Direct Research Journal of Engineering and Information Technology

Vol. 13(3), Pp. 29-34, September 2025,

Research Article
ISSN: 2354-4155
https://journals.directresearchpublisher.org/index.php/drjeit; https://www.ajol.info/index.php/drjeit

Trends in the Application of Blockchain Technology to the Internet of Medical Things (IoMT)

Leke Joseph Oloruntoba[1], and Afolayan Obiniyi[2]

[1]Computer Engineering department, Kogi State Polytechnic, Kogi State, Nigeria.
[2]Computer science department, Federal University Lokoja, Kogi State, Nigeria.
*Corresponding author email: lekejoe@gmail.com; afolayan.obiniyi@fulokoja.edu.ng

ABSTRACT

The integration of blockchain technology with the Internet of Medical Things (IoMT) has seen many changes and evolutions, with the last couple of years really witnessing an upward trajectory in growth and innovation. This paper offers a detailed review of the most recent trends in this area, with a focus on how blockchain technology is solving some of the long-standing problems of IoMT like data privacy, interoperability, security, and scalability. Some key trends discussed are lightweight blockchain architecture, integration of federated learning with blockchain, off-chain and distributed storage systems based on IPFS, and emerging post-quantum cryptographic tools for enhanced security. The review also captures current research trends in academia and industry, including healthcare edge computing, energy-efficient consensus, and smart contract automation. This paper offers a timeline for development, thematic analysis of trends, and areas for productive investigation into the realization of secure, scalable, and interoperable IoMT systems.

Keywords: *Blockchain, Internet of Medical Things, IoMT Security, Federated Learning, Smart Contracts, Post-Quantum Cryptography*

Article information
Received 10 July 2025
Accepted 17 September 2025
Published 26 September 2025
https://doi.org/10.26765/DRJEIT45720746135

Citation: Oloruntoba, L. J., Obiniyi, A. (2025). Trends in the Application of Blockchain Technology to the Internet of Medical Things (IoMT). Direct Research Journal of Engineering and Information Technology, 13(3), 29-34. This article is published under the terms of the Creative Commons Attribution License 4.0.

INTRODUCTION

Internet of Medical Things (IoMT) is considered a paradigm shift in healthcare where it connects wearable devices, implantable sensors, remote monitoring devices, and cloud-based analytics platforms (Mishra & Singh, 2023). Interconnection brings in critical challenges related to data integrity, security, real-time access, and interoperability. Being decentralized, immutable, and transparent, the blockchain has surfaced as the security enabler for IoMT ecosystems. The last decade, however, has witnessed landmark changes in applying blockchain to IoMT (Ghadi et al., 2024). From the very basic logging of patient records in earlier days to today's highly sophisticated decentralized ecosystems using smart contracts and AI, such changes in design and deployment approaches represent a larger paradigm shift (Puri et al., 2024). Such shifts are reshaping technical solutions and

altering the models for compliance, governance, and integration within the healthcare domain.

Background to the Study

The IoMT Overview

The IoMT constitutes a network of medical devices and applications interfacing with healthcare IT systems via online networks (Shafiq et al., 2023). This allows for continuous monitoring of the patient's health, real-time diagnoses, and medical response in advance. Islam (2023), emphasize that the high volume and sensitivity of data generated from IoMT devices demands high-grade security, privacy, and efficient data management.

Blockchain Basics

The blockchain is a distributed database technology that allows secure, transparent, thwart-proof blocking of transactions, secured through cryptography, and validated through the consensus mechanism among decentralized nodes (Ali et al., 2025). Primarily meant for cryptocurrency, blockchain is currently being adapted for various applications, including the healthcare sector. Yet, traditional blockchain systems require considerable energy, lack scalability, and impose latency-their limitations are heightened under the resource constraints imposed by IoMT environments.

Intersection of Blockchain and IoMT

Previous research and implementation of blockchain into IoMT: With the rapid evolution of the Internet of Medical Things (IoMT), researchers have begun to pay serious attention into integration of blockchain technology with IoMT, especially regarding its benefits relating to major challenges like data security, interoperability, and scalability. This has motivated several studies and practical applications about how blockchain can transform healthcare systems that rely on IoMT.

