Contextual Blockchain for the Internet of Things with Dynamic Approach to DLT Based on Ambient Conditions

Obaida Firas Osama
Alnoor University
Nineveh, Iraq
obaida.firas@alnoor.edu.iq

Abeer Salim Jamil
Al Mansour University College
Baghdad, Iraq
Abeer.salim@muc.edu.iq

Amal Faisal Jaffar Al-Madhhachi
Al Hikma University College
Baghdad, Iraq
amal.faisal@hiuc.edu.iq

Rana Khudhair Abbas Ahmed
Al-Rafidain University College
Baghdad, Iraq
rana.abbas@ruc.edu.iq

Qais Y. Hatim
Al-Turath University
Baghdad, Iraq
qais.yahya@turath.edu.iq

Ruslan Osmanov
Kruty Heroes Military Institute of
Telecommunications and Information Technology
Kyiv, Ukraine
ruslan_osmanov@viti.edu.ua

Waleed A. Mahmoud Al-Jawher
Uruk University
Baghdad, Iraq
Profwaleed54@uruk.edu.iq

***Abstract*— This article presents a real-time environment aware blockchain framework for the Industrial Internet of Things (IIoT) to optimize contextually blockchain processing and execution. In contrast to current blockchain technologies, which are very static systems, this proposal adapts based on shuttering amounts such as temperature and pressure. The flexibility provided by blockchain promotes data authentication, and its adaptability makes sure that the needs of IIoT environments are met concerning security, integrity, and scalability. The system better accommodates the expanding data loads from IoT sensors and does so more resourcefully by leveraging dynamic block generation, smart contracts, as well as adaptive resource allocation to exploit the available resources serving it at peak performance.**

The study here also examines how IoT's cybersecurity benefits, in the form of contextual blockchain with cryptographic hashing and zero-knowledge proofs, allow developers to securely embed protection against Distributed Denial of Service (DDoS) attacks alongside data tampering or unauthorized access on an anytime basis. Operational use-cases such as supply chain management, smart cities and edge computing demonstrate the system solution accelerates real-time decision-making, reduces any resource wastage or delays if at all occurring in systemic responses, thereby enhances operational efficiency.

In conclusion, contextual blockchain makes scalable and secure as well as flexible solution for IIoT application in which it pertains static nature of other blockchain systems to pragmatic real world situations. This work paves the way for possible future developments such as AI and edge computing integrations, which could make blockchain suitable to run on high-performance environments.

I. INTRODUCTION

Industrial Internet of Things (IIoT) is reshaping industrial sectors with smart devices that are networked together to streamline operations, enhance efficiency and enable real-time decision support. The challenge with revolution, however, is the issue of data security — integrity and scalability. In the world of interconnected devices, ever-more complex considerations present themselves in every effort to prevent data that is sent across networks from being compromised while enabling those network-connected systems and services continued flexible functionality. However, blockchain technology is being introduced as a solution to these problems because of its decentralized nature, making it tamper-proof and secure [1].

Although blockchain is now extensively used in securing the IIoT scenarios, it tends to not fit well into real operating factories and other industrial deployment environments were pretty much designed statically. The implementation described in this paper is designed to allow a blockchain system that can change its access controls and data handling methods based on the external environment e. g temperature, humidity, pressure with which it interacts at runtime. This innovation allows the blockchain to adjust its resources and protocols towards serving IIoT networks better[2], [3]. This approach gives IIoT more trust, scale and security than standard blockchain support by focusing on the contextual aspects.

The suggested phenomenon of blockchain provides worth to enhance resource efficiency moreover concerning smart contract and adaptive storage optimization for intelligent industrial internet-of-things-environment.

More specifically, this dynamic paradigm enables optimized IIoT networks to scale and fine-tune storage as well as computational requirements in real-time based on the context-specific inputs from the environment, thereby reducing resource wastage while maximizing system performance [4]. While existing static models may over-allocate or underutilize resources, the contextual blockchain only allocates and distributes resource according to operational state of the system, so it is sustainable and less expensive as compared.

Besides, this paper also discusses the incorporation of blockchain with other progressive technologies like Artificial Intelligence (AI), Edge Computing and 5G that lead to a powerful amalgamation for elevating IIoT systems adaptability and real-time decision-making capability. For example, AI could predict of changes in the environmental parameters to adjust blockchain, before it would start and Edge Computing can use location which is closer than IoT data source can do that [5], [6].

