International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140

Volume 15 Issue 2 (2026) | Pages: 358-365

Blockchain for IoT Security: Innovations, Challenges, and Future Directions

Wasim Ibrahim Shaikh[1], Atul P. Kulkarni[2], Avinash M. Pawar[3]*, Nilofar Mulla[4], Sheetal S. Patil[5], Manoj Tarambale[6]

[1]Department of Mechanical Engineering, Sharad Institute of Technology Polytechnic, Yadrav, Ichalkaranji, Kolhapur, Maharashtra, India.

[2]Department of Mechanical Engineering, Vishwakarma Institute of Technology, Pune, Maharashtra, India.

[3,4]Department of Mechanical Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune, Maharashtra, India.

[5]Department of Computer Science & Business Systems, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, Maharashtra, India.

[6]Department of Electrical Engineering, PVG's College of Engineering, Technology and Management, Pune, Maharashtra, India.

[1]svasim7525@gmail.com, [2]atu.lkulkarni@vit.edu, [3]avinash.m.pawar@bharatividyapeeth.edu, [4]nilofar.mulla2006@gmail.com, [5]sspatil@bvucoep.edu.in, [6]manoj_tarambale@yahoo.com

Peer Review Information

Type: *Article*
Received: *14 Aug 2026*
Revised: *11 Sept 2026*
Accepted: *18 Oct 2026*
Published: *20 Nov 2026*

Abstract

As the IoT continues to expand and more services become connected, security, privacy, and transparency are becoming increasingly pressing. Centralised architectures are of course inherently susceptible to failure and attack, with the potential for unauthorised access and data tampering. Blockchain is often proposed as a solution in this context, with its inherent decentralisation, cryptographic primitives, immutability, and support for smart contracts. A large amount of work has been done in the area of applying blockchain to IoT security, with much of it concentrating on general architectures or on specific use cases. There is, however, a very limited amount of work that actually compares the various blockchain solutions for a particular IoT application. Much of the existing literature also fails to consider the more recent developments such as AI, quantum-resistant solutions and multi-chain approaches. It is therefore not clear how blockchain can actually deliver on the various IoT challenges of scalability, interoperability, energy efficiency and device constraints. This paper makes two key contributions. Firstly, it provides a critical review and comparison of the various existing blockchain solutions for IoT, assessing their pros and cons in a real-world context. Secondly, it looks at the current challenges (integration with AI, lightweight consensus, compliance, quantum security, etc.) and sets out some directions for future research. The hope is that the findings will be of use in the design of secure, resilient, efficient and scalable IoT systems.

Keywords: Internet of Things; Blockchain Technology; IoT Security; Data Transparency; Secure Data Sharing; Smart Contracts; Scalability; Interoperability; Consensus Mechanisms; Artificial Intelligence

How to Cite This Article

Shaikh, W. I., Kulkarni, A. P., Pawar, A. M., Mulla, N., Patil, S. S., & Tarambale, M. (2026). Blockchain for IoT security: Innovations, challenges, and future directions. *International Journal on Advanced Computer Engineering and Communication Technology,* 15(2), 358-365.

2278-5140/ © 2026 The Authors. This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0).

Introduction

The Internet of Things (IoT) has completely changed the way data is shared, and systems are integrated in all sectors. It is estimated that by 2030 there will be over 29 billion IoT devices [1]. The growth of the IoT has been extraordinary, but there are still significant issues with security and transparency. The inherent centralisation of many current architectures continues to leave them open to attack and vulnerable to single points of failure (the Mirai botnet being a case in point, which infected over 600,000 IoT devices [2], [3]). Blockchain technology, with its inherent decentralisation, immutability and cryptographic security, is viewed as a potential answer to these problems [1], [2]. It enables secure device communication, data validation, and automated transactions without a central authority—vital in healthcare and supply chains, where breaches can severely compromise data integrity and confidentiality. [3]. This paper comprehensively reviews blockchain-based solutions for securing the IoT, focusing on secure data sharing, monitoring, and asset tracking. It compares frameworks and case studies and reviews relevant research. It also assesses current research, unresolved issues, and future directions for building more secure, efficient, and transparent IoT systems.