Blockchain for Securing IoMT Data: There are numerous studies advocating for the installation of blockchain technology to give strength to IoMT systems through immutable data storage and secure communication channels. Gladyr (2021) advanced a blockchain-based architecture to protect patient-generated data from wearables. There are systems that ensure data integrity with cryptography techniques that avoid access by unauthorized entities (Abbasi et al., 2021). Computer solutions like Guardtime's KSI have already deployed their capabilities in securing EHRs and IoMT field data in current real-life healthcare environments (Suraci et al., 2022).

Blockchain for IoMT Inter-operability: Interoperability among heterogeneous IoMT devices and systems is a longstanding challenge in healthcare. Blockchain is proposed for this purpose as a future enabler for seamless data exchange. Sharma et al., (2020) have presented a blockchain framework for IoMT device interactions and sharing activity. The proposed model utilizes smart contracts to the automated processing of secure data exchange. This is further illustrated in the use of MedRec, an MIT Media Lab system that employs blockchain technologies to generate the one unified patient record thereby providing inter-operability with health care providers. Blockchain to Preserve Privacy in IoMT: Due to its decentralized and cryptographic nature, such types of devices prove beneficial in preserving patient privacy from this IoMT ecosystem. Khan et al. (2022) proposed a blockchain Hyperledger fabric enabled consortium architecture referred to as BIoMT which offers security, integrity, transparency and accountability to health-related transactions and exchanges of sensitive clinical information in an environment of distributed and decentralized and secure by design and without the use of server technology. A consensus is designed and designed to help decrease the impact of such limitations of blockchain applications within IoMT environments. Specific individual health transactions before sharing in the system are protected using the NuCypher Re-Encryption mechanisms that augments security and offers clarity and reliability to the medical dictation records.

Blockchain in IoMT for Supply Chain Transparency: Blockchain is applied to track the lifecycle of IoMT devices and medical supplies by promoting transparency and authenticity. Liu et al. (2021) Proposed a unified platform of Blockchain and Internet of Things-based smart tracking and tracing (abbreviated as BIoT3) spanning five layers, which acts as a decentralized solution for traceability in the drug supply chain. Blockchain Transparent Supply has been employed for case studies related to medical equipment supply chains, ensuring the quality control of these respective lines and traceability (Sunny et al., 2020). These studies prove that significant innovations in problem solving are brought about by blockchain in the face of challenges for IoMT systems. From secure data storage, accessibility to privacy-preserving interoperability that guarantee supply chains to be transparent, these technologies have proven vital for enabling the next generation of healthcare systems dependent upon IoMT.

METHODOLOGY

The review of this work was conducted using scholarly sources and peer-reviewed journals. The analysis was devised to identify the trends of blockchain implementation within IoMT in five domains, i.e. lightweight architecture, federated learning integration, storage and data sharing, privacy frameworks, and consortium governance models. Each paper was scrutinized to learn about the changes in approach and the emerging areas of focus.

Review of Related Works

The recent literature reflects an increasing interest in the

synergy of blockchain and Internet of Medical Things or IoMT to address issues of data security, interoperability, privacy, and system efficiency.

Liao et al. (2025) introduced the Lightweight Sharding Blockchain Snapshot Pruning (LSBSP) method, combining dual-chain architecture and snapshot pruning to overcome synchronization latency and improve storage efficiency of the data in IoMT systems. Their work applies significantly to today's trend toward lightweight blockchain architectures for resource-constrained medical devices.

Similarly, Khajehzadeh et al. (2024) introduced L2AI, a lightweight three-factor authentication scheme based on blockchain. Their scheme secures data access control without burdening energy-constrained IoMT sensors, highlighting the necessity of authentication systems with requirements of security and performance.

Blockchain integrated with federated learning is another prominent development in this field. In today's world, data is being generated from a plethora of different sources. Smartphones, autonomous vehicles, wearable devices, and plenty of sensors are just a few examples. FL is a machine learning method that uses data from multiple devices or institutions (known as clients), allowing them to train a model collectively without needing to transmit their underlying data. Dhasaratha et al. (2024) developed a federated blockchain platform to facilitate privacy-preserving model training and safe data sharing among several healthcare organizations. Their work aims at collaborative intelligence without violating patient confidentiality, which is an increasing requirement for AI-based healthcare services.

Fending off quantum-age attacks, by using post-quantum cryptography (PQC) so that the security of transactions, data and the system are not compromised by quantum computers. El Haddouti et al. (2024) proposed a blockchain system secured by post-quantum cryptography schemes. Their approach offers long-term security resilience, and their work is a milestone for blockchain research in next-generation healthcare systems.