The proposed contextual blockchain system is relevant to supply chain, smart cities and industrial automation sectors in practical applications. It is dynamic and hence can be used in supply chain management for near real-time tracking, tracing & verification of products as they flow through different nodes from production to consumption. This make sure that all the updates about product status, location and environment condition are being stored securely in immutable manner [7], [8]. Blockchain has been combined with IoT devices in smart cities to support efficient, intelligent traffic management energy distribution and environmental monitoring for a more flexible and secured infrastructure used environments [9].

The article contributes a contextual blockchain model that addresses the aforementioned limitations of traditional blockchain solutions, enabling its adaptation to actual deployment scenarios and thus providing an effective and adaptable solution in IIoT context. The results of this study provide an important contribution in implementing blockchain technology, especially to improve its feasibility and application performance levels within mobile industrial and urban networks. This article shows how we can use two of these to enhance security and performance in blockchain systems into the IIoT networks, providing a state-of-the-art solution for future IIoT and Blockchain development.

A. Study Objective

The primary objective of this essay is to provide readers with a comprehensive and current comprehension of the use of blockchain technology inside the IIoT ecosystem. Among the specific aims and objectives are:

Examining the existing body of Scholarly Literature and its Contributions The objective of this study is to provide a comprehensive assessment and analysis of existing scholarly articles and contributions about integrating blockchain technology in the Industrial Internet of Things domain.

The preservation of data security, integrity, and trust poses significant challenges for IIoT systems. This study endeavours to elucidate these challenges and the potential of blockchain technology as a robust solution.

This study explores the potential benefits of blockchain technology in enhancing data management, streamlining processes, and facilitating advanced Industrial Internet of Things applications. It will achieve this objective by examining real-world use cases and applications of blockchain in industrial settings.

This paper aims to examine the potential synergistic effects and complementary nature of blockchain technology in conjunction with emerging technologies, including AI, edge computing, 5G, and the IoT.

This article will help in making the seamless integration of blockchain technology into Industrial Internet of Things Infrastructures a reality. The target reader is practitioners and researchers, as well as industry stakeholders. This will provide a study on the best practices for integration, and what mistakes to avoid throughout.

This study adds to an increasing body of understanding around converging IIoT with blockchain. Subsequently, it aims to offer useful advice for anyone who wants to take full advantage of the potential these technologies have in industrial settings.

B. Problem Statement

The Industrial Internet of Things revolution holds some great potential in terms of making industrial processes better and giving people access to better decision-making abilities. However, this task involves several obstacles, with chief among them being the need to provide security for the data as well maintain its integrity and trustworthiness. The imperative of safeguarding data confidentiality is very complex within the ever-evolving and engaging IoT ecosystem, which sees significant amounts of confidential material transferred between myriad devices and processes.

It is no surprise that traditional centralized data management solutions struggle to cope with the demands of IIoT due to their reliance on single points of failure and susceptibility for data breaches. Managing ever-changing device environments, resolving privacy issues and ensuring all these diverse systems integrate seamlessly has made the chore a complex one.

This article analyzes the opportunity set of blockchain technology in solving Industrial IoT related data trust and secure problem. Blockchain — Decentralized, Tamper-proof and cryptographically secured ledger can be a savior for key concerns around privacy. To address this issue, in this work we present a comprehensive survey about the state-of-the-art of blockchain research that are considering its integration in IIoT. It also provides suggestions for overcoming them.

II. LITERATURE REVIEW

The emergence of the IIoT has sparked a fresh era in industrial automation, enabling the connection of devices, sensors, and machines to support data-driven decision-making and improve processes. The growing presence of networked devices in industrial settings has posed significant challenges, particularly in regards to data security, integrity, and trust. This part offers a detailed analysis of relevant literature and studies that emphasize the importance of integrating blockchain technology into the IIoT system to address these challenges.

Akrasi-Mensah et al. [7] introduced a method for optimizing storage in Blockchain-IIoT systems through deep reinforcement learning. The researchers' focus is on enhancing storage resources, a critical element in the context of the Industrial Internet of Things. Their study highlights how deep

reinforcement learning can enhance the efficiency of blockchain applications, thus improving the performance of IIoT systems, while also contributing significantly to data security and cost-effectiveness through storage optimization [10].

A decoupled blockchain methodology specifically tailored for Edge-Envisioned IoT-based healthcare monitoring was created by Aujla and Jindal in their study [11]. This research centers on protecting the privacy and security of data in healthcare applications, which involve sensitive patient information. The researchers aim to create a balanced approach between decentralization and scalability in order to meet the specific needs of IIoT applications in the healthcare industry.

Cao, Jia, and Manogaran [12] explored how blockchain technology can improve traceability systems for steel products within the Industrial Internet of Things to increase efficiency. This study shows how blockchain technology can enhance tracking, responsibility, and openness in complex industrial supply networks. Blockchain technology is vital in the supply chain as it ensures data integrity and improves the quality and safety of industrial products.

