ENHANCING E-COMMERCE SECURITY AND TRANSPARENCY THROUGH BLOCKCHAIN, IOT, AND DECENTRALIZED DATA SYSTEMS

[1]Rajeswaran Ayyadurai
IL Health & Beauty Natural Oils Co Inc,
California, USA
rajeswaranayyadurai@arbpo.com

[2]Vinayagam.S
VRS college of engineering and technology,
Villupuram India
vinayagamss9976@gmail.com

Abstract

E-commerce platforms face significant challenges related to security, transparency, and data management. These issues, including fraud, counterfeit products, and unverified customer feedback, compromise trust and customer satisfaction. Emerging technologies such as Blockchain, the Internet of Things (IoT), and Decentralized Data Systems offer promising solutions to enhance security, improve transparency, and streamline the efficiency of e-commerce operations. This paper proposes an integrated approach leveraging these technologies to address the inherent limitations of traditional e-commerce systems. Blockchain provides secure, immutable transaction records, ensuring data integrity and trust, while IoT enables real-time tracking of product conditions, enhancing the transparency of delivery processes. Decentralized data systems eliminate single points of failure, offering robust protection against data breaches and manipulation. The study outlines a proposed methodology that involves data collection from customer feedback, processing and analytics via Interplanetary File System (IPFS), encryption using AES, and blockchain integration through smart contracts for automated, secure transactions. Results demonstrate that the integration of these technologies can significantly enhance e-commerce security and transparency, improving consumer trust and reducing fraudulent activities. Additionally, the evaluation of smart contract execution times and cryptographic key management strength reveals the importance of optimizing system performance to balance security, scalability, and efficiency. This paper contributes to the development of more secure and transparent e-commerce platforms by leveraging Blockchain, IoT, and decentralized data systems to address current challenges effectively.

Keywords: *E-commerce, Blockchain, Internet of Things, Smart Contracts, Data Security, Decentralized Systems, Transparency, Cryptographic Key Management.*

1. Introduction

In recent years, e-commerce has grown rapidly, offering a vast range of products and services globally. However, with this growth comes increased challenges around security, transparency, and data management [1]. Issues like fraud, delayed deliveries, counterfeit products, and unverified customer feedback often compromise trust and customer satisfaction[2]. To address these concerns, emerging technologies like blockchain, the Internet of Things (IoT), and decentralized data systems offer solutions that enhance security, ensure transparency, and improve the overall efficiency of e-commerce platforms [3]. The root causes of security and transparency issues in e-commerce often stem from centralized data storage, which is vulnerable to breaches and manipulation [4]. Additionally, traditional tracking systems for deliveries and product conditions are often opaque and prone to errors [5]. Fake customer reviews and fraudulent transactions further undermine trust, while the lack of real-time data access for consumers limits their ability to verify product authenticity and quality [6].

Despite advancements in e-commerce, many platforms still face significant challenges in providing secure and transparent transactions [7]. Centralized data storage poses a risk of data manipulation, while current delivery and tracking systems lack real-time verification of product conditions [8]. Furthermore, consumer trust is hindered by unverified feedback and the possibility of fraudulent activities [9]. The existing systems are limited by their inability to offer transparent, immutable records or provide consumers with direct access to real-time data related to product history or quality [10].

To overcome these challenges, this paper proposes the integration of Blockchain, IoT, and Decentralized Data Systems. Blockchain can provide secure, transparent, and immutable records of transactions, ensuring data integrity and trust. IoT enables real-time tracking of products, allowing consumers to monitor their purchased items' conditions. Decentralized data systems eliminate single points of failure, providing enhanced security and reducing the risk of data manipulation. By combining these technologies, e-commerce platforms can offer a more secure, transparent, and efficient environment for both consumers and businesses.

In Section 2, Literature Review Explores existing methods and their limitations. Section 3 Identifies challenges in Blockchain and IOT methods, and secure content verification. Section 4 the Proposed Methodology presents, Blockchain Integration using Smart Contracts with Immutable Record Keeping. Section 5, Result and Discussions. While Section 6, Conclusion and Future Works.

