International Journal of Leading Research Publication (IJLRP)
E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

# Decentralized Data Governance: Opportunities and Threats of BlockChain for Privacy and Security

**Srinivasa Kalyan Vangibhurathachhi**

Srinivasa.Kalyan2627@gmail.com

**Abstract:**
**The unprecedented growth of Internet of Things (IoT) has introduced complex challenges in data governance such as privacy, security and scalability. While traditional centralized governance models present vulnerabilities such as single points of failure, limited transparency and poor scalability, decentralised blockchain technology seeks to address these challenges. This paper examines the opportunities and threats of blockchain-enabled decentralized governance of data with specific focus on privacy and security. By analysing blockchain's features such as immutability, distributed consensus, and cryptographic verification, the research determined that significant opportunities including data security, secure digital identity systems, data sharing and auditable transparency. The findings also indicated that mining attacks, smart contract vulnerabilities, network threats are the key threats to blockchain-enabled governance of data. Case studies and technological reviews expose limitations in real-time processing and interoperability. Future researchers and industry professionals should focus on security, scalability, regulatory compliance, governance and sustainability.**

**Keywords: blockchain technology, privacy, security, immutability, opportunities, threats.**

## 1. INTRODUCTION

The internet of things (IoT) has witnessed unprecedented growth in recent years with billions of interconnected devices facilitating seamless collection, processing and sharing of data to enable smarter and more effective systems (Belfqih & Abdellaoui, 2025). However, these interconnectivity of devices have introduced numerous security challenges especially in the areas of authentication, confidentiality and data integrity. Gabriel et al. (2019) observed that the highly resource-constrained and distributed nature of IoTs environment contributes to their susceptibility to cyber threats like impersonation attacks, data breaches and denial of service attacks.

Traditionally,) data governance models have been centralized and often controlled by a few major intermediaries such as social media giants and cloud providers (Garcia, 2023). However, reliance on central authority introduces a number of vulnerabilities such as single points of failure, lack of transparency and potential misuse of personal data. Centralized data governance models also suffer from limited scalability, and latency which makes them inadequate for real-time and large scale IoT deployments (Belfqih & Abdellaoui, 2025). As the IoT ecosystems grow, these risks become increasingly important, thus calling for innovative and decentralised approaches.

Originally designed for cryptocurrencies, blockchain has emerged as a powerful and innovative solution for addressing security concerns associated with usage of IoT. Kaul (2024) reports that blockchain's decentralised architecture helps in eliminating single points of failure, with its inherent properties such as immutability, transparency and distributed consensus offering enhanced resilience and security. While blockchain technology has enormous potential in data governance, Gugueoth et al. (2023) argued that the IoT tend to be

constrained by limited energy, computational power, and bandwidth which makes application of blockchain solutions more complex. Lao et al. (2020) adds that real-time data sharing, secure key management and efficient data storage remain key challenges in realising effective and scalable blockchain based IoT solutions. To this end, this research paper examines the opportunities and threats of blockchain-enabled decentralized governance of data with specific focus on privacy and security.

## 2.0 BLOCK-CHAIN BASED SYSTEMS AS SOLUTION

By definition, blockchain is a series of blocks that are linked together in sequential chains to securely record transactions or data entry without needing central authority (Kabra et al., 2020). Unlike traditional and centralised database models, blockchain utilises a peer to peer network where every participant maintains a ledger copy and data is stored across multiple nodes. Mittal (2021) argues that this decentralisation ensures that no single entity has control over the entire database thus reducing the risk of unauthorised access and data breaches. In blockchain, each data entry or transaction is recorded in a block and linked to the previous block, forming a chain.

As shown in figure 1 below, each block in blockchain consists of several components like block header, block body, nonce and genesis block (Belfqih & Abdellaoui, 2025). The block header contains metadata that includes timestamp, hash of previous block, Merkle root of transactions and proof-of-work systems which ensures that each block is identified uniquely and linked to previous one. The block body stores a list of validated transactions/entries in a structured merkle tree which allows for efficient verification of integrity and consistency of every transaction/entry (Mittal, 2021). The nonce on its part is a random number used in mining which ensures that each block created is resistant to attacks. Importantly, the genesis block serves as the foundational block upon which subsequent blocks are created and ensures data integrity based on its initial hash (Belfqih & Abdellaoui, 2025). Together, these components form an immutable chain meaning that data cannot be altered or deleted once recorded. This feature plays a critical role in maintaining data integrity as it prevents unauthorised modifications and tampering thus providing transparent and reliable data management system (Belfqih & Abdellaoui, 2025).