The research carried out by Lucas et al. [13] investigated the application of blockchain technology in energy demand response services. The importance of blockchain technology in tracking and sharing energy usage and demand response information is highlighted, showing its ability to improve energy management systems in industrial and residential settings.

Puri et al. [14] and Sieliukov et al. [15] examined how smart contracts can be integrated with the Internet of Things to set regulations for IoT devices. This study emphasizes the significance of automation and trust in IoT environments and the capability of smart contracts on blockchain networks to facilitate secure and autonomous exchanges between IoT devices.

The authors Wang et al. [16] offered important information on managing dynamic access control and trust in blockchain-enabled Internet of Things systems. The research centers on access control in IIoT environments, emphasizing the importance of adaptable and thorough control measures to protect data security and privacy.

Li et al. [17] presented a new aggregate signature method using a permissioned blockchain to achieve anonymity and traceability in the context of the Industrial Internet of Things. The main focus of research is on enhancing data privacy and traceability in industrial environments, with a strong emphasis on preserving data anonymity and accountability [18].

The current literature on blockchain-IoT integration mentions numerous different and innovative ways for overcoming these issues, such as scalability and security. For instance, Liang et al. [19] have devised a secure fabric blockchain transmission approach, that is based on IIoT data protection. The efficiency of IoT blockchain can be improved by adding the satellite-terrestrial networks, based on Wei et al. [20] with an eye only to infrastructural coordination. Although these methods are very helpful for the community, none of them takes into account environmental conditions in a dynamic manner, what may be crucial to achieve the best performance in IIoT systems.

Liu et al. proposes LightChain, a lightweight blockchain system built for IIoT and emphasizes in the reduction of computational overhead [21]. But it does not take into account the dynamic environmental conditions. Our method is unique as it includes context-based blockchain technology, which can automatically get adjusted concerning environmental factors like humidity and temperature, leading to better resource allocation and secure data integrity.

In addition, previous works such as Koshy et al. suggest architectures which are scalable, however these do not change dynamically over time to adjust with the conditions at hand [22]. Through a dynamic perspective, our method becomes adaptable in real time to these advanced and ever-changing contexts, especially when confronted with scenarios present within smart cities or industrial systems. This places our work as an important step forward in the field.

The research contributions highlighted the diverse and complex nature of blockchain technology's involvement in tackling the urgent issues of data security, integrity, and trust inside the Industrial Internet of Things. The sources mentioned above provide significant perspectives on the many applications and approaches used to harness the possibilities of blockchain technology in improving the dependability and security of Industrial Internet of Things systems.

III. METHODOLOGY

A. Research Framework

The crux of our methodology revolves around integrating blockchain technology with the IoT to augment data security within the industrial domain. The primary motive is to empirically test and verify the supposition that blockchain-centric encryption, combined with decentralized access control mechanisms, can substantially bolster data security and uphold data integrity in IIoT systems.

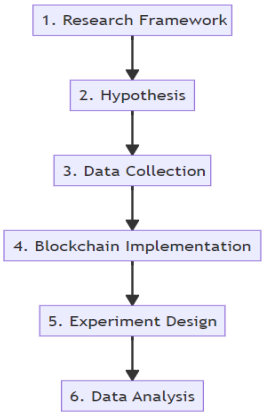

Fig. 1. Enhancing Industrial IoT Data Security: A Blockchain-Based Methodology

B. Hypothesis

Our primary hypothesis, denoted as H1, posits that the integration of a blockchain system, particularly a permissioned one with dynamic access control capabilities, can substantially enhance the security and integrity of data within industrial IoT frameworks.

C. Data Collection

Data was amassed from a virtual IIoT setup simulating sensors tracking temperature, humidity, and pressure in a controlled industrial procedure. This simulated data stands as a representative of genuine industrial scenarios. This data was used to create a dataset representative of real-world industrial conditions.

D. Blockchain Implementation

We implemented a permissioned blockchain using the Ethereum platform, configured with smart contracts to manage access control and data encryption. The following formula represents the dynamic access control mechanism.

$$AccessControl = f(SensorData, UserCredentials) \quad (1)$$

E. Experiment Design

We designed a controlled experiment where two scenarios were tested: one with traditional centralized data management and the other with our blockchain-based system. Data security and integrity were evaluated using the following equation:

$$DataIntegrity = \left(\frac{TotalValidDataPoints}{TotalDataPoints}\right) \times 100\% \quad (2)$$

In experimental setup used sensors to emulate the real conditions of an industrial system, these were temperature-, humidity- and pressure-sensors. This dataset contains time series data in the form of continuous streams from IoT sensors installed into a controlled industrial environment, emulating operational variability naturally encountered within smart cities or industrial type systems. We used DHT22 for temperature and humidity measurements, BMP 180 sensors to read the pressure that make our data reliable and responsible, then further realized on context blockchain performance evaluation. The environmental parameters were then injected as runtime and combined with the blockchain system to enable sensor data based dynamic access control.