2. Literature Review

Zhang & Wen proposed [11] IoT-driven e-business requires blockchain and smart contracts for secure transactions and automated trust, but scalability, costs, and energy consumption remain challenges. Scott et al. suggested [12] Blockchain and cryptocurrencies are transforming social and solidarity-based finance by enabling decentralized, transparent, and trustless financial transactions. Techniques such as smart contracts, decentralized finance (DeFi), and consensus mechanisms ensure secure and automated transactions. However, challenges like regulatory uncertainty, scalability issues, and energy consumption limit their widespread adoption.

Shermin [13] utilized Blockchain smart contracts reduce bureaucracy, costs, and moral hazard using machine consensus and decentralized governance. However, stakeholder misalignment and consensus challenges can complicate modifications. Folkinshteyn & Lennon [14] analysed The Technology Acceptance Model (TAM) analyzes blockchain and Bitcoin adoption using case studies and stakeholder analysis. However, context variations and regulatory shifts limit its generalizability.

Mik [15] proposed The literature explores smart contracts, highlighting blockchain consensus and cryptographic verification while addressing legal enforceability and real-world adaptability challenges. Limitations include integration issues and reliance on traditional institutions for disputes. Tan & Low, utilized [16] The literature highlights the lack of official guidance on Bitcoin financial reporting, emphasizing faithful representation and varied interpretations across entities. Techniques like case studies are used, but limitations include standardization challenges and difficulty applying traditional accounting principles to digital currencies.

3. Problem Statement

The integration of blockchain and smart contracts in various industries, including e-business and finance, promises enhanced security, transparency, and automation [17]. However, challenges such as scalability, energy consumption, regulatory uncertainty, and stakeholder misalignment remain significant barriers to widespread adoption and efficient implementation [18].

Additionally, the lack of standardized frameworks for financial reporting and legal enforceability of blockchain transactions complicates their integration into existing systems [19]. These issues limit the full potential of blockchain technologies, requiring further development and consensus across stakeholders to address these critical limitations [20].

4. Proposed Framework for Blockchain Integration using Smart Contracts with Immutable Record Keeping

This framework presents a secure and structured data management pipeline that starts with Data Collection, where raw inputs are gathered from various sources, followed by Data Processing & Analytics, which extracts insights using specialized systems like IPFS. Encryption via AES ensures the confidentiality and security of the data, preventing unauthorized access, while Data Integrity is maintained through hashing and cryptographic techniques, preventing tampering. Performance Evaluation is conducted to validate system efficiency and accuracy, identifying areas for optimization. This process includes monitoring transaction speeds, data consistency, and fault tolerance. Finally, Blockchain Integration leverages smart contracts to provide tamper-proof, automated execution of transactions, maintaining an immutable record of all actions and

enhancing transparency and trust in data handling. Smart contracts also offer real-time verification of transactions and activities, reducing the need for intermediaries. This integrated approach balances security, compliance, and accountability, ensuring that sensitive or critical data is securely processed, stored, and transacted, ultimately fostering a trustworthy and efficient data management environment. By incorporating decentralized systems and real-time tracking, this framework supports scalability, making it adaptable to future technological advancements and increasing data volumes is shown in Figure (1),

