Frontiers in Emerging Computer Science and Information Technology (Open Access)

Volume 02, Issue 04, April 2025,
Publish Date: 01-04-2025
PageNo.01-06

Blockchain for Trustworthy Interoperability in Industry 4.0: Opportunities and Implementation Considerations

Dr. Lucas Pereira
Institute for Systems and Computer Engineering, Technology and Science (INESC TEC), Porto, Portugal

ABSTRACT

Industry 4.0 envisions highly interconnected, intelligent manufacturing ecosystems where seamless interoperability between machines, systems, and stakeholders is critical. However, ensuring data integrity, trust, and secure collaboration across organizational boundaries remains a significant challenge. Blockchain technology offers a promising solution to establish trustworthy interoperability by providing decentralized, tamper-evident records and automated consensus mechanisms. This paper explores the opportunities and implementation considerations of leveraging blockchain within Industry 4.0 environments. It discusses potential benefits such as enhanced data provenance, secure machine-to-machine communication, transparent supply chain tracking, and automated smart contract enforcement. Furthermore, it examines practical challenges, including scalability limitations, integration with legacy systems, standardization gaps, and regulatory implications. By analyzing current research and real-world pilot deployments, this study provides insights to guide practitioners and policymakers in adopting blockchain-enabled interoperability frameworks for smart manufacturing.

KEYWORDS: Blockchain, Industry 4.0, interoperability, trustworthy systems, smart manufacturing, decentralized ledger, supply chain transparency, data integrity, machine-to-machine communication, smart contracts.

INTRODUCTION

Industry 4.0, characterized by the convergence of cyber-physical systems (CPS), the Internet of Things (IoT), cloud computing, and big data analytics, is reshaping the manufacturing and industrial landscape [Lu, 2017; Suresh et al., 2020; Kumar et al., 2023]. This paradigm envisions highly automated, intelligent, and interconnected factories where physical processes are digitally twinned and optimized in real-time [Uhlemann et al., 2017; Javaid et al., 2023]. The successful realization of Industry 4.0 relies critically on the seamless exchange and understanding of information among diverse, heterogeneous systems, machines, sensors, and software applications—a concept known as interoperability [Allian, 2021; Allian et al., 2021; Link et al., 2018]. Without robust interoperability, the promise of interconnected smart factories remains largely unrealized, leading to data silos, inefficiencies, and limited automation [Schulte and Colombo, 2017].

Beyond mere connectivity and data exchange, the complexity and distributed nature of Industry 4.0 environments introduce a paramount requirement for trustworthiness. Participants in these ecosystems—ranging from suppliers and manufacturers to logistics providers and end-users—must be confident in the integrity, authenticity, and confidentiality of shared data and processes [Al-Ali et al., 2018; Bicaku et al., 2017; Fraile et al., 2018]. Traditional centralized trust models, relying on single points of control, often fall short in such dynamic, multi-party settings, presenting vulnerabilities to malicious attacks, data manipulation, and single-point failures [Hawlitschek et al., 2018]. The need for secure, transparent, and immutable records becomes increasingly vital.

In this context, blockchain technology has emerged as a disruptive innovation with the potential to fundamentally transform how trust and interoperability are managed in Industry 4.0 systems [Ahram et al., 2017; Christidis and Devetsikiotis, 2016; Fernandez-Carames and Fraga-Lamas, 2019]. As a decentralized, distributed, and immutable ledger technology, blockchain inherently offers properties such as transparency, security, and resistance to tampering [Nakamoto, 2009; Alghamdi et al., 2024]. Its capacity to enable secure, peer-to-peer transactions without the need for a central authority directly addresses the trust deficit in distributed environments. Furthermore, its underlying mechanisms, particularly smart contracts, hold significant promise for automating interactions and enforcing agreed-upon protocols, thereby facilitating richer forms of interoperability.

This article aims to explore the opportunities that blockchain technology presents for achieving trustworthy interoperability in Industry 4.0 systems. We will synthesize current research to highlight how blockchain's core properties can address the unique challenges of trust and interoperability in this domain. Furthermore, we will discuss key implementation considerations and challenges that must be overcome for the successful adoption of blockchain in industrial settings. By doing so, this work seeks to provide a comprehensive overview for researchers and practitioners navigating the integration of cutting-edge technologies within the Industry 4.0 paradigm.