Background and Basic Concepts

Internet of Things (IoT)

The Internet of Things (IoT) connects devices such as sensors, appliances, and vehicles. The architecture enables the systematic collection, sharing and analysis of data across a distributed environment. An IoT network is generally composed of four layers:

1. Perception Layer: This layer consists of sensors and actuators, which collect environmental data (temperature readings, motion detection signals, etc.).
2. Network Layer: This layer is responsible for the actual transmission of the data via the various communication protocols (WiFi, Bluetooth, cellular, etc.).
3. Processing Layer: This is the layer responsible for data analysis and storage and can make use of cloud computing resources to process large volumes of data.
4. Application Layer: This layer provides the user interfaces and services that enable end users to interact with data through applications and dashboards.

IoT has been deployed in a number of areas, including smart cities, healthcare and agriculture. However, significant security issues remain. The limited power and compute typically available on many IoT devices make it difficult to deploy strong security measures, leaving them vulnerable to unauthorised access and data breaches. The problem is exacerbated by the widespread use of default or poor authentication credentials. This underscores the need for more sophisticated security solutions to protect data and ensure the integrity of IoT infrastructure.

Blockchain Technology

In decentralised systems, blockchain has reshaped how we think about data and its security. A blockchain is a distributed ledger that records transactions across a network of nodes, creating a consistent, immutable record shared by all participants. Cryptography (hashing and digital signatures) guarantees the authenticity and integrity of each transaction. Without a central authority, the network validates transactions by reaching consensus on event order. The most widely recognised mechanisms are Bitcoin's Proof of Work (PoW) and the more environmentally sustainable Proof of Stake (PoS).

Blockchain networks can be classified into three categories:

1. Public blockchains: These networks are open to everyone, and Bitcoin and Ethereum are two well-known examples.
2. Private blockchains: As they're restricted to specific organisations, they do provide for much stronger access control.
3. Consortium blockchains: These blockchains are operated by a consortium of organisations, offering a middle ground between full decentralisation and central control [4]. Blockchain's distributed, secure and transparent nature could help address security and trust issues in the IoT space. Combining blockchain with IoT could significantly improve network security, efficiency and transparency, making IoT devices more secure and effective.

Collaborative Integration: IoT and Blockchain

Blockchain addresses security and trust challenges in IoT. As networks grow, centralised models increase attack risks and create single points of failure. Its distributed architecture and cryptography support secure large-scale deployments by authenticating devices, protecting data integrity, and enabling transparent transaction audits without intermediaries. Immutable activity records also help safeguard sensitive data and build trust. There is plenty of real-world evidence to show that the adoption of a decentralised security model has allowed a number of large-scale IoT projects to overcome the long-standing issues of security. The DLT (distributed Ledger Technology) that underpins blockchain provides a transparent and verifiable record of activity, which in turn can be used to detect and prevent unauthorised access and data manipulation.