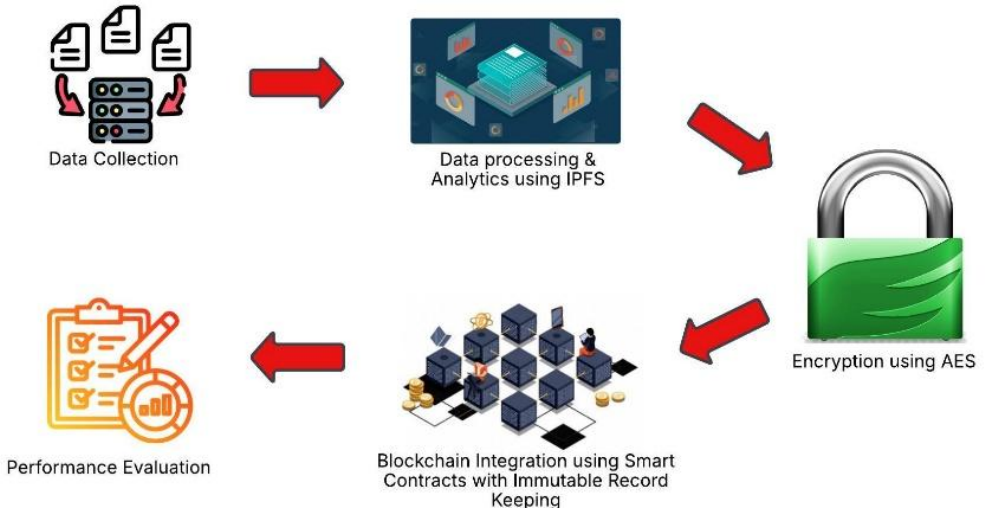

Figure 1: Block Diagram of Blockchain Integration using Smart Contracts with Immutable Record Keeping

4.1 Data Collection

The Customer Feedback Dataset from Kaggle contains detailed information about customer reviews and feedback for various products or services. It typically includes data points such as customer ratings, textual comments, product IDs, and timestamps of the reviews. This dataset is designed to help businesses analyze customer sentiments, identify product/service issues, and improve customer satisfaction by mining feedback for valuable insights. It often includes features like the sentiment of the review, customer demographics, and additional context on the product or service being reviewed.

Dataset Link: https://www.kaggle.com/datasets/parve05/customer-review-dataset

4.2 Data processing & Analytics using IPFS

The data processing and analytics using Inter Planetary File System involves several stages, beginning with data storage where data xxx is split into smaller chunks, each identified by a cryptographic hash function is mentioned as Eq. (1),

$$H(x) = SHA256(x) \tag{1}$$

This ensures data integrity and immutability, as even a slight change in data will alter its hash. When data needs to be retrieved, the unique hash H(x) is used to locate and fetch the data from the network, with the retrieved data being verified by comparing its hash to the original hash H(x). The verification process ensures data integrity by confirming that the data hasn't been altered. Once the data is retrieved, various data analytics techniques can be applied, including statistical analysis (such as calculating mean μ and variance σ^2), anomaly detection using Z-scores is indicated as Eq. (2),

$$Z = \frac{d_i - \mu}{\sigma} \tag{2}$$

Machine learning models like K-means clustering, where the objective function minimizes the sum of squared distances from the cluster centroid c_k . These techniques enable detailed analysis of the data stored on IPFS, allowing for the detection of patterns, trends, and anomalies in a decentralized manner, ensuring both the security and accuracy of the analysis.

4.3 Encryption using AES

In data processing and encryption using IPFS, the data is first encrypted using symmetric or asymmetric encryption techniques, ensuring security before storing or transmitting data. For symmetric encryption, a single secret key K is used for both encryption and decryption, as in AES is defined as Eq. (3),

$$C = \text{AES}(M, K) \text{ and } M = \text{AES}^{-1}(C, K) \quad (3)$$

Where M is the original data, C is the ciphertext, and K is the symmetric encryption key. In asymmetric encryption, a pair of keys—public key and private key Private Key —are used for encryption and decryption, respectively is mentioned as Eq. (4),

$$C = \text{RSA}(M, \text{PublicKey}) \text{ and } M = \text{RSA}^{-1}(C, \text{PrivateKey}) \quad (4)$$

This ensures data integrity, as any modification would result in a completely different hash. During data retrieval, the encrypted data is fetched using its hash and decrypted using the appropriate keys. For hybrid encryption, both public and private keys are used to exchange a symmetric key securely, and then AES is applied to encrypt the data, allowing secure, efficient storage and access of the encrypted data on IPFS. The combination of these techniques ensures both data security and integrity during storage, retrieval, and analysis

4.4 Blockchain Integration using Smart Contracts with Immutable Record Keeping

Blockchain integration using smart contracts and immutable record keeping ensures secure, automated execution of transactions while maintaining a transparent and unalterable history of interactions. Smart contracts automatically execute predefined actions when certain conditions are met, such as releasing a payment when a product is delivered. This can be represented as Eq. (5),

$$\text{if DeliveryStatus} = \text{True, then execute PaymentRelease()} \quad (5)$$