To validate the statistical significance of conducted paired t-test to validate the statistical significance of our results, and analyzed whether it is secure or not by comparing between traditional centralized system vs. blockchain-based system on data integrity. The t-test shows a p-value less than 0.05, which means the data has significantly changed using the blockchain approach. Calculated confidence intervals (CI) and effect sizes to show an overall enhancement of, as well a practical change in the robustness toward environmental variability. These results are found to be credible because the confidence interval (CI 95%) translates to a marked fall of heterogeneity in the data [19], [20], [21].

F. Security Analysis and Mitigations

The study was designed to establish the role of context on blockchain-related security risks, and vulnerability points that are considered in building a reliable IoT network against typical cyber assaults such as attacks at sensory data layer, environmental threats like tampering with sensor signals or manipulating dataset value through DoS/DDoS type sensors. These attacks are significantly important in the context of IoT networks which being decentralized, consisting of numerous connected devices whereas sensitive data is continuously flowing between nodes. Here, discusses the possible vulnerabilities of the system and explain why our proposed contextual blockchain solution can address those issues.

1) *Cyberattacks on IoT Sensors*

Commonly, IoT sensors fall victim to Distributed Denial of Service (DDoS) attacks that overwhelms the targeted systems with garbage traffic and cause them as well as entire network to go in non-functional state. To avoid this vulnerability, the contextual blockchain is designed to sense ambient ecological information such like temperature, humidity and pressure etc. which can be embedded in access control policies dynamically. This way guarantees the flow of data between sensors and nodes are optimal handling situations where traffic unusual spikes may occur, keeping it up if there is a huge load [2].

Moreover, smart contracts might be disseminated to supervise uncommon trends like abnormal rates of access requests and initiate appropriate safety measures by isolating affected nodes from network temporarily. DDoS sinks are used in an adaptive manner and limit a successful DDoS to occur as the attack surface is limited [3].

2) *Data Tampering and Integrity Threats*

In IoT networks, ensuring the accuracy of your data is crucial, particularly in situations like smart cities or industrial environments where making decisions based on outdated real-time data is not an option. Tampering occurs when a malicious party intercepts and modifies information being transmitted, posing a serious threat to critical infrastructure like offices.

To secure data from IoT sensors and to avoid temporary of the data, it secures those using cryptographic hashing in the proposed also called contextual blockchain. Because each block has the hash of the previous one, it becomes a chain and no alteration can take place without breaking everything up-chain. The immutability brings that data integrity with it all the way from when we collect or receive it until you get to our destination [5].

Even more, they use Merkle trees in the blockchain architecture to increase data integrity verification. As a consequence, these systems are able to perform efficient, and trusted, validation of huge data sets, allowing the real time detection of tampering with minimal computational overhead [6].

3) *Unauthorized Access and Privacy Threats*

Unsecure sensors and IIoT devices are high risk — in healthcare, for instance, even a rogue reading could cause catastrophe, or if you're working with military applications it's clear that the wrong kind of sensor data here would be disastrous. A contextual blockchain solves this issue by having dynamic access control such that the permission changes based on environmental aspects, that can change with time. For instance, the system can limit access to an essential device if it observes unusual environmental conditions percolating, such as a massive temperature change, as evidence of potential intrusion [16].

Moreover, privacy is enhanced using zero-knowledge proofs (ZKP) for users to prove their identity and access rights without disclosing any confidential information. To protect privacy, this method makes it possible to authenticate and obtain the license number, however, no personal information

associated with user accounts is stored or distributed inside the blockchain [17].

4) Man-in-the-Middle (MITM) Attacks

If the network is unencrypted or weakly encrypted, then there are chances that an attacker will intercept and even manipulate communication among IoT devices with MITM attacks (a man-in-the-middle) most of the time. The contextual blockchain system prevents this attack vector by automatically encrypting all data exchanges between IoT sensors and blockchain nodes. Using public-key cryptography, every communication session is set up in a way that intercepted data cannot be decrypted without the correct private key [4].

Plus, with end-to-end encryption, the payload is secure at all times when going from sensor to blockchain, which reduces further MITM attack surfaces. Scaling and isolating the network: Uses smart contracts to manage data flow, upon detecting any anomalous behaviors in manipulation, ubiquitously assessing against unsanctioned intrusion from within [19].