In the context of effective and secure storage of data, Li et al. (2023) proposed combining InterPlanetary File System (IPFS) with Ethereum for off-chain storage of large medical files with blockchain-based traceability. This kind of architecture increases storage and system throughput in real-time medical applications.

Rahman et al. (2024) highlighted the use of smart contracts for managing consent, enabling automated legal compliance and privacy policy enforcement in decentralized IoMT networks. Their research highlights the importance of regulatory-conscious blockchain technology in healthcare.

Finally, ok et al. (2025) proposed an energy-efficient consensus protocol that reduces the immediate power consumption issues of blockchain-based IoMT devices. Such mechanisms as Proof-of-Authority (PoA) are particularly well-suited to small-scale, real-time medical environments.

Combined, these studies constitute a heterogeneous and forward-looking corpus that mirrors the dominant trends in blockchain-IoMT research. They highlight the shift away from monolithic, one-size-fits-all systems towards modular, scalable, and privacy-preserving frameworks that can effectively support the tailored needs of today's healthcare systems.

Evolution and Application of Trends in Blockchain Integration with IoMT

The conjunction of blockchain with IoMT has not been stagnant; it underwent a few phases of development, corresponding to changes in these two technologies and the demand from modern healthcare. In early days, the focus was basically on securing medical data and ensuring its integrity, whereas recent developments aimed at interoperability, scalability, and real-time decision support. These trends show how blockchain is slowly permeating IoMT applications, which range from patient monitoring and telemedicine to medical supply chain management and predictive healthcare. The following subsections explain this evolution and shoot through the major application areas upon which current and emerging practices are based.

Trend Evolution in Blockchain-IoMT Applications (2017–2025)

This Figure 1 narrates the progressive maturity of blockchain trends applied to the Internet of Medical Things (IoMT).

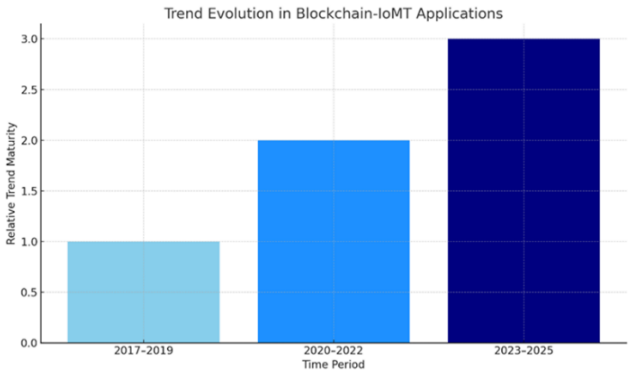

Figure 1: Trend evolution in blockchain-IoMT Applications

a) 2017–2019 period is the earliest adoption phase with applications focused on basic record-keeping and static ledgers (Yaga et al., 2018; Lipton et al 2018).

b) 2020–2022 period observes trends of smart-contracts and decentralized access control mechanisms with enhancement of automation and governance on data (Hewa et al., 2021)

c) 2023–2025 period shows trends of federated learning, edge computing, and post-quantum cryptography at the forefront as an evolution toward the intelligent, privacy-preserving, and scalable blockchain-IoMT ecosystems

Table 1: Summary of trends, their benefits and challenges

Trend	Benefits	Challenges	Citation
Lightweight sharding	Faster Bootstrapping, Reduced Storage and scalability Improvement, fault isolation and resilience.	Possible fragmentation, increased system complexity, Security Concerns with Node Assignment, Overhead in Maintaining Dual Chains	Liao et al. (2025)
Federated Learning and Block chain	Secure, privacy-preserving intelligence, Resistance to Poisoning Attacks, Improved Model Accuracy Under Privacy.	Synchronization and deployment challenges, Communication Overhead, Sensitivity to Noise in Privacy Mechanisms, Delay in Crowdsourcing.	(Zhao et al., 2020).
Off-chain and IPFS	Decentralization and Redundancy, Efficient Blockchain Integration Secure, privacy-preserving intelligence	Synchronization and deployment challenges	(Eren et al., 2025)
Post-quantum cryptography	Future-proof security, Complement to Homomorphic & Attribute-Based Encryption	Large Key and Ciphertext Sizes, Computational cost on devices	(Padmavathy et al., 2022)
Consortium blockchains	Support for Decentralized Applications, Control, efficiency, institutional trust	Consensus scalability limitations (e.g., BFT bottlenecks), integration: Hard to integrate with legacy systems or other platforms	(Chen et al., 2024)

(Sindhusaranya et al., 2023). The timeline showing key evolutionary trends in Blockchain-IoMT applications (2017–2025) as shown in figure 1.

