol, and D. Doğan, "Digital twin in the military field," *IEEE Internet Computing*, vol. 26, no. 5, pp. 33–40, 2022.

[10] G. Diamantopoulos, N. Tziritas, R. Bahsoon, and G. Theodoropoulos, "Dynamic data-driven digital twins for blockchain systems," in *Dynamic Data Driven Applications Systems*, E. Blasch, F. Darema, and A. Aved, Eds. Cham: Springer Nature Switzerland, 2024, pp. 283–292.

[11] A. Altaf, F. Iqbal, R. Latif, B. M. Yakubu, S. Latif, and H. Samiullah, "A survey of blockchain technology: Architecture, applied domains, platforms, and security threats," *Social Science Computer Review*, vol. 41, no. 5, pp. 1941–1962, 2023.

[12] K. Venkatesan and S. B. Rahayu, "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques," *Scientific Reports*, vol. 14, no. 1, p. 1149, 2024.