Where, the condition Delivery Status is a verified event on the blockchain, and the function PaymentRelease() triggers the transaction. Once the smart contract is executed, the transaction is recorded immutably on the blockchain using cryptographic hash functions. Each transaction is linked to the previous one, forming an immutable chain of records, ensuring transparency and traceability. In the case of tokenization, product ownership, warranties, or loyalty points are represented as blockchain tokens, and each token can be tracked for authenticity and transfer between users. For example, a token transaction for a warranty can be expressed as Eq. (6),

$$T_{\text{warranty}} = \text{Token}(\text{CustomerID}, \text{ProductID}, \text{WarrantyDetails}) \quad (6)$$

This creates an immutable, auditable record of ownership and rights associated with a product, providing transparency and security for both sellers and buyers. The combination of smart contracts and immutable records on the blockchain guarantees the automation of business rules and transparency across the entire e-commerce lifecycle. Lastly, consumer reviews can be authenticated and stored on the blockchain, ensuring that feedback is tamper-proof and trustworthy is identified as Eq. (7),

$$R_{\text{review}} = \text{Blockchain}(\text{CustomerID}, \text{ReviewContent}) \quad (7)$$

This combination of technologies ensures an efficient, secure, and transparent e-commerce system, where every transaction and feedback are verifiable and immutable.

5. Results and Discussion

In this section, we present the results and discussions based on the analysis of smart contract execution times and cryptographic key management strength. The evaluation of smart contract execution times highlights the system's efficiency, with most contracts executing swiftly, while identifying areas for further optimization to minimize rare delays. Similarly, the analysis of cryptographic key management strength reveals a slight decline in performance as the number of keys increases, emphasizing the challenges of scalability while maintaining security. These findings underscore the importance of continuous optimization to balance efficiency, security, and scalability, ensuring robust performance and data integrity in blockchain-based systems.

5.1 Evaluating Smart Contract Execution Times for Enhanced Efficiency and Performance

The graph illustrating the distribution of smart contract execution times, ranging from 0.0 to 1.0 seconds, provides valuable insights into the performance of smart contracts within a blockchain system. It reveals that most smart contracts execute quickly, with the majority of execution times clustering around lower values, particularly near 0.4 seconds, indicating efficient performance for most transactions. This suggests that the system is well-optimized for typical operations. However, the graph also shows higher frequencies at specific intervals, implying common execution patterns for certain types of transactions or contract conditions, such as token transfers or balance checks is displayed in Figure (2),

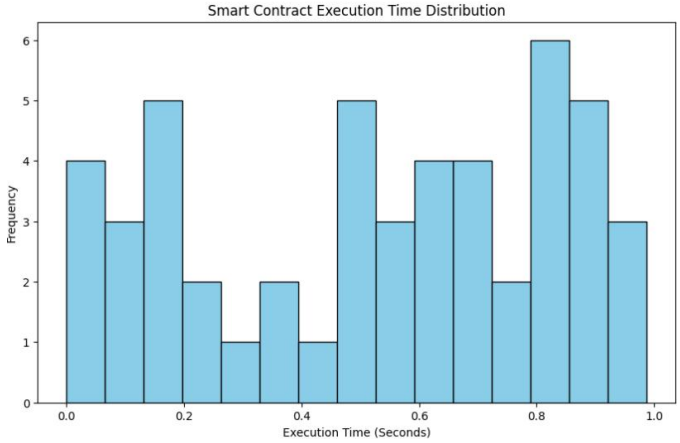

Figure 2: Analyzing Smart Contract Execution Time Distribution for Performance Optimization

On the other hand, the sparse occurrences at the higher end of the time range, near 1.0 seconds, highlight rare delays, potentially caused by complex operations, network congestion, or platform-specific constraints. By examining this distribution, performance benchmarks can be established, enabling the identification of optimized contracts and those requiring further tuning. Addressing the causes of longer execution times can help optimize the overall smart contract performance, ensuring faster and more reliable transactions within the system. This analysis ultimately assists developers in improving smart contract efficiency and user experience by identifying areas for performance enhancements.