METHODS

To provide a comprehensive understanding of blockchain's role in trustworthy interoperability for Industry 4.0, this article employs a conceptual review methodology. This approach involves synthesizing findings from a curated selection of existing literature to construct a coherent argument and identify key themes, opportunities, and challenges. Unlike an empirical study involving data collection from a specific case, this methodology draws on a broad range of scholarly and industry publications to establish a theoretical framework and present consolidated insights.

Data Source and Selection

The primary data source for this article is the set of references provided, which covers various aspects of Industry 4.0, blockchain technology, interoperability, and trustworthiness. These references were selected for their direct relevance to the intersection of these domains. The selected literature includes:

- Overviews of Industry 4.0 technologies and challenges [Lu, 2017; Suresh et al., 2020; Horváth and Szabó, 2019; Kumar et al., 2023].
- Foundational concepts and challenges of interoperability and trustworthiness in industrial systems [Allian, 2021; Allian et al., 2021; Al-Ali et al., 2018; Bicaku et al., 2017; Fraile et al., 2018; Link et al., 2018].
- Comprehensive reviews and specific applications of blockchain technology [Ahram et al., 2017; Christidis and Devetsikiotis, 2016; Fernandez-Carames and Fraga-Lamas, 2019; Alghamdi et al., 2024; Nakamoto, 2009].
- Discussions on the convergence of blockchain with IoT, data management, and supply chain [Chen et al., 2019; Kolahan et al., 2021; Li and Qiao, 2023; Manasa and Leo Joseph, 2023; Peralta et al., 2019; S.Perera et al., 2020; ul Ain Arshad et al., 2023; Wang et al., 2018].
- Software architecture principles and evaluation [Bass et al., 2012; Knodel and Naab, 2016; Kuhn et al., 2018; Antonino et al., 2019].
- Ethical and regulatory considerations for blockchain and Industry 4.0 [Anjum et al., 2017; ISO/IEC, 2011; Pazaitis et al., 2017].

This broad selection ensures a multi-faceted perspective on the subject matter, covering both theoretical underpinnings and practical considerations.

Data Extraction and Synthesis

Information from each relevant reference was extracted and thematically synthesized. The core elements extracted included:

- Definitions and characteristics of Industry 4.0, interoperability, and trustworthiness.
- Specific challenges related to trust and interoperability in industrial environments.
- Blockchain's properties and mechanisms (e.g., decentralization, immutability, smart contracts).
- Proposed or implemented applications of blockchain in Industry 4.0 to address trust and interoperability.
- Identified benefits and drawbacks of integrating blockchain into industrial systems.
- Implications for system architecture, security, and data management.

The extracted insights were then conceptually grouped into categories representing the core contributions of blockchain to trustworthy interoperability and the key challenges to its implementation. This categorization process was iterative, allowing for the emergence of dominant themes from the literature. The synthesis process involved cross-referencing findings across different studies to identify consensus, contrasting viewpoints, and areas requiring further investigation.

Conceptual Framework Development

Based on the synthesized literature, a conceptual framework was developed to illustrate how blockchain contributes to achieving trustworthy interoperability. This framework posits that blockchain acts as a foundational layer, providing decentralized trust and secure data provenance, which in turn enhances the various layers of interoperability (e.g., technical, syntactic, semantic, and organizational) that are critical for Industry 4.0. The framework also considers the architectural drivers and solutions relevant to Industry 4.0, as articulated by Antonino et al. [2019] and Allian et al. [2021], and integrates them with blockchain's capabilities.

While this article does not present empirical results from a specific case study, the discussion will draw upon existing real-world or simulated applications mentioned in the literature to provide context and illustrate the practical implications of blockchain integration. The methodology emphasizes a qualitative synthesis approach [Strauss and Corbin, 1998] to build a comprehensive understanding, providing a theoretical basis for future empirical research. The guidelines for survey studies in software engineering [Molléri et al., 2016] and experimental design [Wohlin et al., 2012] were considered to ensure the rigor of the conceptual review, even if not directly applied in an empirical context.

RESULTS

The synthesis of the literature reveals several key ways in which blockchain technology can contribute to establishing trustworthy interoperability within Industry 4.0 systems. These contributions span enhanced security, improved data integrity, facilitated automated interactions, and new models for decentralized collaboration.