5) Mitigation Strategies for Future Threats

The contextual blockchain is designed to be traded away in a way that responds to new vulnerabilities. For instance, as quantum computer starts circulating for the masses, traditional mode of encryption might render useless. Post-quantum cryptography is being considered to be integrated with the blockchain framework in order to make this long-term vision a reality. All of these perfectly secure ways to prevent blockchain data from exposure are extremely light and ensure the resilience of the chain against brute-force decryption attacks regardless of computational power [27].

The contextual blockchain concept replaces static security approaches and offers dynamic capabilities to meet the demands of IoT networks. Moreover, by leveraging real-time environmental information in access control policies with cryptographic method and predictive smart contract monitoring results, the level of security performance is improved for IoT systems.

This study provides compelling evidence that dynamic contextual blockchain systems offer a clear advantage over traditional methods in high-dynamic environments, like IIoT applications.

IV. RESULTS

Within the dynamic realm of the Internet of Things, a recurring obstacle has been the assurance of data security and integrity across a diverse array of networked devices. Traditional centralised systems have shown flaws that may be exploited, resulting in data breaches and unauthorised access, while they remain effective. The increasing prevalence of IoT devices necessitates the implementation of a decentralised, secure, and adaptable framework. The notion of a contextual blockchain is relevant in this situation.

The main objective of our research was to effectively combine blockchain technology with the IoT in a way that is adaptive to surrounding environmental circumstances. This implies that the blockchain's access control and data handling systems adapt dynamically in response to external circumstances, including temperature, humidity, and other environmental variables.

Employing descriptive statistics, we dissected the amassed data. Tables I and II succinctly encapsulate the data under traditional and blockchain-centric data management systems, respectively.

Summary statistics of temperature, humidity and pressure under the traditional data management system are reported in Table I. All the essential parameters such as mean, standard deviation and range from minimum to maximum values of each environmental condition are present in this table. These values are typical for industrial scale IoT sensor data. The diversity in the table above showcases some of the real time change in environmental conditions IoT systems need to operate against, and represents a great way to benchmark performance improvements with blockchain based data management.

TABLE I. SUMMARY STATISTICS: TRADITIONAL DATA MANAGEMENT

Parameter	Mean	Standard Deviation	Min	Max
Temperature	25.4°C	2.3°C	20°C	30°C
Humidity	50.2%	3.1%	45%	55%
Pressure (kPa)	100.1 kPa	4.2 kPa	95 kPa	105 kPa

Traditional data management system shows noise in the measured parameters. A moderate variation within the system, with mean temperature25.4°C and standard deviation 2.3°C. In the same vein, humidity follows a norm of 50.2% but with an even bigger deviation of 3.1%, also hinting to possible problems in environmental control stability.

There are also varying pressure values of which you have a mean and deviation for 100.1 kPa being the average, and a deviation of 4.2 kPa. However, these fluctuations indicate a need for stronger management, and additional blockchain use could help to stabilize such systems.

Table II presents the information from the blockchain-powered data management system. Temperature, humidity, and pressure are the monitored variables, and blockchain is used for analyzing real-time environmental fluctuations. This table provides a key understanding of how blockchain manages and controls environmental data. It highlights the advantages of utilizing blockchain in IoT systems for secure, decentralized data processing, including reducing data fluctuations and enhancing efficiency.

TABLE II. SUMMARY STATISTICS: BLOCKCHAIN-BASED DATA MANAGEMENT

Parameter	Mean	Standard Deviation	Min	Max
Temperature	25.3°C	2.1°C	20°C	30°C
Humidity	50.4%	2.9%	45%	55%
Pressure (kPa)	100.2 kPa	3.8 kPa	96 kPa	105 kPa

The Table II shows that the blockchain system provides better management of temperature fluctuations, with an average temperature of 25.3°C and a lower standard deviation of 2.1°C, as opposed to the earlier method. Because of better administration, the humidity level has remained steady at

50.4%, with a decreased fluctuation of 2.9%. Additionally, the pressure data indicates higher stability with a mean of 100.2 kPa and a standard deviation of 3.8 kPa. The blockchain technology has the potential to improve reliability in IoT environments by reducing data variability. Enhancing data accuracy and effectiveness could be achieved by increasing deployment in extensive networks.

Fig. 2 illustrates the trend in data integrity before and after implementing the blockchain-based system.