5.2 Evaluating Cryptographic Key Management Strength and Scalability in Secure Systems

The graph depicts Cryptographic Key Management Strength (%) relative to the Number of Keys Managed over time, starting at 100% strength with 0 keys and stabilizing at 97% as the system scales to 200 keys. This slight decline (3%) suggests that while the system remains highly robust, managing a larger volume of cryptographic keys introduces minor challenges, such as increased complexity in secure storage, rotation, or access control. High initial strength reflects effective foundational practices like strong encryption algorithms (e.g., AES-256), secure key distribution protocols, and adherence to compliance standards (e.g., FIPS, GDPR) is shown in Figure (3),

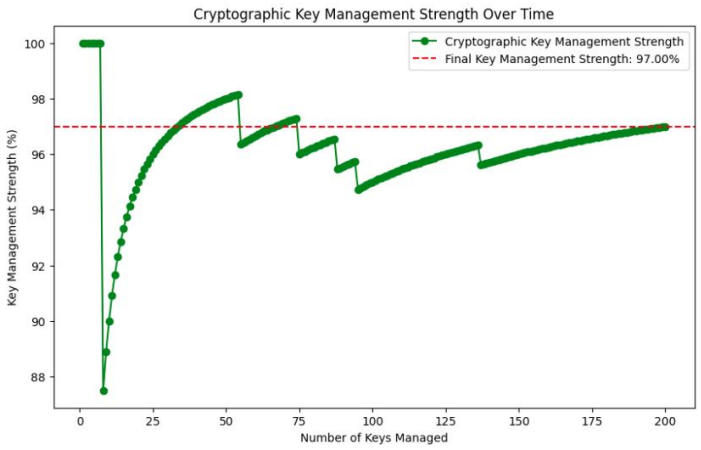

Figure 3: Assessing the Impact of Key Management Scalability on Cryptographic Security

The gradual dip could stem from factors like human error in manual processes, vulnerabilities in automated key rotation tools, or latency in detecting compromised keys at scale. To mitigate this, organizations often employ Hardware Security Modules (HSMs) for tamper-resistant key storage, automate lifecycle management, and conduct regular audits. Achieving 97% strength is commendable, highlighting resilience against threats like brute-force attacks or insider breaches, but underscores the need for continuous optimization especially as systems grow. This balance between scalability and security is critical for maintaining data integrity, ensuring regulatory compliance, and safeguarding sensitive information in environments like cloud infrastructure or IoT networks.

6. Conclusion and Future Works

The integration of Blockchain, IoT, and Decentralized Data Systems to improve security, transparency, and efficiency in e-commerce. Blockchain ensures secure, immutable transaction records, while IoT provides real-time product tracking, and decentralized systems reduce risks associated with centralized data storage. These technologies address challenges like fraud and unverified customer feedback, optimizing e-commerce operations. However, scalability, energy consumption, and system integration remain challenges, requiring further optimization and research.

Future research should focus on improving the scalability and energy efficiency of blockchain and IoT systems in e-commerce, particularly as transaction volumes increase. Exploring the integration of artificial intelligence and machine learning to predict and prevent fraudulent activities in real-time could further enhance the system's effectiveness. Additionally, investigating the potential for establishing standardized frameworks for blockchain-based financial reporting and legal enforceability will help mitigate current regulatory challenges. Future work should also aim at developing frameworks for the seamless integration of blockchain and IoT with existing e-commerce infrastructures to ensure widespread adoption and efficient operation.

References

[1] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, “Blockchain Based Data Integrity Service Framework for IoT Data,” in *2017 IEEE International Conference on Web Services (ICWS)*, Honolulu, HI, USA: IEEE, Jun. 2017, pp. 468–475. doi: 10.1109/ICWS.2017.54.

[2] Raj, G., M. Thanjaivadivel, M. Viswanathan, and N. Bindhu. "Efficient sensing of data when aggregated with integrity and authenticity." Indian J. Sci. Technol 9, no. 3 (2016).

[3] M. Samaniego, U. Jamsrandorj, and R. Deters, “Blockchain as a Service for IoT,” in *2016 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)*, Chengdu: IEEE, Dec. 2016, pp. 433–436. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102.

[4] N. Abdullah, A. Hakansson, and E. Moradian, “Blockchain based approach to enhance big data authentication in distributed environment,” in *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, Milan: IEEE, Jul. 2017, pp. 887–892. doi: 10.1109/ICUFN.2017.7993927.