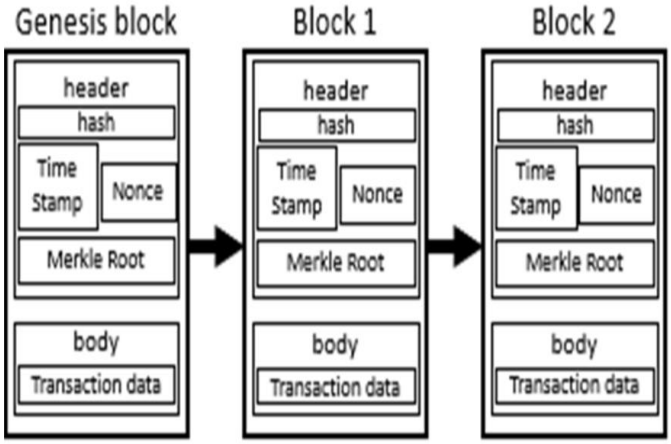


Figure 1: Blockchain structure (Belfqih & Abdellaoui, 2025)

In the blockchain technology architecture, the progressive relationship between application and technology is defined by five core layers as shown in figure 2 (Yu, 2024). The service layer is tasked with practical applications of blockchain technology in fields like supply chain, financial services, public services, copyright protection among others (Yu, 2024). The consensus and contract layers focus on incentivizing network clients and executing contract terms by setting rules that promote application of blockchain. While the network layer distributes information that can be transmitted quickly and securely in decentralized network, the data layer

encapsulates data into blocks by connecting them through complex computational processes and encryption methods to form immutable blockchain structure (Yu, 2024).

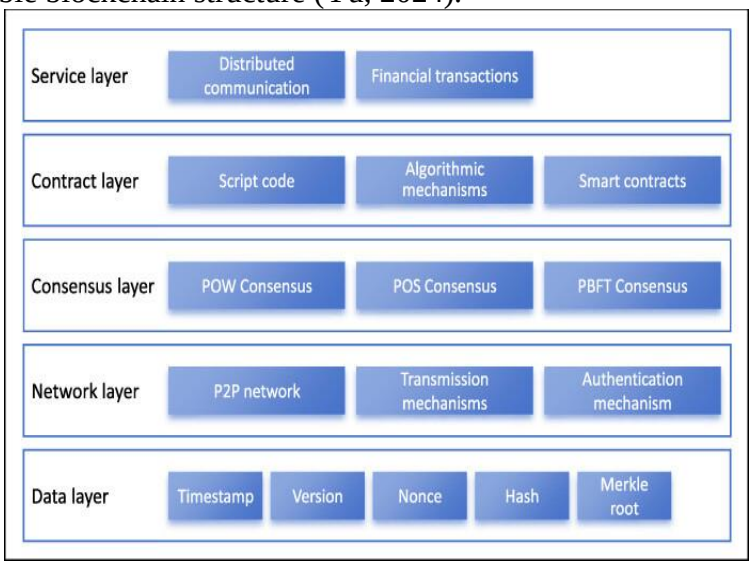


Figure 2: Blockchain technology architecture (Yu, 2024)

## 3.0 How Blockchain's Fundamental Properties Contribute To Data Governance

According to Kaul (2024), the decentralised architecture of blockchain plays a critical role in data governance within the IoT environment. Unlike traditional data management systems which rely on central servers and create vulnerabilities, blockchain's decentralised network architecture stores data in distributed multiple nodes. This distribution ensures that even if several nodes are compromised, the availability and integrity of overall data remains intact (Kaul, 2024). Most blockchain based solutions provide a stack where data resilience is built into the system thus offering robust defence from system failures and attacks. Apart from the decentralised architecture, immutability of records is a key defining feature of blockchain technology. Immutability implies that once a transaction/data entry has been made, it cannot be altered or deleted (Kumar & Sahil, 2025). Through complex cryptographic hash functions, data entries are secured in the blockchain ledger to achieve immutability.

