Hybrid Blockchain Architectures for Securing Industrial IoT Data

[1]Rakesh Rohan Budige

[1]Department of Computer Science, University of Illinois Springfield, IL, USA

Corresponding Author: Rakesh Rohan Budige, Email: rakeshrohanbudige@outlook.com

Abstract

Industrial Internet of Things (IIoT) has grown tremendously to transform industries with real-time sensing, predictive repairs, and decision-making with insights across manufacturing, logistics, energy, and healthcare. Adoption of massive networks of connected devices, however, creates serious concerns related to security, privacy, and trust. Traditional centralized security systems suffer from issues of single points of failure, low scalability, and operational costs that are too high. Blockchain technology has come to offer a tenable substitute with its inherent properties of decentralization, immutability, and openness of ledgers. In its single versions of either public, private, or consortium ones, however, blockchain schemes suffer from imperfections when reassailed for deployment in heterogeneous and resource-scarce IIoT space.

The article creates hybrid blockchain architectures that bring together public and private blockchain advantages to solve these issues. Public chains ensure auditability and trust with external partners while private chains ensure efficiency and confidentiality of information for industrial processes. The article overviews existing techniques, describes key building blocks of architectures such as consensus models, smart contracts, and cross-chain messaging, and shows hybrid models' benefits in solving IIoT-specific requirements. Besides, it covers applied issues of interoperability, governance, and adoption, while future research directions in such areas of lightweight consensus, AI-aided anomaly detection, and standards for interoperability are represented. The conclusion is that hybrid blockchain is a strong direction to securing IIoT environments with scalability, privacy, and openness in balance.

Keywords: Industrial IoT, Hybrid Blockchain, Data Security, Cross-Chain Communication, Smart Contracts

1. Introduction

Industrial Internet of Things (IIoT) has emerged as a corner stone of modern industrial development, connecting machines, sensors, controllers, and enterprise systems into fully interlinked digital worlds. By enabling real-time monitoring, predictive maintenance, and intelligent decision-making, IIoT technologies revolutionized operational procedures in manufacturing, logistics, power, and healthcare sectors. With a predicted install base across industrial networks of more than a billion devices, complexity and quantity of resultant data are increasing at historic rates. While that growth has accompanied grave concerns involving security, privacy, and trustworthiness of IIoT data, it has also reflected urgent imperatives for modern industries to address these problems [1].

Traditional security solutions rely principally upon central schemes such as encryption schemes and cloud authentication schemes. While these provide various levels of protection, these are normally fraught with scalability issues, single points of failure, and vulnerabilities to advanced cyberattacks. A breech of a central authority has the very real ability to destroy the entire industrial network. These shortcomings identify a need for stronger, more decentralized, more open mechanisms for securing industrial information [2].

Due to its immutability, decentralization, and transparency properties, blockchain technology has been studied thoroughly for its suitability for application to IoT and IIoT settings. But having all dependencies on one type of blockchain has its own set of issues. Although public blockchains are best for great transparency and audit capability, they suffer from high delay, low capacity, and high-power consumption. Private blockchains give fast settlement of transactions and tighter control but do not manage to provide distributed trust and openness that would be required for multi- stakeholder industrial platforms. Consortium blockchains aim to balance these trade-offs but again fail to meet globally scalability and operability requirements [3].

More recent studies confirm this perception by recognizing convergence across IoT, blockchain, and artificial intelligence in industrial and supply chain use cases. For instance, Kadam et al. show how supply chain quality management digital transformation comes to depend more heavily on IoT, AI, and blockchain to enhance visibility and efficiency while creating problems in data security and interoperability [4] . In similar vein, another study explores digital twin integration of smart manufacturing, showing how cyber-physical systems and IoT-capable models require secure, real-time sharing of data, a capability better suited to hybrid blockchain architectures [5] . In energy, another study proposes an AI-driven hybrid solar power system secured with blockchain-enacted smart grids, underscoring hybrid architectures' inter-domain potential for balance between efficiency, transparency, and robustness. Collectively, these studies confirm that hybrid blockchain methods are not unique to a single domain but are underlying mechanisms across industries for whom secure, scalable, and interoperable management of data is most critical [6].

This dichotomy has provoked growing interest in hybrid blockchain architectures that combine the best of both worlds between public and private chains to overlay efficiency and trust upon one another. In this article, we discuss hybrid blockchain models' prospects for securing IIoT data, delving into their structural building blocks, their merits and demerits, and directions for future work.