[5] T. Yang *et al.*, “Applying blockchain technology to decentralized operation in future energy internet,” in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, Beijing: IEEE, Nov. 2017, pp. 1–5. doi: 10.1109/EI2.2017.8244418.

[6] S. K. Lo, X. Xu, Y. K. Chiam, and Q. Lu, “Evaluating Suitability of Applying Blockchain,” in *2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS)*, Fukuoka: IEEE, Nov. 2017, pp. 158–161. doi: 10.1109/ICECCS.2017.26.

[7] F. Imbault, M. Swiatek, R. De Beaufort, and R. Plana, “The green blockchain: Managing decentralized energy production and consumption,” in *2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*, Milan, Italy: IEEE, Jun. 2017, pp. 1–5. doi: 10.1109/EEEIC.2017.7977613.

[8] G. Zyskind, O. Nathan, and A. “Sandy” Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” in *2015 IEEE Security and Privacy Workshops*, San Jose, CA: IEEE, May 2015, pp. 180–184. doi: 10.1109/SPW.2015.27.

[9] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, “MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data,” in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, vol. 10658, G. Wang, M. Atiquzzaman, Z. Yan, and K.-K. R. Choo, Eds., in

Lecture Notes in Computer Science, vol. 10658. , Cham: Springer International Publishing, 2017, pp. 534–543. doi: 10.1007/978-3-319-72395-2_49.
[10] Y.-P. Lin *et al.*, "Blockchain: The Evolutionary Next Step for ICT E-Agriculture," *Environments*, vol. 4, no. 3, p. 50, Jul. 2017, doi: 10.3390/environments4030050.
[11] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 4, pp. 983–994, Jul. 2017, doi: 10.1007/s12083-016-0456-1.
[12] B. Scott, J. Loonam, and V. Kumar, "Exploring the rise of blockchain technology: Towards distributed collaborative organizations," *Strategic Change*, vol. 26, no. 5, pp. 423–428, Sep. 2017, doi: 10.1002/jsc.2142.
[13] V. Shermin, "Disrupting governance with blockchains and smart contracts," *Strategic Change*, vol. 26, no. 5, pp. 499–509, Sep. 2017, doi: 10.1002/jsc.2150.
[14] D. Folkinshteyn and M. Lennon, "Braving Bitcoin: A technology acceptance model (TAM) analysis," *Journal of Information Technology Case and Application Research*, vol. 18, no. 4, pp. 220–249, Oct. 2016, doi: 10.1080/15228053.2016.1275242.
[15] E. Mik, "Smart contracts: terminology, technical limitations and real world complexity," *Law, Innovation and Technology*, vol. 9, no. 2, pp. 269–300, Jul. 2017, doi: 10.1080/17579961.2017.1378468.
[16] B. S. Tan and K. Y. Low, "Bitcoin – Its Economics for Financial Reporting," *Australian Accounting Review*, vol. 27, no. 2, pp. 220–227, Jun. 2017, doi: 10.1111/auar.12167.
[17] I. Purdon and E. Erturk, "Perspectives of Blockchain Technology, its Relation to the Cloud and its Potential Role in Computer Science Education," *Eng. Technol. Appl. Sci. Res.*, vol. 7, no. 6, pp. 2340–2344, Dec. 2017, doi: 10.48084/etasr.1629.
[18] L. Orsolini, D. Papanti, J. Corkery, and F. Schifano, "An insight into the deep web; why it matters for addiction psychiatry?," *Human Psychopharmacology*, vol. 32, no. 3, p. e2573, May 2017, doi: 10.1002/hup.2573.
[19] J. Zou, Y. Wang, and M. A. Orgun, "A Dispute Arbitration Protocol Based on a Peer-to-Peer Service Contract Management Scheme," in *2016 IEEE International Conference on Web Services (ICWS)*, San Francisco, CA, USA: IEEE, Jun. 2016, pp. 41–48. doi: 10.1109/ICWS.2016.15.
[20] M. Conoscenti, A. Vetro, and J. C. De Martin, "Peer to Peer for Privacy and Decentralization in the Internet of Things," in *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, Buenos Aires, Argentina: IEEE, May 2017, pp. 288–290. doi: 10.1109/ICSE-C.2017.60.