Unprecedented transparency is another key feature of blockchain technology that helps in data governance. Kumar and Sahil (2025) highlights that every transaction and its associated data in blockchain are visible to all participants and can be verified independently thus fostering high level of trust among participants. Such transparency is important for applications that requires rigorous audit trails and for users who demand clarity over managing their data. Hazra et al. (2022) adds that blockchain technology reduces the need for intermediaries or trusted third parties in data transactions. Through smart contracts and self-executing contractual states stored on the blockchain, transactions can be automated without the help of third parties which reduces costs, speeds up processes and limits potential bias or error in data management. More important, blockchain empowers users with control over their data as they can decide who can access their data and under what conditions (Hazra et al., 2022). This empowerment aligns with the increasing global demand for user sovereignty and data privacy which allows individuals and organisations to manage their digital data safely and confidently. Figure 3 highlights key properties of blockchain technology that are crucial for data governance.

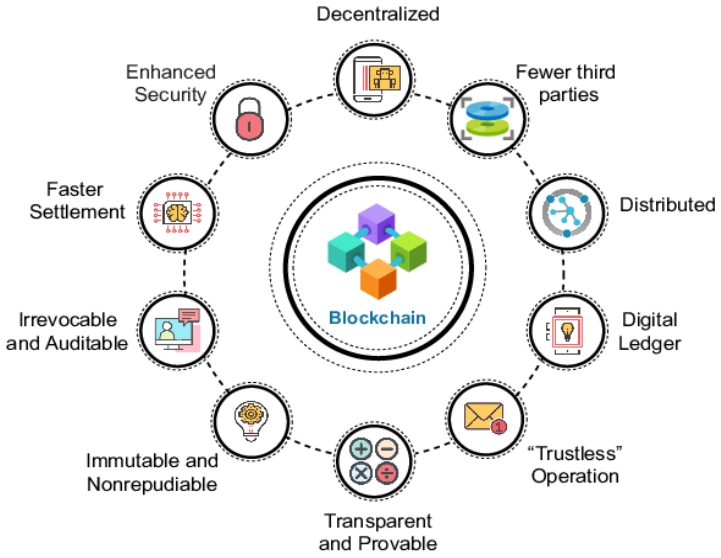


Figure 3: key features of blockchain technology (Hazra et al., 2022)

## 4.0 OPPORTUNITIES BROUGHT BY BLOCKCHAIN-BASED DECENTRALISED DATA GOVERNANCE

A number of existing studies have documented unprecedented opportunities brought by blockchain-based decentralised governance of data. For instance, Saleh (2024) noted that data privacy is a growing concern in the IoT environments and blockchain technology presents robust opportunities of protecting sensitive information. Blockchain's cryptographic features ensures that data is encrypted securely and accessed only by authorised users (Saleh, 2024). Specifically, public and private key cryptography allows individuals to control access to their data and enhance privacy/security. Due to blockchains' decentralised nature, the risk of data breaches is reduced due to no single point of failure (McCarthy, 2024). This makes blockchain a suitable solution for managing sensitive personal data like financial information, personal health records and critical business data. In the judicial system, Yu (2024) noted that blockchain technology helps in storage of elctornic evidence which ensures immutability and authenticity of evidence. Thus accelerates case handling process and improves fairness as well as efficiency of judicial rulings.

Apart from data security, block chain technology offers digital identity platforms which follows either self-sovereign identity platforms or decentralised trusted identity platforms (Guggenmos et al., 2018). In self-sovereign identity platforms, users can create and control their decentral digital identity using private keys. Sovrin exemplifies an organisation that has created self-sovereign identity ecosystem. On the other hand, decentralised trusted identity platforms tend to rely on single trusted service providers when issuing digital identities (Dunphy & Petitcolas, 2018). The service providers identify users based on existing trusted credentials such as passports or National IDs and records the identities on blockchain for validation by third parties. This is the case with unified and secure digital identity which allows personal information to flow between various government departments without the need for repeated verification. In China, Yu (2024) reported that the government have begun using blockchain technology to issue digital identity cards and electronic business license to ensure privacy protection of identities and reduce the risk of fraud and forgery. Additionally, blockchain technology facilitates secure data sharing by offering decentralised platform for sharing data among authorised participants without the risk of unauthorised access or tampering (Dubovitskaya et al., 2020). In the blockchain network, each participant has a copy of entire blockchain which ensures secure and transparent data sharing. Through blockchain's consensus mechanisms, data transactions are validated and recorded thus providing reliable data record before sharing. In healthcare, blockchain's consensus mechanism ensures secure and transparent sharing of patient's data among healthcare providers (McCarthy, 2024). Across government departments and levels, blockchain data sharing ensures seamless

exchange of information (Yu, 2024). Smart contracts for example can automatically execute sharing rules, improve efficiency of data processing and reduce human errors.