1. Enabling Decentralized Trust and Enhanced Security

Blockchain's fundamental properties directly address the trust challenges inherent in multi-stakeholder Industry 4.0 environments.

- Immutability and Transparency: The distributed ledger nature of blockchain ensures that once data is recorded, it cannot be altered without detection. This immutability provides a high degree of data integrity and auditability, fostering trust among participants who might not otherwise trust each other [Alghamdi et al., 2024; Christidis and Devetsikiotis, 2016]. The transparent, yet pseudonymized, record of transactions enhances accountability across the system.
- Decentralized Control: By eliminating the need for a central authority, blockchain mitigates risks associated with single points of failure and malicious central actors [Nakamoto, 2009]. This decentralized trust mechanism is crucial for the distributed nature of Industry 4.0, where numerous independent entities need to interact securely [ul Ain Arshad et al., 2023].
- Cryptographic Security: The use of cryptographic hashes and digital signatures ensures the authenticity and integrity of data and transactions. This provides a robust layer of security for IoT devices and other components within Industry 4.0 networks, protecting against tampering and unauthorized access [Manasa and Leo Joseph, 2023; Peralta et al., 2019]. Specific applications include enhancing initial trust and access control for industrial systems [Kjersgaard and Eriksena, 2018].

2. Facilitating Enhanced Interoperability Through Smart Contracts and Data Management

Beyond basic connectivity, blockchain can enable deeper levels of interoperability, particularly through smart contracts.

- Automated Interaction with Smart Contracts: Smart contracts—self-executing contracts with the terms of the agreement directly written into code—can automate complex interactions and data exchanges between machines and systems in Industry 4.0 [Christidis and Devetsikiotis, 2016; Fernandez-Carames and Fraga-Lamas, 2019]. This reduces the need for human intervention and minimizes errors, streamlining workflows and enabling seamless interoperability at a process level [Al-Ali et al., 2018].
- Secure and Shared Data Management: Blockchain can provide a secure and consistent platform for managing large volumes of data generated in Industry 4.0. For instance, blockchain-based personnel big data management systems demonstrate its utility in handling and sharing data across distributed entities [Chen et al., 2019]. This also applies to cross-border B2B platforms, where blockchain can enhance data interoperability and trust building [Li and Qiao, 2023].
- Interoperability for Digital Twins: The integrity and trustworthiness of data used in digital twin applications for Industry 4.0 can be significantly enhanced by blockchain, ensuring that the digital representation accurately reflects the physical asset [Javaid et al., 2023].
- Standardization and Trustworthiness Drivers: By providing a common, immutable ledger, blockchain can implicitly drive standardization of data exchange protocols and interactions, supporting architecture drivers for trustworthy interoperability [Allian, 2021; Allian et al., 2021]. Blockchain standards themselves are evolving to support compliance and trust [Anjum et al., 2017].

3. Applications in Industry 4.0 Contexts (Illustrative)

Blockchain's potential extends to various specific Industry 4.0 applications:

- Supply Chain Transparency: In manufacturing supply chains, blockchain can provide end-to-end traceability of products and components, from raw materials to finished goods [S.Perera et al., 2020]. This enhances transparency, reduces fraud, and builds trust among all supply chain participants, which is crucial for complex industrial production.
- Energy Management: Blockchain-based solutions are being explored for decentralized energy demand-side management in industrial settings and residential buildings, showcasing its potential in

energy transactions and data integrity [Kolahan et al., 2021].

- Healthcare and IoT: While not directly Industry 4.0, applications in parallel healthcare systems [Wang et al., 2018] and IoT interoperability [ul Ain Arshad et al., 2023] demonstrate blockchain's capacity for secure data sharing and decentralized trust management across distributed, heterogeneous networks, mirroring Industry 4.0 requirements.

The results indicate that blockchain offers a robust framework for addressing the intertwined challenges of trust and interoperability in Industry 4.0. Its core features—decentralization, immutability, and smart contract capabilities—provide tangible architectural solutions to enhance the security, transparency, and automated interaction necessary for complex industrial ecosystems.