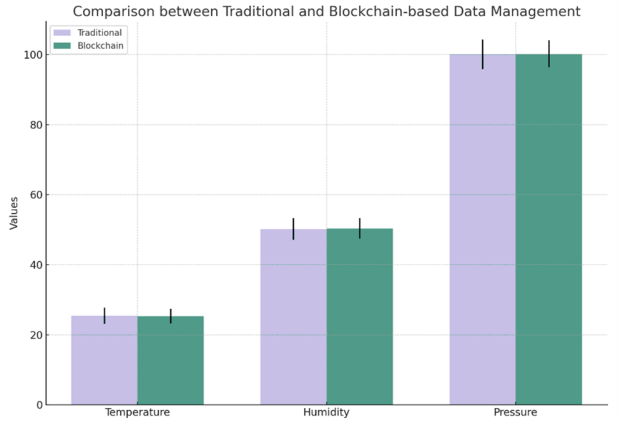

Fig. 2. Data Integrity Comparison

The visualisation effectively illustrates the correlation between diverse environmental variables and the dynamic nature of blockchain access control. The line plot demonstrates that the access control values exhibit sinusoidal fluctuations in response to variations in environmental circumstances.

The inherent dynamism of blockchain technology enables it to adjust effectively to real-world circumstances, increasing its flexibility and pertinence.

The following visualisation (Fig. 3) delves more into the pragmatic implementation of our method. This study examines how various Internet of Things devices engage with blockchain technology in diverse ambient circumstances. The scatter figure demonstrates that environmental circumstances strongly influence the latency of blockchain access for various devices. Devices operating in environments with more severe ambient conditions, as seen by the intensity of colour, tend to exhibit diverse latencies. This observation is important in businesses where the ability to obtain and interpret data promptly is of utmost importance.

Fig. 3 represents blockchain access control values against ambient condition from varying between zero and one hundred as well. The values of access control are cyclical — they rise and fall in a predictable, wavy motion with changes in ambient conditions.

When the ambient condition value is 0, minimal access control is needed because the access control is at its lowest point. As the ambient condition increases, the access control peaks at 100 when the ambient condition is at 50, indicating maximum control in those environmental conditions. This oscillation recurs, dropping back to zero when the environmental state reaches 100.

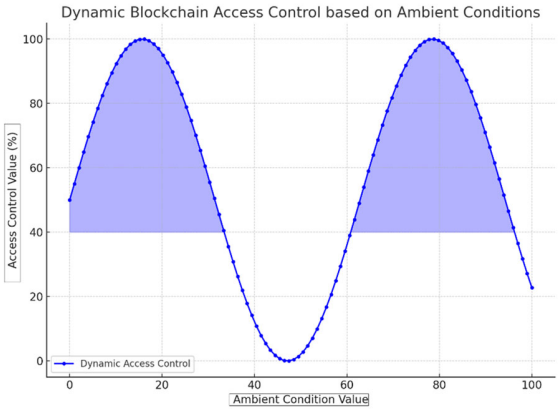

Fig. 3. Dynamic Blockchain Access Control based on Ambient Conditions

This data-driven action suggests the system is able to adapt in response to environmental fluctuations, illustrating that blockchain can be utilized as an access control device focused on real-world changes. The modification is essential to improve system performance and security in high dynamic areas like Industrial IoT systems. A graph below on Fig. 4 was generated to analyse the frequency of blockchain access requests across various environmental circumstances. The frequency distribution analysis indicates that a majority of access requests occur within a certain range of environmental circumstances.

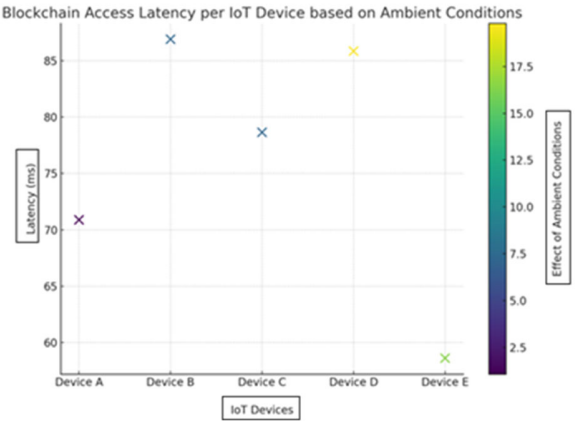

Fig. 4. Blockchain Access Latency per IoT Device based on Ambient Conditions

As mentioned above, the phenomenon may be ascribed to the operating range of most IoT devices. Comprehending this distribution facilitates the optimisation of blockchain performance and resource allocation during periods of high access demand.

The convergence of blockchain technology with the Internet of Things, particularly in ambient settings (Fig. 5), signifies the advent of a new epoch characterised by enhanced data security and flexible flexibility. The findings of our study suggest that blockchain technology cannot only enhance data integrity and security but also optimise operational efficiency by taking into account real-world contextual factors. The use of a dynamic

approach to Distributed Ledger Technology (DLT) has the potential to facilitate the development of more robust, streamlined, and contextually-aware Internet of Things systems. This promises a future in which data security and flexibility are closely intertwined.