Ma et al. (2024) proposed a blockchain-based strategy for secure data sharing which reduces the burden on storage resources and augments the security of data-sharing process. As seen in figure 4 below, the data owner, authorization center, data demander, IPFS storage system and blockchain platform play crucial role in data sharing.

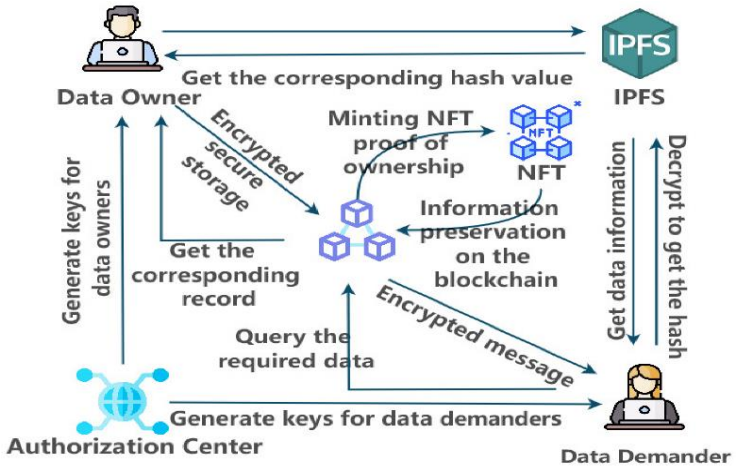


Figure 4: data sharing system architecture (Ma et al., 2024)

More important, blockchain technology presents opportunities through enhancing transparency in data management among stakeholders. As noted by McCarthy (2024), blockchain technology offers traceable and transparent system where all transactions are visible to authorised participants. This level of transparency ensures that all data are verified and audited thus reducing the likelihood of corruption and fraud. In supply chain, Agarwal et al. (2022) observed that high transparency levels allow participants to verify authenticity of products and track their movements. In financial transactions, Wati and Yazid (2023) noted that transparency allows stakeholders to verify integrity of financial records thus enhancing accountability and trust. For governments, the transparency of blockchain allows for verifiable records and establishes trust between the public and the government (Yu, 2024). Specifically, blockchain technology enhances transparency and accuracy of social security systems by ensuring transparent allocation of resources.

Figure 5 summarises key benefits brought by blockchain-enabled data governance for privacy and security.

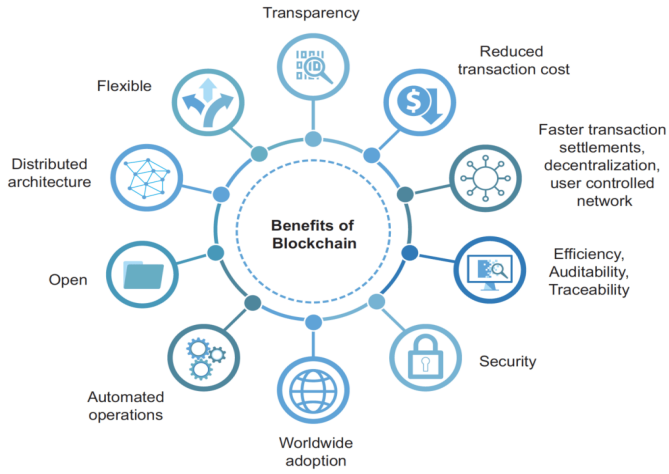


Figure 5: opportunities brought by blockchain technology (Cloud credential council, 2025)

## 5.0 THREATS AND CHALLENGES TO BLOCKCHAIN-BASED DECENTRALISED DATA GOVERNANCE

Existing studies have discussed threats and challenges associated with blockchain-based decentralised data governance with regard to security and privacy. Puthal et al. (2021) pointed out that mining, smart contracts and networking are three critical steps in the blockchain system where potential privacy and security threats can occur as indicated in figure 6 below.