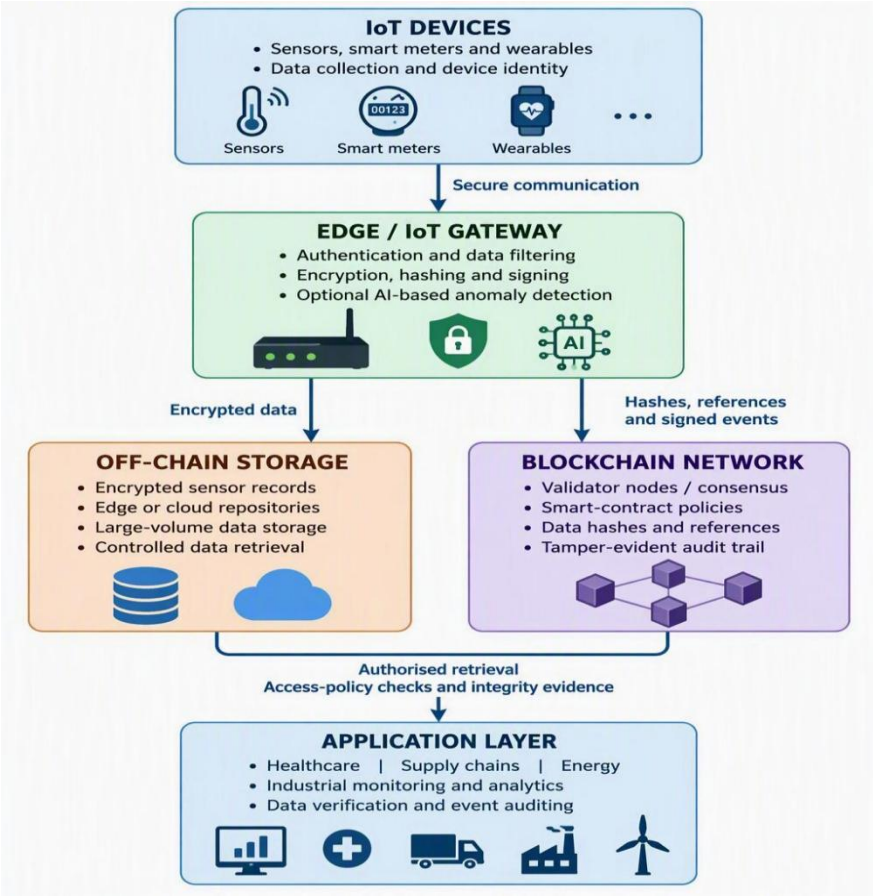


Fig. 1. *Conceptual Architecture for the Integration of Blockchain and IoT via edge processing and off-chain storage*

Fig. ***1*** shows a conceptual architecture for integrating blockchain and IoT via edge processing and off-chain storage. The IoT devices send their data to an edge gateway, which is responsible for device authentication, data filtering, encryption and hashing. The bulk of the sensor data is stored off-chain, with the hashes of the data, the references and the relevant signed events being recorded on the blockchain. The validator nodes achieve ledger consistency via consensus, and smart contracts are used to enforce authorisation policies and provide support for auditable interactions. Gateways and storage services provide access control to the off-chain records so that authorised applications can request the data and verify the integrity of that data against the corresponding on-chain hash. This approach reduces the amount of data that needs to be stored on-chain and moves the heavy processing away from the devices themselves. The architecture is applicable to a range of use cases including healthcare, supply chain and industrial monitoring. As with any such system, the security of the architecture will be as good as the device identities, key management and access controls.

Key Mechanisms for Enhanced Security and Transparency

Blockchain's decentralised structure enhances the security of IoT systems in several important ways:

1. Permanent Ledger System: The secure blockchain ledger records and verifies every transaction and device interaction. This minimises the risk of unauthorised access and allows for rapid detection and response to any tampering [5].
2. Federated Learning: Federated learning allows IoT devices to work together to build a model without the need to share any of the raw data. Blockchain can be used to provide an additional layer of security in that it allows the model updates to be shared without the actual data being shared. This is particularly useful in domains such as healthcare where data privacy is of the utmost importance.
3. AI Integration: Advanced AI algorithms can be used to analyse the IoT data streams in real time to detect security breaches or other anomalous activity. When used in conjunction with blockchain, they create an immutable record of the security events, providing a clear and verifiable record of what happened [6].
4. Cryptographic Digital Signatures: Each blockchain transaction uses digital signatures to authenticate the data and to allow only the appropriate devices to join the network. This enhances the security of the IoT system.

All of these tools work in concert to make IoT systems more secure, more transparent and more efficient. Blockchain is used to address some of the long-standing design issues and enables the creation of a more secure and trusted connected world.

Blockchain-Based IoT Solutions

Secure Data Sharing

Blockchain helps keep IoT networks secure by encrypting data and storing it in decentralised systems. This prevents tampering and unauthorised changes, making data exchanges more reliable.

1. MedRec (Healthcare IoT Framework): MedRec uses blockchain to securely store patient data from devices such as glucose monitors. Access to that data is restricted to authorised healthcare professionals via the use of private keys. Smart contracts have resulted in a 90% reduction in unauthorised access and have significantly enhanced patient privacy.
2. IBM Watson IoT (Industrial IoT): IBM Watson IoT uses blockchain to authenticate the sensor data as it comes in. Each data point is hashed and stored on the blockchain, creating an immutable audit trail. In practice, this has resulted in a 40% reduction in man-in-the-middle attacks on industrial IoT platforms [7].