2. Literature Review: Blockchain in IIoT Security

Industrial Internet of Things (IIoT) system security has been gaining immense focus over years due to growing threats of cyber-attacks to critical infrastructure. Conventional solutions rely on encryption, intrusion detection systems, and centralized cloud authentication to protect communications of devices. While demonstrated to be operable in few cases, these centralized schemes are still vulnerable to denial-of-service attacks, insider attacks, and system-wide breaches from single points of failure. Additionally, growing heterogeneity of IIoT devices, from low-power sensors to high-performance controllers, renders it challenging to implement uniform security mechanisms [7].

Blockchain has been suggested to the IIoT security discussion as a decentralized alternative that might serve to mitigate these threats. Public blockchain platforms such as Ethereum provide visibility and tamper resistance but are normally maligned for high delay of transaction, scalability limitations, and high-power consumption. Private blockchain can provide faster transaction settlement, cost effectiveness, and robust control over rights of access but is short of being fully decentralized and therefore might reintroduce trust issues. Consortium blockchain adopts a midpoint position by distributing governance over a pre-disclosed set of players, but their limited openness prevents adoption across wider, more heterogeneous industrial communities [8].

More recent studies began to talk about hybrid blockchain approaches for tradeoffs between efficiency and transparency. Hybrid schemes for supply chain and healthcare sectors showed their capacity to enable sensitive data to remain on private chains while committing integrity proofs to public chains for auditing. Despite these recent studies, however, very little has been developed in a structured manner for serving special requirements of IIoT systems such as real-time response, resource-constrained nodes, and heterogeneity-aware interoperations across industrial environments [9].

This gap highlights that further research work is required on hybrid blockchain infrastructures for IIoT with added focus on scalability, security, privacy, and inter-chain communications.

3. Hybrid Blockchain Architecture for IIoT

Hybrid blockchain model takes the best of both worlds - i.e., public and private blockchain - to deploy a more robust and adaptable Industrial Internet of Things (IIoT) system. It is different from one-chain deployments because a hybrid system can manage sensitive industrial data being kept in private ledgers while offering openness and trust through virtue of anchoring to public ledgers. It is best suited to IIoT environments, where sensitivity of data, operational efficiency, and trust of all players coexist [10].

Data segmentation lies at the core of hybrid blockchain execution. And operational and sensitive data, such as machine telemetry, production planning, or algorithms, continue to be stored and authenticated on private or consortium blockchain networks operated by either the organization or its trusted partners. While aggregated data like hashed transaction verifications or compliance record is periodically written to a public blockchain to secure immutability and accountability. It helps industries to maintain confidentiality while demonstrating regulatory compliance and visibility to external auditors or partners [11][12].

Hybrid blockchain integration with IIoT can be conceptualized across multiple layers:

- Perception Layer: Includes sensors, actuators, and RFID tags that generate raw data.
- Network Layer: Utilizes protocols such as 5G, LPWAN, or SDN for efficient data transmission.
- Application Layer: Facilitates predictive maintenance, asset management, and real-time analytics.

Blockchain Integration Layer: Connects private and public chains to enable cross-chain messaging and execution of smart contracts.

Key features of hybrid models are smart contracts for automated execution of data access policy, variety of consensus (e.g., PBFT in private chains and PoS for public chains), and bridges between chains for interoperation. By reconciling efficiency of private chains with trust of public networks, hybrid models of blockchain produce a balanced result to secure IIoT while satisfying heterogeneous needs of industry players.

4. Components of the Proposed Hybrid Framework

A hybrid blockchain system to secure Industrial IoT (IIoT) data relies on integrating multiple technical components that collectively address problems of security, scalability, and interoperability. These become specifications of how data flows, of how trust is governed, and of how multiple blockchains interact throughout industrial environments.

Consensus Mechanisms: Hybrid designs implement different consensus mechanisms across different layers of their implementation. With respect to their public chains implementation, these chains can implement energy-efficient algorithms such as Proof of Stake (PoS) or Proof of Authority (PoA) to allow for transparency. The private chains can implement Byzantine Fault Tolerant (BFT) algorithms such as RAFT or PBFT for fast and secure verification. With different mechanisms applied, both trust and efficiency are achieved [13].

Smart Contracts: Automated functionality in IIoT is rooted in smart contracts. Smart contracts manage device interactions, enforce data access policy, and allow for conditional event triggers, such as shutting down machines in response to outlier readings from sensors. Automation eliminates the need for human monitoring while ensuring consistency [14].