DISCUSSION

The preceding synthesis highlights blockchain's transformative potential in achieving trustworthy interoperability within Industry 4.0. By offering inherent security, transparency, and decentralized trust mechanisms, blockchain directly addresses fundamental architectural and operational challenges faced by interconnected industrial systems. However, the path to widespread adoption is not without significant implementation considerations and challenges.

Opportunities and Benefits

The unique characteristics of blockchain technology present compelling opportunities for Industry 4.0:

- Enhanced Trust in Decentralized Environments: The ability to establish trust without reliance on a single central authority is perhaps blockchain's most significant contribution. In Industry 4.0, where multiple independent entities (e.g., machines, departments, companies) must collaborate and exchange sensitive data, blockchain provides a verifiable and tamper-proof record of all interactions. This builds confidence and reduces the need for costly intermediaries or extensive auditing.
- Seamless and Secure Data Exchange: Blockchain can underpin a secure data exchange fabric, ensuring that information shared between machines, sensors, and enterprise systems is authentic and unaltered. This is crucial for real-time decision-making and automated processes within smart factories. The cryptographic security ensures data integrity, which is vital for the reliability of cyber-physical systems [Link et al., 2018].
- Automated and Enforceable Agreements via Smart Contracts: Smart contracts enable the automation of complex business logic and agreements directly on the blockchain. This allows for conditional data release, automated payments upon completion of tasks, and enforcement of service-level agreements between disparate industrial components or partners. Such automation reduces human error, speeds up processes, and provides a trustless execution environment, greatly enhancing operational interoperability.
- Improved Traceability and Auditability: The immutable ledger provides a comprehensive and transparent history of all transactions and data points. This inherent traceability is invaluable for quality control, regulatory compliance, and troubleshooting in complex manufacturing processes and supply chains. For example, knowing the provenance of every component in a product becomes straightforward and verifiable.

Implementation Considerations and Challenges

Despite the immense potential, several significant challenges must be addressed for blockchain to achieve widespread adoption in Industry 4.0:

1. Scalability: Current blockchain networks, particularly public ones, often face scalability limitations in terms of transaction throughput and latency [Alghamdi et al., 2024]. Industry 4.0 environments generate vast amounts of data and require real-time processing, demanding high-performance blockchain solutions. Research into layer-2 solutions, sharding, and more efficient consensus mechanisms is crucial to overcome this.
2. Integration with Legacy Systems: Many existing industrial systems are proprietary and not designed for blockchain integration. Seamlessly integrating blockchain solutions with legacy IT and operational technology (OT) infrastructure presents significant technical challenges. This necessitates the development of specialized adapters and middleware, akin to the conceptual virtual automation bus [Kuhn et al., 2018], to bridge the gap. Software architecture principles [Bass et al., 2012; Knodel and Naab, 2016] will be vital here.
3. Data Privacy and Confidentiality: While blockchain offers transparency, many industrial applications require strict data confidentiality. Balancing the need for transparency with privacy requirements (e.g., intellectual property, trade secrets) is a critical design challenge. Solutions may involve privacy-preserving technologies (e.g., zero-knowledge proofs, homomorphic encryption [Peralta et al., 2019]), permissioned blockchains, or off-chain data storage with on-chain hashes.

4. Regulatory and Legal Frameworks: The legal implications of blockchain-based smart contracts and decentralized autonomous organizations (DAOs) in an industrial context are still evolving [Anjum et al., 2017]. Clear regulatory guidance is needed to define legal enforceability, liability, and compliance with existing industry standards (e.g., ISO/IEC SQuaRE [ISO/IEC, 2011]).
5. Cost and Energy Consumption: The computational cost associated with certain blockchain consensus mechanisms (e.g., Proof of Work) and the overall infrastructure investment can be substantial. For resource-constrained industrial IoT devices, energy efficiency is a major concern [Manasa and Leo Joseph, 2023].
6. Organizational Adoption and Skill Gaps: The adoption of blockchain requires not only technical changes but also significant organizational shifts, including new business processes, governance models, and a workforce with specialized blockchain expertise. The "driving forces and barriers of Industry 4.0" apply equally to its underlying technologies [Horváth and Szabó, 2019].