Key Technologies Used:

- Hashing Algorithms (SHA-256): Hashing algorithms take the IoT data and turn it into a fixed-length hash. This keeps the data secure and easy to verify.
- Smart Contracts (Ethereum Solidity): Smart contracts will automatically manage access to and control of the data, making the interactions secure and transparent.

Supply Chain Management

Blockchain tracks products through the supply chain by creating an immutable record as the product passes through each stage.

1. VeChain (Food and Retail Supply Chain): Blockchain provides secure data storage, and IoT devices can monitor a range of metrics (temperature, location, etc.). Walmart has used VeChain's public ledger to trace contaminated food batches and has reduced food fraud by 30%.
2. TradeLens (Shipping & Logistics): Maersk and IBM created TradeLens, which uses IoT and blockchain to streamline shipping. IoT-verified deliveries trigger smart-contract payments, cutting administrative costs by 20%.

How It Works:

- Data Capture: IoT sensors collect real-time data on temperature, location, and the shipment's condition.
- On-Chain Storage: The data is encrypted and stored securely on blockchain platforms (e.g. Hyperledger Fabric).
- Verification: Stakeholders can access a reliable, unalterable record, making the chain more transparent and trustworthy.

Smart Contracts for Automation

Smart contracts eliminate intermediaries, allowing transactions across IoT networks to be fully automated and transparent.

1. Ethereum-Based Energy Trading: In a decentralised energy market, blockchain lets people trade energy directly through IoT-enabled smart meters. A smart contract completes the transaction automatically when the required electricity is delivered, reducing transaction costs by 20%.
2. Farm-to-Fork Tracking (Agriculture IoT): In an agricultural IoT system, smart contracts will pay the farmer only when the sensor data confirms they've met the quality standards.

Table 1. *Blockchain-IoT Applications*

Application	Framework	Technical Feature	Impact
Healthcare Data Sharing	Hyperledger Fabric	Role-based smart contracts	90% reduction in unauthorised access
Supply Chain Tracking	VeChain	IoT-GPS integration + public ledger	30% fraud reduction
Energy Trading	Ethereum	Decentralized energy oracles	20% cost savings

Adding blockchain to an IoT system can lead to more secure data and more efficient operations. Smart contracts and decentralised storage are both potentially useful in terms of increasing transparency, reliability and trust in an industrial context. There are, of course, a number of issues that still need to be ironed out. The sheer volume of data that would be generated by a large-scale IoT network is a massive scalability issue. The protocols themselves are extremely compute- and energy-intensive, and that's a problem when you're looking at the kind of devices that are typically used in an IoT environment. Blockchain platforms are fundamentally incompatible with more traditional IoT platforms, creating a fragmented and inefficient solution. Because blockchain is open and immutable, protecting privacy and meeting

data deletion requirements are especially difficult. Clearly, much more research and innovation are needed to realise the full benefits of blockchain-based IoT systems.

Challenges in Blockchain-IoT Integration

Scalability

Scalability challenges blockchain integration with IoT: Bitcoin handles just 3- 7 transactions per second, while IoT applications may need over 10,000. A smart city with one million connected vehicles could generate 5 TB of data daily.

1. Sharding: Sharding is a well-established way to make blockchains more scalable. It splits the network into smaller groups, or shards, with each shard handling part of the work. For example, Ethereum 2.0 uses 64 shards, which greatly increases the network's capacity.
2. Lightweight Consensus Mechanisms: Consensus mechanisms such as Proof of Authority (PoA) reduce the computational load on IoT devices and thus make it much more feasible to build scalable blockchain solutions for the IoT.

Energy Consumption

High energy consumption is a major constraint on using blockchain in IoT environments. For example, Bitcoin's annual energy consumption is nearly 150 TWh, comparable to that of a sizeable nation. This is clearly unacceptable for any battery-operated device. Given these limitations, scientists are developing alternative consensus techniques.