Lightweight & Scalable Architectures

Lightweight architecture creates growing trends in more recent years suitable for IoMT's constrained environment. Liao et al. (2025) and Guoqiong et al. (2025) explore Lightweight Sharding method of Blockchain based on State Pruning (LSBSP) to find dual-chain architecture and snapshot pruning to minimize synchronization delay and storage requirements for end devices. Likewise, lightweight three-factor authentication and authorization protocol called L2AI designs its protocol and three-factor authentication scheme for low-power medical devices (Khajehzadeh et al., 2024). These trends show a movement away from general-purpose blockchain models toward customized, resource-efficient ones.

Blockchain + Federated Learning

Another budding trend is the coexistence of federated learning (FL) and blockchain. Such integration supports decentralized model training without exposure to raw medical data, thus conforming to privacy regulations. The federated blockchain framework supports co-intelligence among medical institutions, while issues of trust and accountability are resolved upfront (Zhao et al., 2020). This trend points towards an increasing emphasis on AI and distributed learning systems for privacy-preserving analytics.

Off Chain Storage and Big Data Integration

Handling large volumes of health data demands an efficient off-chain storage solution (Eren et al., 2025). One hot trend connects the blockchain with IPFS and BigchainDB where only the metadata is stored on-chain, while huge content such as imaging data is stored off-chain (Saif et al., 2024). This supports scalability, traceability, and integrity. Hence there is a shift of application from monolithic blockchain use to distributed hybrid data systems.

Privacy, Access Control, and Post-Quantum Cryptography

To provide a high level of privacy and patient identity protection in blockchain-IoMT systems, there are increasing research interests toward post-quantum cryptographic schemes and zero-knowledge proofs (Padmavathy et al. 2022). These address the future threats of quantum attacks and provide near-perfect mechanisms for access control. Regarding trends in access control systems, a natural evolution has been observed from static, rule-based approaches to dynamic, cryptography-based frameworks that take patient's consent and data sovereignty into consideration.

Consortium and Permissioned Blockchains

Chen et al. (2024) pointed that contrary to public blockchains, permission and consortium networks are forging ahead in the healthcare sector for control, privacy, and efficiency. Institutions may experiment with blockchain consortiums among themselves for the exchange and auditing of health data while maintaining institutional autonomy. This trend indicates the drifting away from public ledger solutions toward special-purpose, role-based governance structures that may satisfy regulatory requirements (Table 1).

Ongoing Challenges Amid Emerging Trends

Even if the gap in architectural and application-level trends looks very promising, there are several obstacles and great challenges:

a. Scalability vs. Security: Lightweight protocols may sacrifice security for better scalability.

b. Energy Consumption: Current consensus protocols such as PoW (Proof of Work) are still not applicable for IoMT-grade deployment.

c. No standardization: Different protocols and lack of standardization by vendors and in some regions blocks trend convergence.

d. Compliance confusion: With standards changing, compliance with things like HIPAA (Health Insurance Portability and Accountability Act) or GDPR (General Data Protection Regulation) can still be difficult.

e. Hardware Limitations: Most of the IoMT devices continue to suffer from limited computational resources to be able to perform complex functions of cryptographic operation.

Trend-Inspired Research Frontiers

a. Edge Powered Blockchain Architectures: Distributed processing for low latencies and less dependence on central cloud infrastructure.

b. ZKP (Zero-Knowledge Proofs): Allowing to prove one is an eligible patient/health provider without leaking one's identity.

c. Federated Blockchains Framework: for cross-infrastructure data sharing, with layers of partial decentralization.

d. Quantum-Invulnerable Algorithms: Securing blockchain against next-generation threats with post-quantum cryptography.

e. Ecofriendly Consensus Mechanisms: Low-power options, including Proof-of-Authority (PoA) for green installations.

f. Smart Contracts Legality Automation through Policy as Code and Patient Consent Logic.