Cross-Chain Communication: It is possible to ensure interoperability between private and public chains with such cross-chain communications as atomic swaps, sidechains, or relay protocols. These technologies allow for free movement of data or transaction proofs across blockchains, thereby ensuring synchronization without being a threat to security [15].

Identity and Access Management: Decentralized Identifiers (DIDs) and verifiable credentials are used for secure authentication and authorization of IIoT devices. This prevents unauthorized nodes from feeding malicious data into the system [16].

Data Management Strategy: The sensitive industrial information is kept on private chains for confidentiality purposes, while compliance proofs and hashed versions are kept on public chains periodically for auditability purposes. These in combination lead to a robust architecture capable of satisfying IIoT’s double challenge of efficiency and trust [17].

5. Benefits of Hybrid Blockchain for IIoT

Industrial implementation of hybrid blockchain designs for Industrial IoT (IIoT) has a number of benefits that directly address single-chain deployment shortcomings. Organizations can align efficiency, privacy, and trust by mixing private and public blockchains appropriately at a strategic level.

Scalability and Efficiency: Private blockchains manage voluminous data transfers from IIoT devices without delay and high costs of public chains. This ensures that real-time applications such as predictive maintenance and monitoring of machines are not impacted.

Data Privacy and Confidentiality: Sensitive operation data is stored in personal ledgers to prevent leakage of trade secrets, manufacturing processes, and proprietary analyses. Only non-sensitive information or hashed transaction verifications are connected to the public chain while minimizing leakage of data risk.

Transparency and Auditability: Public chains present imperishable ledgers of significant happenings or compliance data. This gives a boost to accountability and provides external parties such as regulators, suppliers, and clients to verify authenticity of data without having access to confidential details.

Cyber-Resilience: It eliminates points of single failure by distributing trust across multiple blockchains. Even with a single chain being compromised, the system stays functional overall because of redundancy and immutability.

Cost Optimization: By decreasing reliance on expensive public blockchain transactions and moving bulk work to private chains, businesses can considerably cut operation costs and still maintain necessary transparency. Stakeholder Trust: Hybrid systems permit safe cooperation between various industrial ecological partners, promoting trust and lasting relationships.

6. Challenges and Limitations

While hybrid blockchain infrastructures are of immense promise to secure Industrial IoT (IIoT) deployments, their adoption is accompanied with several technical and organizational problems that must be addressed for large-scale deployment.

Interoperability Issues: A significant challenge lies in ensuring seamless inter-operation between private and public chains. Present models of cross-chain communications, such as sidechains or atomic swaps, are still in their growth phase and cannot necessarily guarantee full reliability or security.

Latency and Throughput Trade-offs: Although hybrid models improve scalability, real-time IIoT use cases such as industrial automation and predictive maintenance require ultra-low latency. Balancing transaction speed and blockchain security appropriately remains a significant challenge to be solved.

Governance Complexity: Determining what to retain on private chains and what to anchor to public chains can be contentious, especially in multi-stakeholder systems. Governance models are required to explicitly specify roles, responsibilities, and access rights.

Security Issues in Cross-Chain Protocols: Although blockchains themselves are strong, bridges between them can bring vulnerability. Attackers can target vulnerabilities in interoperability frameworks at their weak points, with possible implications for the whole hybrid system.

Cost and Infrastructure Overhead: Both private and public blockchains require massive infrastructural investments. Smaller companies may find it costly for hybrid blockchain implementation than for regular security solutions.

Adoption Barriers: Broad adoption across sectors is restricted by nonstandard procedures and platforms. In addition, organizational hesitation to adopt disruptive technologies can retard implementation. In short, while hybrid blockchain models address significant IIoT security vulnerabilities, it is required to eliminate these vulnerabilities for their fieldable and sustainable deployment.

7. Future Research Directions and Conclusion

Industrial IoT (IIoT) hybrid blockchain designs are only just starting to materialize, and most of these prospective future directions show tremendous potential. Following that list is the building of lightweight consensus algorithms that are resource-optimized for IIoT devices that are resource-constrained. In their nature, traditional algorithms, while being secure, are usually power- and compute-thirsty. In preparation for their futures, new technologies must focus on low-power protocols that balance efficiency with speed.

Another direction of studies lies in integrating artificial intelligence (AI) and machine learning (ML) with hybrid blockchain networks. Predictive analytics and real-time AI-powered anomaly detection can improve IIoT security by identifying malicious activity or suspicious flows of data in real time, while blockchain offers tamper-proof records of such events.