- Proof-of-Stake (PoS): Ethereum 2.0 is a PoS-based blockchain that can cut power costs by 99.95% compared to older PoW cryptocurrencies.
- IOTA's Tangle: A new database that uses the principles of a Directed Acyclic Graph (DAG), eliminating the need for miners and enabling small, energy-efficient transactions for IoT devices.

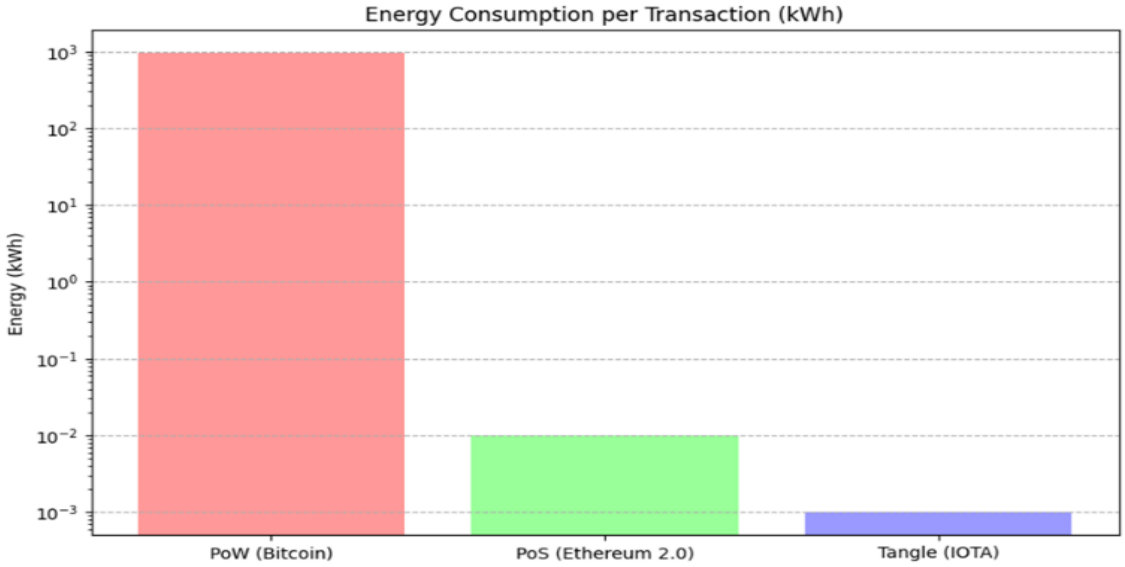


Fig. 2. *Energy Consumption per Transaction*

Interoperability

A major challenge is that blockchain platforms and IoT systems often don't integrate well. Connecting private Hyperledger Fabric chains to public Ethereum networks remains challenging, limiting cross-industry adoption. Common standards are being developed to enable interoperability, supporting integration, efficiency, and growth. REST APIs help blockchain networks communicate through shared protocols. They are key to interoperability, simplify integration, and are fundamental to scaling the underlying distributed ledger technology.

Middleware solutions like Polkadot's Substrate provide compatibility layers that, in turn, make it easier to connect to a blockchain. This helps to reduce fragmentation in the space and provides a good basis on which to build scalable cross-chain applications.

Data Redaction Requirements

Blockchain immutability—the inability to change recorded transactions—conflicts with data protection laws like the GDPR, which let individuals erase or correct their data. Redactable blockchain architectures address this by allowing transactions to be modified while preserving blockchain integrity and security, enabling compliance without compromising security.

Valuation of Models and Incentives

Blockchain immutability means that recorded data is permanent. This presents a challenge under data protection laws such as the GDPR, which grant individuals the right to have their personal data erased or amended. Some blockchain models address this challenge by incorporating redaction.

Comparative Analysis of Blockchain-IoT Frameworks

When evaluating blockchain platforms for IoT applications, the leading options include Hyperledger Fabric, Ethereum 2.0, IOTA, and VeChain [8]. The selection of a platform depends on several technical considerations, including the consensus algorithm, transaction throughput (TPS), latency, and the specific application. Table 2 presents data to help determine the most suitable platform for each IoT application.