### a) Mining threats

Mining threats to data security and user privacy in a blockchain is brought by several attackers who have more than 50% of the mining hash rate in the network. According to Hazra et al. (2022), attackers with control of the network may stop recording of new blocks by limiting other miners from completing the blocks. It is important to note that the blockchain has distributed consensus mechanism that ensures mutual trust as a key feature. Some of the mining threats that present security and privacy issues are selfish mining, block-withholding attack and >50% attack. In selfish mining, the attacker is viewed as reputable miner but fails to share results with the network users whereas a block withholding attack occurs when the attacker identifies genuine blocks but fails to submit them (Hazra et al., 2022). In >50% attack, the blockchain is controlled by trustworthy nodes but is executed when an attacker has control of more than half of network users.

### b) Smart contract threats

According to Hazra et al. (2022), lack of smart contract guidelines places significant responsibilities on firms which exposes contract data to risk. Most cyberattacks and technical failures tend to target smart contracts as their execution do not need physical presence thus increasing the risk of forgery or fraud. Ethereum is the most innovative and successful blockchain contract (Hazra et al., 2022). Smart contracts threats can take the form of source code or blockchain vulnerabilities. Dika and Nowostawski (2018) highlights that source code vulnerabilities imply a weakness in the programming that puts users' data at risk of hacking. Hackers can retrieve users' data from by linking an outlet to the code which interferes with system to eradicate data. However, blockchain vulnerabilities arises when user transactions are initiated in preconfigured contracts but they fail to execute in identical configuration when different transaction invoke corresponding smart contracts in parallel (Dika & Nowostawski, 2018).

### c) Network threats

Network threats arise when threats are aimed at disrupting organisational operations rather than collecting information for espionage or financial gain. Aggarwal and Kumar (2021) noted that distributed denial of service attack (DDoS), Sybil attack and delay attack are the most common network threats to data privacy and security in blockchain. Shah et al. (2022) noted that DDoS assault involves interrupting a server or network by flooding with internet traffic and may include DNS amplification, SYN flooding and UDP flooding. Whereas network DDoS assault interferes with physical blocks, DDoS attack application can damage a server and demolish all its sources. In regards to Sybil attack, it involves creating unique peer to peer networks that undermine reputation system (Aggarwal & Kumar, 2021). Accordingly, hostile actors and bots may manipulate social navigation systems through simulation of GPS information. For the delay attack, the attackers may disrupt block transfers among network partners by seizing the blocks in their paths, holding them for 20-30 minutes and sending them to users (Aggarwal & Kumar, 2021). Due to this, users expend resources to acquire current data from the block.

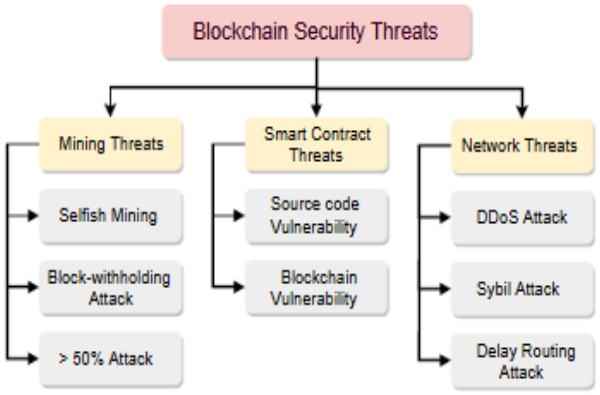


Figure 6: Blockchain security threats (Hazra et al., 2022)

## 6.0 FUTURE RESEARCH DIRECTIONS

As blockchain technology matures, researchers and industry professionals focus on security, scalability, regulatory compliance, governance, and sustainability.

- **Security:**

While blockchain offers immutability and transparency, these features tend to clash with privacy. Even when pseudonymized, on chain data can be de-anonymized using analytics and graph-based inference attacks. Teng et al. (2025) argues that future work should focus on Zero-Knowledge Proofs (ZKPs) systems where users can prove access rights or credentials without revealing identity or underlying data. Current research in ZK-SNARKs and Bulletproofs needs optimization for general-purpose applications (Teng et al., 2025). Additionally, future researchers should explore Private Information Retrieval (PIR) and Secure Multiparty Computation (SMPC) systems which can support decentralized queries and computations without leaking data location or content (Sahil et al., 2025).