Future Directions

Future research and development efforts should focus on:

- Hybrid Architectures: Exploring hybrid blockchain solutions that combine the strengths of public and private chains, or integrate blockchain with traditional databases and cloud services, to optimize for scalability, privacy, and performance.
- Standardization for Industrial Use Cases: Developing industry-specific standards and protocols for blockchain integration in manufacturing, supply chain, and IoT contexts to facilitate broader adoption and interoperability.
- Performance Optimization: Advancing research into more efficient consensus mechanisms and scaling solutions tailored for the high-throughput, low-latency demands of Industry 4.0.
- Security and Threat Modeling: Continually assessing and mitigating new security vulnerabilities that may emerge with the increasing complexity of blockchain-enabled industrial systems.
- Economic Viability and ROI: Conducting rigorous economic analyses and pilot projects to clearly demonstrate the return on investment and tangible benefits of blockchain for specific Industry 4.0 use cases, like energy management [Kolahan et al., 2021] or parallel healthcare systems [Wang et al., 2018].

In conclusion, blockchain technology holds immense promise for enabling trustworthy interoperability in Industry 4.0 by fostering decentralized trust, enhancing data security, and automating interactions through smart contracts. While significant technical, regulatory, and organizational hurdles remain, ongoing research and strategic implementations can pave the way for a more secure, transparent, and seamlessly integrated industrial future. The systematic approach to understanding architectural drivers and solutions [Antonino et al., 2019] will be critical in this journey.

REFERENCES

[1] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., and Amaba, B. (2017). Blockchain technology innovations. In IEEE TEMSCON, pages 137–141, Santa Clara, CA, USA.

[2] Al-Ali, R., Heinrich, R., Hnetynka, P., Juan-Verdejo, A., Seifermann, S., and Walter, M. (2018). Modeling of dynamic trust contracts for industry 4.0 systems. In ECSA, pages 45:1–45:4, Madrid, Spain.

[3] Alghamdi, Ali, T., Khalid, Rabiya, Javaid, and Nadeem (2024). A survey of blockchain based systems: Scalability issues and solutions, applications and future challenges. IEEE Access, 12:79626–79651.

[4] Allian, A. P. (2021). A Trustworthy Interoperability Architecture for Industry 4.0. Tese de doutorado, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos.

[5] Allian, A. P., Schnicke, F., Antonino, P. O., Rombach, D., and Nakagawa, E. Y. (2021). Architecture drivers for trustworthy interoperability in industry 4.0. IEEE Systems Journal, 15(4):5454–5463.

[6] Anjum, A., Sporny, M., and Sill, A. (2017). Blockchain standards for compliance and trust. IEEE Cloud Computing, 4(4):84–90.

[7] Antonino,P. O.,Schnicke,F.,Zhang,Z.,andKuhn,T.(2019). Blueprints for architecture drivers and architecture solutions for Industry 4.0 shopfloor applications. In ECSA, pages 261–268, Paris, France.

[8] Bass, L., Clements, P., and Kazman, R. (2012). Software Architecture in Practice. Addison-Wesley, 3 edition.

[9] Bicaku, A., Maksuti, S., Palkovits-Rauter, S., Tauber, M., Matischek, R., Schmittner,C.,andMantas,G.(2017). Towardstrustworthyend-to-endcommunicationinindustry 4.0. In IEEE INDIN, pages 889–896, Emden, Germany.

[10] Chen, J., Lv, Z., and Song, H. (2019). Design of personnel big data management system based on blockchain. Future Generation Computer Systems, 101:1122 – 1129.

[11] Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4:2292–2303.

[12] Fernandez-Carames, T. M. and Fraga-Lamas, P. (2019). A review on the application of blockchain to the next