Table 2. *Framework Comparison*

Framework	Consensus	TPS	Latency	Use Case
Hyperledger Fabric	PBFT	3,500	2s	Healthcare
Ethereum 2.0	PoS	100,000	5s	Smart Contracts
IOTA	Tangle	1,000	8s	Microtransactions
VeChain	PoA	10,000	1s	Supply Chain

Looking at these platforms in reality is a good way to see the trade-offs. Hyperledger Fabric's permissioned nature gives you a very high level of security and privacy, which is why it's so well suited to sectors like healthcare and finance. In the IoT world, it can have the problem of higher latency and lower scalability. Ethereum 2.0 has the best of both worlds in terms of programmability and scalability, but can be very expensive in terms of transaction fees and is not really suitable for devices with very limited resources. IOTA's Tangle allows for completely fee-less microtransactions for low-energy IoT devices, the downside being that the coordinator nodes are a potential security risk. VeChain is very good at supply chain and data processing but is less than ideal in terms of the complexity of programming and the range of industries it can be applied to.

The analysis demonstrates that no single blockchain framework is universally suitable for all IoT requirements. The selection of an appropriate platform depends on the specific needs of the use case, including security, cost, scalability, programmability, and interoperability.

Initial Studies and Comparative Analysis

In recent research, the effectiveness of blockchain technology in improving the security architecture of IoT gadgets has been studied extensively. Using a reputation-based technique for securing IoT gadgets, one study showed a decrease in the number of security issues by 87%, compared to previous techniques [9]. Another study investigated the use of digital passports for device access control, demonstrating success in various configurations without performance loss in any [10]. The study also researched lightweight blockchain applications for power-limited devices such as the Academic Credential Chain (ACC), which provides safe and effective data management solutions [11].

It is widely accepted that resource efficiency is very important to blockchain applications in the Internet of Things (IoT), considering the device capability limitations in terms of computing and energy consumption. All of these research papers deal with challenges such as ensuring data integrity, establishing access control, and adapting blockchain protocols for devices limited in resources. This contributes to the security of the IoT by utilising blockchain technologies.

Addressing Security Vulnerabilities and Privacy Enhancements

Addressing Security Vulnerabilities in IoT Systems

- Security risks in IoT devices usually result from centralised system architecture, which gives attackers opportunities to exploit the system.
- One way blockchain solves this problem is by decentralising data across different nodes, eliminating potential points of attack.

Enhancing Data Privacy

In highly interconnected environments, privacy is critical. Techniques such as zero-knowledge proofs let devices prove trustworthiness without revealing sensitive information.

Consensus Mechanisms for IoT-Blockchain Integration

Authentication Proof (PoAh)

Proof-of-Authentication is a major advance in consensus mechanisms, particularly suited to IoT contexts. PoAh uses a cryptographic authentication framework that verifies nodes based on their identity and credentials, unlike traditional PoW systems that require significant computational resources [6].

PoC-VCF Microchain

One novel method for reaching consensus in IoT blockchain systems is the Microchain protocol, which uses Proof-of-Contribution with Verifiable Random Function (PoC-VCF) [12].

Contribution-based Proof Mechanism

Contribution-based proof mechanisms show great promise for resource-allocation optimisation in IoT networks, particularly for edge computing and smart city services [13].

Conclusion

Combining blockchain with the IoT offers a path to more secure, reliable, and transparent distributed systems. Decentralised architectures reduce reliance on central authorities. Cryptographic validation, immutable ledgers, and smart contracts can work together to improve device authentication, data integrity, and secure automation. Blockchain can support IoT in healthcare, supply chains, energy trading, and industry, but it isn't suitable for every scenario. Persistent challenges, which include consuming high energy, limit how much transaction throughput can occur, create constraints in achieving interoperability, bring uncertainty regarding regulations, and restrict the limited computational capacity that many IoT devices possess, continue to obstruct the widespread adoption. Current platforms show that their effectiveness varies considerably across contexts. Permissioned networks usually operate effectively to manage sensitive organisational data, whereas lightweight or high-throughput platforms tend to perform well in order to support resource-constrained devices or applications characterised by frequent microtransactions.