- **Data governance;**

As blockchain ecosystems diversify, data governance may not be confined to a single chain. For instance, health records may span Ethereum-based systems and Hyperledger Fabric in a multi-stakeholder environment (Oke et al., 2025). Future researchers should explore interoperable data governance protocols which sets standards for consent, provenance and revocation across chains. Projects like Polkadot and Cosmos offer groundwork, but governance semantics vary drastically (Cheng, 2025).

- **Scalability;**

As data grows, storing all relevant metadata and audit trails on-chain becomes inefficient and expensive. Cheng (2025) noted that current layer-2 technologies like ZK-Rollups and Optimistic have greatly enhanced blockchain transaction speed. However, coming developments are focussing on recursive rollups where multiple rollups are aggregated into one proof to decrease expenses related to verification expenses (Cheng, 2025). Additionally, research on blockchain scalability focuses on the interoperability where protocols such as Polkadot, Cosmos and Chainlink CCIP facilitates communication between various blockchains. For example, Polkadot's parachain architecture are increasingly making it possible for blockchains to be independent but share security (Liu et al., 2025).

## 7.0 CONCLUSION

As an emerging technology, blockchain offers transformative pathway for decentralized data governance in addressing key issues in IoT such as data breaches, lack of user control and systemic inefficiencies. Its decentralization, immutability and transparency provide critical support for privacy preservation and secure data sharing. The research findings demonstrate how blockchain-based architectures can mitigate risks of central authority, enhance auditability, transparency and empower user sovereignty. However, the research reveals critically persistent challenges including energy-intensive mining, smart contract vulnerabilities, regulatory uncertainties and scalability constraints. Privacy concerns in healthcare and other sensitive sectors

underscore the need for cryptographic innovation and societal acceptance. Future research should look at zero-knowledge proof systems, cross-chain governance protocols, human-centric usability models and scalable blockchain architectures. Bridging technical, legal, and social domains could be essential for realizing the full potential of blockchain in creating a secure, privacy-preserving, and decentralized data governance future.

**REFERENCES:**

1. A.C.P. Wati & M. Yazid, "Blockchain Technology in Financial Transactions under Sharia Banking Practice," *EkBis: Jurnal Ekonomi dan Bisnis, 7*(2), pp. 81-91, 2023.
2. Dika & M. Nowostawski, "Security Vulnerabilities in Ethereum Smart Contracts," *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 955-962, 2018. doi: 10.1109/Cybermatics_2018.2018.00182.
3. Dubovitskaya, P. Novotny, Z. Xu, & F. Wang, "Applications of blockchain technology for data-sharing in oncology: Results from a systematic literature review," *Oncology*, vol. 98, no. 6, pp. 403-411, 2020.
4. Hazra, A. Alkhayyat, & M. Adhikari, "Blockchain-aided Integrated Edge Framework of Cybersecurity for Internet of Things, *IEEE Consumer Electronics Magazine*, vol. 99, pp. 1-1, Jan 2022. doi:10.1109/MCE.2022.3141068
5. A.M.S. Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review," *Blockchain: Research and applications,* vol. 5, no. 3, 2024. Doi: 10.1016/j.bcra.2024.100193
6. Cloud Credential Council, *"Knowledge Byte: The Real Benefits of Blockchain,"* https://www.cloudcredential.org/blog/who-participates-in-a-blockchain-network-and-what-are-its-benefits/ (Accessed: 29th June 2025)
7. D. Puthal, S. P. Mohanty, E. Kougianos, & G. Das, "When Do We Need the Blockchain?" IEEE Consumer Electronics Magazine, vol. 10, no. 2, pp. 53–56, 2021.
8. D. Teng, Y. Yao, & C. Huang, "Optimizing signature space performance in privacy-enhanced blockchains: novel ring signature solutions," *EURASIP Journal on Information Security*, vol. no. 1, 6, 2025.
9. F. F. Oke, S.A. Adeniji, O. Bolaji, O. Dopamu & B.S. Ajibade, "Blockchain-Enabled Consent Management in FHIR-Compliant Oncology Platforms," *Journal of Health technology*, 2025. Doi:10.36227/techrxiv.174918103.37396756/v1
10. F. Guggenmos, J. Lockl & A. Rieger, "Challenges and Opportunities of Blockchain-based Platformization of Digital Identities in the Public Sector," Conference: European Conference on Information Systems (ECIS2018) Workshop on Platformization in the Public Sector, 2018.
11. H. Belfqih and A. Abdellaoui, "Decentralized blockchain-based authentication and Interplanetary File System-based data management protocol for internet of things using Ascon," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, p. 16, Apr. 2025. doi:10.3390/jcp5020016
12. H. Mittal, "Blockchain Technology: Architecture, consensus protocol and applications," *Blockchain 3.0 for Sustainable Development*, vol. 10, no.1, pp. 1–8, Jul. 2021. doi:10.1515/9783110702507-001
13. J. Yu, "Exploration of the application of blockchain in e-government: Opportunities and risks coexist," *Information Services and Use*, 2024, 44(3), pp. 255-266. doi:10.3233/ISU-240013
14. Kaul, "Decentralized Data Management: Enhancing Data Security and user control," *Medium*, https://medium.com/liveplexmetaverseecosystem/decentralized-data-management-enhancing-data-security-and-user-control-f1d30127b38b (accessed June 28th, 2025).
15. K.Y. Cheng, "The legal structure of decentralised autonomous organisations (DAOs): governance, legal personality and liability. *Information & Communications Technology Law*, PP. 1-17, 2025.
16. K. Sahil, K. Kunadan & N. Yadav, "Decentralization Through Blockchain: Opportunities and Challenges, 2025. http://dx.doi.org/10.2139/ssrn.5166203