generation of cybersecure industry 4.0 smart factories. IEEE Access, 7:45201–45218.
[13] Fraile, F., Tagawa, T., Poler, R., and Ortiz, A. (2018). Trustworthy industrial IoT gateways for interoperability platforms and ecosystems. IEEE Internet of Things Journal, 5(6):4506–4514.
[14] Hawlitschek, F., Notheisen, B., and Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electronic Commerce Research and Applications, 29:50–63.
[15] Horváth, D. and Szabó, R. Z. (2019). Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities? Technological Forecasting and Social Change, 146:119–132.
[16] ISO/IEC (2011). Systems and software quality requirements and evaluation (SQuaRE) – System and software quality models. 1-41.
[17] Javaid, M., Haleem, A., and Suman, R. (2023). Digital twin applications toward industry 4: A review. Cognitive Robotics, 3:71–92.
[18] Kjersgaard, J. and Eriksena, M. (2018). Access control for industry 4.0 initial trust with blockchain. Technical report, Aalborg University, Aalborg, Denmark. https://projekter.aau.dk/projekter/files/281557079 pp. 1–99.
[19] Knodel, J. and Naab, M. (2016). Pragmatic Evaluation of Software Architectures. Springer, Germany.
[20] Kolahan, A., Maadi, S. R., Teymouri, Z., and Schenone, C. (2021). Blockchain-based solution for energy demand-side management of residential buildings. Sustainable Cities and Society, 75:103316.
[21] Kuhn, T., Antonino, P. O., Damm, M., Morgenstern, A., Schulz, D., Ziesche, C., and Müller, T. (2018). Industrie 4.0 virtual automation bus. In ICSE, pages 121–122, Gothenburg, Sweden.
[22] Kumar, L., Ajay, Sharma, R. K., and Parveen (2023). Smart Manufacturing and Industry 4.0: State-of-the-Art Review, volume 1. Taylor and Francis.
[23] Li, Z. and Qiao, G. (2023). Trust building in cross-border e-commerce: A blockchain-based approach for b2b platform interoperability. pages 246–259.
[24] Link, J., Waedt, K., Ben Zid, I., and Lou, X. (2018). Current challenges of the joint consideration of functional safety cyber security, their interoperability and impact on organizations: How to manage rams + s (reliability availability maintainability safety + security). In ICRMS, pages 185–191, Shanghai, China.
[25] Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research. J. of Industrial Information Integration, 6:1–10.
[26] Manasa, K. and Leo Joseph, L. M. I. (2023). IoT Security Vulnerabilities and Defensive Measures in Industry 4.0, pages 71–112. Springer Nature Singapore, Singapore.
[27] Molléri, J. S., Petersen, K., and Mendes, E. (2016). Survey guidelines in software engineering: An annotated review. In ESEM, pages 58:1–58:6, Ciudad Real, Spain.
[28] Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. Technical report, Bitcoing.org. https://bitcoin.org/bitcoin.pdf pp. 1–9.
[29] Pazaitis, A., Filippi, P. D., and Kostakis, V. (2017). Blockchain and value systems in the sharing economy: The illustrative case of backfeed. Technological Forecasting and Social Change, 125:105 – 115.
[30] Peralta, G., Cid-Fuentes, R. G., Bilbao, J., and Crespo, P. M. (2019). Homomorphic encryption and network coding in IoT architectures: Advantages and future challenges. Electronics, 8(827):1–14.
[31] Schulte, D. and Colombo, A. W. (2017). Rami 4.0 based digitalization of an industrial plate extruder system: Technical and infrastructural challenges. In IECON, pages 3506–3511, Beijing, China.
[32] S.Perera,S.Nanayakkara,M.Rodrigo,S.Senaratne,andWeinand,R.(2020). Blockchain technology: Is it hype or real in the construction industry? J. of Industrial Information Integration, 17:100–12
[33] Strauss, A. L. and Corbin, J. M. (1998). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. SAGE Publications, 2nd edition.
[34] Suresh, A., Udendhran, R., and Balamurugan, M. (2020). Integrating IoT and machine learning–the driving force of industry 4.0. In Internet of Things for Industry 4.0, pages 219–235. Springer.
[35] Uhlemann, T., Lehmann, C., and Steinhilper, R. (2017). The digital twin: Realizing the cyber-physical production system for Industry 4.0. In CIRP, volume 61, pages 335–340, Kamakura, Japan.
[36] ul Ain Arshad, Q., Khan, W. Z., Azam, F., Khan, M. K., and Yu, H. (2023). Blockchain-based decentralized trust management in iot: systems, requirements and challenges. Complex Intelligent Systems, 9:6155–6176.
[37] Wang, S., Wang, J., Wang, X., Qiu, T., Yuan, Y., Ouyang, L., Guo, Y., and Wang, F. (2018). Blockchain-powered parallel healthcare systems based on the acp approach. IEEE Transactions on Computational Social Systems, 5(4):942–950.
[38] Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., and Wess-lén, A. (2012). Experimentation in Software Engineering: An Introduction. Springer-Verlag, Norwell, USA, 2nd edition.