Conclusion

The various trends that come along with the integration of the Internet of Medical Things (IoMT) with blockchain indicate that the field is finally entering a maturing phase. This transition from early experiments to strong, safe, and sustainable applications has led the healthcare ecosystem in the past few years towards intelligent, energy-aware, and patient centric solutions. Notwithstanding challenges around standards, compliance, and resources, emerging trends suggest exciting directions in research and deployment. Therefore, the combination of blockchain and IoMT is transforming the present and future of healthcare by providing a more secure environment where security and privacy of medical data are top priority.

REFERENCES

Abbasi, F and Singh, P. (2021). Cryptography: Security and Integrity of Data Management. *Journal of Management and Service Science,1(2), 4, pp. 1-9*. https://doi.org/10.54060/JMSS/001.02.004

Ali, A, S, M., Ali, S., Ziaullah, K., Joo, M., & Kim, H-C. (2025). IoMT and Blockchain Synergy: A Novel Approach to Health Data Validation and Storage. *IEEEAccess*, http://doi.org/10.1109/ACCESS.2025.3555289

Chen, X., He, S., Sun, L., Zheng, Y., & Wu, C.Q. (2024). A Survey of Consortium Blockchain and Its Applications. *Cryptography* 2024, 8, 12. https://doi.org/10.3390/cryptography8020012

Dhasaratha, C., Hasan, M, K., Islam, S., Khapre, S., Abdullah, S., Ghazal, T, M., Alzahrani, A, I., Alalwan, N., Nguyen., & Akhtaruzzaman, MD. (2024). Data privacy model using blockchain reinforcement approach for scalable internet of medical things, 2024CAAI Transactions on Intelligence Technology, https://doi.org/10.1049/cit2. 12287

El Haddouti, S & Kettani, D. (2024). Unveiling Blockchain Security and Resilience in the Quantum Age: An Analytical Study of Post-Quantum and Quantum Approaches. *ResearchGate, https://doi.org/10.1109/CommNet63022.2024.107933* 63

Eren, H., Karaduman, Ö., & Gençoˇglu, M.T. (2025). Security Challenges and Performance Trade-Offs in On-Chain and Off-Chain Blockchain Storage: A Comprehensive Review. *Appl. Sci*. 2025, 15, 3225. https://doi.org/10.3390/app15063225

Ghadi, Y, Y., Mazhar, T., Shahzad, T., Khan M, A., Abd-Alrazaq, A., Ahmed, A., & Hamam, H. (2024). The Role of Blockchain to Secure Internet of Medical Things. *Scientific reports*. https://doi.org/10.1038/s41598-024-68529-x

Gladyr, A. (2021). Design and development of a secure and patient-controlled systemto share healthcare data for research A thesis submitted to McGill University in partial fulfillment of the requirements of the degree Master of Computer Science. November, 2021. School of Computer ScienceMcGill University,Montreal

Guoqiong, L., Yinxiang. L., Yufang, X., Xiong, & Neal N. (2025). A Lightweight Sharding Method of Blockchain Based on State Pruning for Efficient Data Sharing in IoMT (2025). Computers, Materials & Continua, 2025, Vol 82, Issue 2, p3309, https://doi.org/10.32604/cmc.2024.060077.

Hewa, T, M., Hu, Y., Liyanage, M., Kanhare, S., & Ylianttila, M. (2021). Survey on Blockchain based Smart Contracts: Technical Aspects and Future Research. *IEEEAccess,* https://doi.org/10.1109/ACCESS.2021.3068178

Islam, S, Md., Bin Ameedeen, M, A., Ajra, H., & Ismail, Z, B. (2023). Blockchain-enabled Secure Privacy-preserving System for Public Health-center Data. *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 14, No. 5, 2023, https://doi.org/10.14569/IJACSA.2023.01405118

Khajehzadeh, L., Barati, H., & Barati, A (2024). L2AI: lightweight three-factor authentication and authorization in IOMT blockchain-based environment https://doi.org/10.48550/arXiv.2407. 12187

Khan, A,A., Wagan, A,A., Laghari, A,A., Gilal, A,R., Aziz, I,A., Talpur, B,A. (2022). Biomt: A State Of-The-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts. *IEEEAcess* , Vol 10, 2022, Digital Object Identifier 10.1109/ACCESS.2022.3194195.