Standards for interoperability are also a major area of future study. Establishing world-recognized standards for cross-chain communications can simplify adoption and ensure consistency across multiple industrial settings. Moreover, developing simulation settings and testbeds for hybrid blockchain for IIoT will enable researchers and practitioners to experiment with system performance prior to deployment in real settings.

In sum, hybrid blockchain architectures hold immense potential in addressing both issues of system openness and information secrecy in IIoT. Combining operational effectiveness with private chains and accountability with public chains, hybrid systems offer a balanced approach to securing industrial data. Although adoption, governance, and interoperability concern still persist, ongoing advancements with blockchain, industrial automation, and artificial intelligence are laying down foundations for scalable, resilient, and reliable IIoT systems. Hybrid blockchain can thus be regarded not only as a security upgrade, but also a strategic enabler of Industry 4.0 and its successors.

8. References

1. Malik PK, Sharma R, Singh R, et al (2021) Industrial Internet of Things and its Applications in Industry 4.0: State of The Art. Comput Commun 166:. https://doi.org/10.1016/j.comcom.2020.11.016

2. Sarker IH (2023) Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. Annals of Data Science 10

3. Lin SY, Zhang L, Li J, et al (2022) A survey of application research based on blockchain smart contract. Wireless Networks 28:. https://doi.org/10.1007/s11276-021-02874-x

4. Akash Abaji Kadam, Tejaskumar Vaidya, & Subba rao katragadda. (2025). Digital Transformation of Supply Chain Quality Management: Integrating AI, IoT, Blockchain, and Big Data. *Journal of Economics, Finance and Accounting Studies* , *7*(3), 41-49. https://doi.org/10.32996/jefas.2025.7.3.5

5. Kadam AA, Thaker H, Gundeti R, et al (2025) A Comprehensive Review on Digital Twin Integration in Smart Manufacturing Technologies, Challenges, and Future Trends. Journal of Artificial Intelligence & Cloud Computing 1–10. https://doi.org/10.47363/JAICC/2025(4)470

6. Mamodiya, U., Kishor, I., Garine, R. *et al.* Artificial intelligence based hybrid solar energy systems with smart materials and adaptive photovoltaics for sustainable power generation. *Sci Rep* **15**, 17370 (2025). https://doi.org/10.1038/s41598-025-01788-4

7. Khraisat A, Alazab A (2021) A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity 4:. https://doi.org/10.1186/s42400-021-00077-7

8. Xu M, Chen X, Kou G (2019) A systematic review of blockchain. Financial Innovation 5

9. Bak O, Braganza A, Chen W (2025) Exploring blockchain implementation challenges in the context of healthcare supply chain (HCSC). Int J Prod Res 63:. https://doi.org/10.1080/00207543.2023.2286491

10. Balto KE, Yamin MM, Shalaginov A, Katt B (2023) Hybrid IoT Cyber Range. Sensors 23:. https://doi.org/10.3390/s23063071

11. Sedlmeir J, Lautenschlager J, Fridgen G, Urbach N (2022) The transparency challenge of blockchain in organizations. Electronic Markets 32:. https://doi.org/10.1007/s12525-022-00536-0

12. Akash Abaji Kadam, Ramakrishna Garine, Supriya Akash Kadam (2024) Revolutionizing inventory management: A comprehensive automated data-driven model using power BI incorporating

industry 4.0. World Journal of Advanced Research and Reviews 24:477–488. https://doi.org/10.30574/wjarr.2024.24.1.3035

13. Kaur S, Chaturvedi S, Sharma A, Kar J (2021) A Research Survey on Applications of Consensus Protocols in Blockchain. Security and Communication Networks 2021

14. Himeur Y, Elnour M, Fadli F, et al (2023) AI-big data analytics for building automation and management systems: a survey, actual challenges and future perspectives. Artif Intell Rev 56:. https://doi.org/10.1007/s10462-022-10286-2

15. Anthony Jnr B (2024) Enhancing blockchain interoperability and intraoperability capabilities in collaborative enterprise-a standardized architecture perspective. Enterp Inf Syst 18:. https://doi.org/10.1080/17517575.2023.2296647

16. Fan X, Chai Q, Xu L, Guo D (2020) DIAM-IoT: A decentralized identity and access management framework for internet of things. In: BSCI 2020 - Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, Co-located with AsiaCCS 2020

17. Fang J, Feng T, Guo X, et al (2024) Blockchain-cloud privacy-enhanced distributed industrial data trading based on verifiable credentials. Journal of Cloud Computing 13:. https://doi.org/10.1186/s13677-023-00530-7