17. K. Kumar & Sahil, "Decentralization Through Blockchain: Opportunities and Challenges. https://ssrn.com/abstract=5166203 (accessed 29th June 2025)
18. H. Liu, T. Lu, Y. Yang, Y. Guo, Q. Wu, X. Xu & H. Zeng, "Blockchain-based optimization of operation and trading among multiple microgrids considering market fairness," *International Journal of Electrical Power & Energy Systems*,166, 110523, 2025.
19. L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo & Y. Yang, "A survey of IOT applications in Blockchain Systems," *ACM Computing Surveys*, vol. 53, no. 1, pp. 1–32, Feb. 2020. doi:10.1145/3372136
20. N. Kabra, P. Bhattacharya, S. Tanwar, and S. Tyagi, "Mudrachain: Blockchain-based framework for automated cheque clearance in financial institutions," *Future Generation Computer Systems*, vol. 102, pp. 574–587, Jan. 2020. doi: 10.1016/j.future.2019.08.035
21. P. Dunphy & F. A. P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain" arXiv preprint arXiv:1801.03294, 2018.
22. R. D. Garcia, *Blockchain-based data governance for privacy-preserving in multi-stakeholder settings*. doi: 10.11606/d.55.2023.tde-06092023-102200
23. R. McCarthy, "Blockchain for Secure Data Management: Ensuring Integrity and Transparency," *Developer Nation*, https://www.developernation.net/blog/blockchain-for-secure-data-management-ensuring-integrity-and-transparency/ accessed 29th June 2025)
24. S. Aggarwal, & N. Kumar, "Attacks on blockchain," *Advances in computers*, Vol. 121, pp. 399-410, 2021
25. T. Gabriel, A. Cornel-Cristian, M. Arhip-Calin, and A. Zamfirescu, "Cloud storage. A comparison between centralized solutions versus decentralized cloud storage solutions using blockchain technology," *2019 54th International Universities Power Engineering Conference (UPEC)*, pp. 1–5, Sep. 2019. doi:10.1109/upec.2019.8893440
26. U. Agarwal, V. Rishiwal, S. Tanwar, R. Chaudhary, G. Sharma, P.N. Bokoro, & R. Sharma, "Blockchain Technology for Secure Supply Chain Management: A Comprehensive Review," in *IEEE Access*, vol. 10, pp. 85493-85517, 2022, doi: 10.1109/ACCESS.2022.3194319.
27. V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A review of IOT security and privacy using decentralized blockchain techniques," *Computer Science Review*, vol. 50, p. 100585, Nov. 2023. doi: 10.1016/j.cosrev.2023.100585
28. W. Ma, X. Wei & L. Wang, "A Security-Oriented Data-Sharing Scheme Based on Blockchain," *Applied Sciences*, vol.14, no. 16, 6940, 2024. Doi: https://doi.org/10.3390/app14166940
29. Z. Shah, I. Ullah, H. Li, A. Levula & K. Khurshid, "Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey," *Sensors*, vol. 22, no. 3, pp. 1094-1115, 2022. Doi: https://doi.org/10.3390/s22031094