Li, L., Jin, D., Zhang, T., & Li, N. (2023). A Secure, Reliable and Low-Cost Distributed Storage Scheme Based on Blockchain and IPFS for Firefighting IoT Data. *IEEEAccess*, https://doi.org/10.1109/ACCESS.2023.3311712.

Lipton A., Hardjono T., Pentland A. (2018). Digital trade coin: towards a more stable digital currency. R. Soc. open sci.5: 180155. http://dx.doi.org/10.1098/rsos.180155.

Liu, X., Barenji, A,V., Zhi Li,Z., Montreuil, B., Huang, G,Q. (2021). Blockchain-based smart tracking and tracing platform for drug supply chain. Computers & Industrial Engineering 161 (2021) 107669. https://doi.org/10.1016/j.cie.2021.107669

Mishra, P & Singh, G. (2023). Internet of Medical Things Healthcare for Sustainable Smart Cities: *Current Status and Future Applied Science, MDPI*, Appl. Sci. 2023, 13, 8869. https://doi.org/10.3390/app13158869. https://www.mdpi.com/journal/applsci

Ok, E., Barnty, B., & Joseph, O. (2025). Energy-Efficient Consensus Mechanisms, Research Gate, https://www.researchgate.net/publication/389175281

Padmavathy, R. (2022). Leveraging Blockchain for Confidentiality in Cloud-Hosted Smart Health Platforms., Indo-Am. J. of Life Sc & Bt.2022, Vol.19, Issue 4, 2022, https://www.researchgate.net/publication/392621209

Puri, V., Kataria, A., & Sharma, V. (2024). Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0. *Trans Emerging Tel Tech*.2024;35(4): e4245. https://doi.org/10.1002/ett.4245

Rahman, M. A., Hasan, M., Rahman, M. M., & Momotaj, M. (2024). A Framework for Patient-Centric Consent Management Using Blockchain Smart Contracts in Predictive Analysis for Healthcare Industry. International Journal of Health Systems and Medical Sciences 2024, 3(3), 45-59, http://inter-publishing.com/index.php/IJHSMS

Saif, M. B, Migliorini, S., & Spoto, F. (2024). Efficient and Secure Distributed Data Storage and Retrieval Using Interplanetary File System and Blockchain. *Future Internet*, 16, 98. https://doi.org/10.3390/fi16030098

Shafiq, M., Choi, J.-G., Cheikhrouhou, O., & Hamam, H. (2023). Advances in IoMT for Healthcare Systems. *Sensors*, 24, 10. https://doi.org/10.3390/s24010010

Sharma, A., Sarishma,Tomar, R., Chilamkurti, N., Kim, B. (2020). Blockchain Based Smart Contracts for Internet of Medical Things in e-Healthcare. *Electronics* 2020, 9, 1609; doi:10.3390/electronics9101609.

Sindhusaranya, B., Yamini, R., Manimekalai, M, A, P., & Geetha, K. (2023). Federated Learning and Blockchain-Enabled Privacy Preserving Healthcare 5.0 System: A Comprehensive Approach to Fraud Prevention and Security in IoMT. *Journal of Internet Services and Information Security (JISIS)*, volume: 13, number: 4 (November), pp. 199-209. https://doi.org/10.58346/JISIS.2023.I4.014

Sunny, J., Undralla,N., Pillai,V,M. (2020). Supply Chain Transparency through Blockchain-Based Traceability: An Overview with Demonstration *Computers & Industrial Engineering* https://doi.org/10.1016/j.cie.2020.106895

Suraci, C., De Angelis, V., Lofaro, G., Giudice, M,L., Marrara, G., Rinaldi, F., Russo, A.,Bevacqua, M.T., Lax, G., Mammone, N., Laboccetta,A,M., Morabito, F,C. (2022). The Next Generation Of Ehealth: A Multidisciplinary Survey. *IEEEAcess*, Vol10 2022. Digital Object Identifier 10.1109/ACCESS.2022.3231446

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview. National Institute of Standards and Technology Internal Report 8202, NISTIR, https://doi.org/10.6028/NIST.IR.8202

Zhao, Y., Zhao, J., Jiang, L., Tan, R., Niyato, D., Li, Z., Lyu, L., & Liu, Y. (2020). Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices. IEEE Internet of Things Journal (IoT-J), https://doi.org/10.1109/JIOT.2020.3017377.