Future research should prioritise the development of lightweight consensus mechanisms, various efficient data storage solutions, smooth cross-chain interoperability, in addition to strong privacy safeguards within blockchain systems. Integrating blockchain in edge computing along with artificial intelligence will considerably change the role. The combination is expected to significantly affect the environment. Long-term security requires individuals to adopt quantum-resistant cryptography and authorities to establish clear regulations. Collaboration among academia, industry, government, and standardization bodies is essential. Key challenges include optimizing consensus protocols for low-power devices, managing large-scale on- and off-chain data, standardizing cross-chain protocols for secure transfers, and balancing transparency with privacy to ensure regulatory compliance. They also focus on designing incentives for reputation systems that promote secure data sharing across platforms. Addressing these important issues will be essential for effectively guiding future research efforts. It is essential for supporting the evolution of blockchain technologies while adapting to the dynamic requirements of IoT ecosystems.

References

1. S. Hirner, J. Dhakal, M. C. Broccoli, M. Ross, E. J. Calvello Hynes, and C. B. Bills, "Defining measures of emergency care access in low-income and middle-income countries: A scoping review," *BMJ Open*, vol. 13, no. 4, pp. 505–518, 2023, doi: 10.1136/bmjopen-2022-067884.
2. "Blockchain State-of-the-Art: Architecture, Use Cases, Consensus, Challenges and Opportunities," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 8, pp. 1010–1023, 2021, doi: 10.1016/j.jksuci.2021.08.005.
3. "The Environmental Impact of Cryptocurrencies Using Proof of Work and Proof of Stake Consensus Algorithms: A Systematic Review," *Journal of Environmental Management*, p. 116530, 2023, doi: 10.1016/j.jenvman.2022.116530.
4. S. Raizada, "Public, Private & Consortium Blockchains: Which Network Fits the Use Case?," 2026. Accessed: Oct. 11, 2026. [Online]. Available: https://www.blockchain-council.org/blockchain/public-private-consortium-blockchains/
5. Suliman, "Monetization of IoT Data Using Smart Contracts," *IET Networks*, vol. 8, no. 1, pp. 32–37, 2019, doi: 10.1049/iet-net.2018.5026.
6. J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," 2016. [Online]. Available: https://lightning.network/lightning-network-paper.pdf
7. V. Varriale, A. Cammarano, F. Michelino, and M. Caputo, "Integrating Blockchain, RFID and IoT Within a Cheese Supply Chain: A Cost Analysis," *Journal of Industrial Information Integration*, vol. 34, p. 100486, 2023, doi: 10.1016/j.jii.2023.100486.
8. H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with Internet of Things: Benefits, Challenges, and Future

Directions," *International Journal of Intelligent Systems and Applications*, vol. 10, no. 6, pp. 40–48, 2018, doi: 10.5815/ijisa.2018.06.05.

9. D. Na and S. Park, "IoT-Chain and Monitoring-Chain Using Multilevel Blockchain for IoT Security," *Sensors*, vol. 22, no. 21, p. 8271, 2022, doi: 10.3390/s22218271.
10. L. Song, X. Ju, Z. Zhu, and M. Li, "An Access Control Model for the Internet of Things Based on Zero-Knowledge Token and Blockchain," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, 2021, doi: 10.1186/s13638-021-01986-4.
11. G. Fernández-Blanco, I. Froiz-M'íguez, P. Fraga-Lamas, and T. M. Fernández-Caramés, "Design, Implementation and Practical Energy-Efficiency Evaluation of a Blockchain Based Academic Credential Verification System for Low-Power Nodes," *Applied Sciences*, vol. 15, no. 12, p. 6596, 2025, doi: 10.3390/app15126596.
12. D. Puthal, S. P. Mohanty, V. P. Yanambaka, and E. Kougianos, ": A Novel Consensus Algorithm for Fast, Scalable Private Blockchain for Large-Scale Frameworks," *arXiv preprint arXiv:2001.07297*, 2020, [Online]. Available: https://arxiv.org/abs/2001.07297
13. P. Charalampidis and A. Fragkiadakis, "When Distributed Ledger Technology Meets Internet of Things: Benefits and Challenges," *arXiv preprint arXiv:2008.12569*, 2020, doi: 10.48550/arXiv.2008.12569.