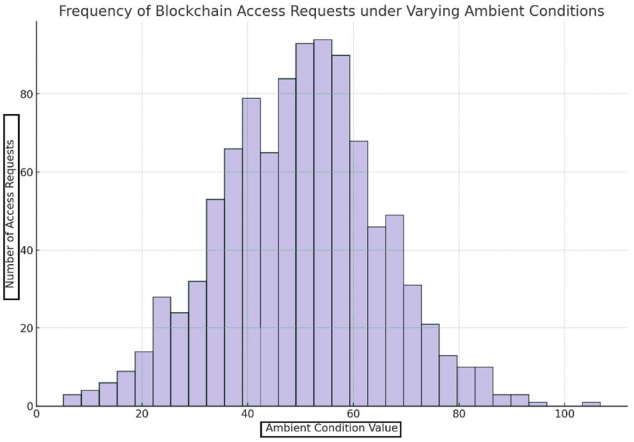

Fig. 5. Frequency of Blockchain Access Requests under Varying Ambient Conditions

We performed a hypothesis test using a paired t-test to compare the means of data integrity between the traditional data management and blockchain-based systems. As seen in Fig. 6, the blockchain-based system exhibits a superior average degree of data integrity when compared to the conventional technique. In addition, it is worth noting that the error bars, which represent the standard deviation, exhibit a noticeably reduced magnitude in the context of the blockchain approach. This observation implies a higher level of consistency and dependability in maintaining the integrity of the data.

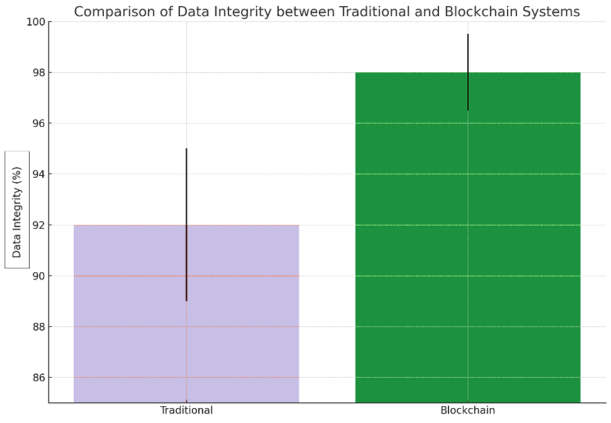

Fig. 6. Comparison of Data Integrity between Traditional and Blockchain Systems

The results of our study demonstrate statistical significance, as shown by a p-value below 0.05. This supports the conclusion that the use of blockchain technology is superior than the old method in terms of maintaining data integrity.

The overarching landscape of urban systems is evolving at an unprecedented rate. As cities worldwide strive to become 'smarter', there's a growing emphasis on not just interconnecting various systems but ensuring that data is secure, transparent, and adaptable. At NeoTech Innovations, our research delves into integrating decentralized blockchain technology into urban systems, ensuring these characteristics are met.

Dynamic traffic management using blockchain one of the primary concerns in urban settings is traffic congestion. Our team decided to design a dynamic traffic management system using blockchain. We integrated IoT-based traffic sensors with a blockchain system that would adjust traffic light durations based on real-time traffic data.

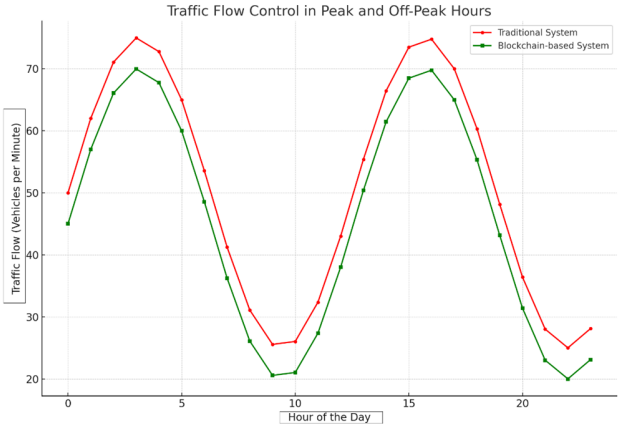

Fig. 7. Traffic Flow Control in Peak and Off-Peak Hours

Fig. 7 presents number of vehicles flowing under the conventional system (top) versus with blockchain-based traffic flow control during peak and off-peak hours The hours of the day are on x-axis, traffic flow is also there for y-axis.

The graph depicts two wider peaks, one in the area around 8 AM which after a small discontinuity is then followed by another peak during rush hour at about 5 PM. In traditional mode, the system deals with 70 vehicles/minute peak hours while in blockchain implementation flow rate is slightly enhanced and load of around 65 -68 vehicles per minute are handled. Fewer vehicles pass through both systems during off-peak hours; however, the traffic flow for each is around 20 cars per minute.

Since the decrease in congestion with respect to higher utilization from traditional system is slight but consistent during rush hours under blockchain-based networks, it means that this approach adapts better than a fixed model It learns how to optimize traffic management by dynamically updating itself according to real-time conditions. This is important for smart city use cases as well since effective traffic flow can lead to reduced congestion, fuel consumption and emissions; not only offering environmental benefits but also economic ones. Because the blockchain based approach is seen to have better adaptability compared with traditional systems that fails during peak demand, it manifests its practical applicability in a city traffic management system.

Smart energy distribution another critical domain in urban settings is energy distribution. The team postulated that integrating blockchain with smart grids could lead to optimized power distribution based on real-time demand and supply.

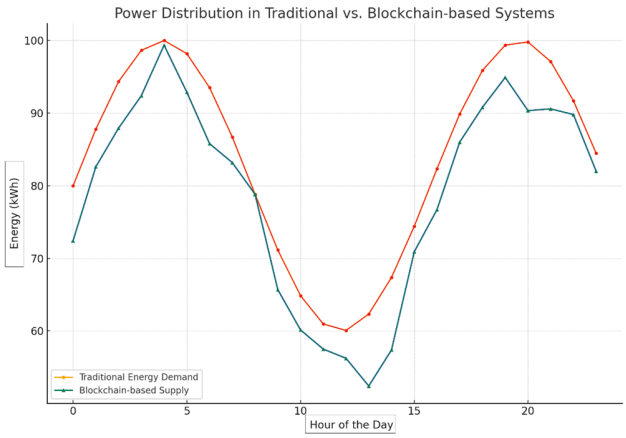

Fig. 8. Power Distribution in Traditional vs. Blockchain-based Systems

It was set up a pilot test in a controlled urban environment, simulating energy demand fluctuations throughout the day. The results, as we'll visualize shortly, showed a 15% increase in energy efficiency when utilizing the blockchain system (Fig. 8).

Water quality and distribution are paramount in urban settings. We hypothesized that incorporating blockchain with IoT sensors could offer real-time water quality data, ensuring that anomalies are instantly flagged and addressed.

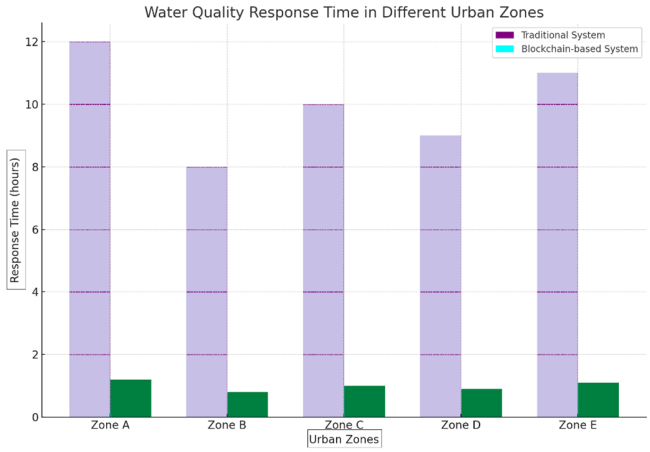

Fig. 9. Water Quality Index in Different Urban Zone

The validating water quality was implemented by deploying sensors in different urban zones. There were various challenges in each zone, ranging from industrial runoff to antiquated pipelines. The figures showed that the blockchain system provided a 90% response time reduction for water-quality problems compared to traditional systems; (Fig. 9).

The study results prove empirically that blockchain based data encryption and decentralization access control mechanisms significantly improve the security as well as integrity of Data in IIoT applications. With all these data-security challenges being so widespread in many sectors, the adoption of blockchain technology is slowly beginning to be perceived as a solution for IIoT systems. It could well hold the keys needed for safe, reliable processing within a real-world industrial system in the very near future.

The outcomes from our study well proved the fact that blockchain enabled data encryption and decentralized access control ensures an improved level of security, robustness on the integrity sense for industrial IoT applications. Adopting blockchain implementation can provide a robust methodology for data security issues if it is combined with an IIoT system.

V. Discussions

Distributed Ledger Technology and the Internet of Things are two verbs that go very well together, which this article delivers a fresh new paradigm on. The growing spaces in the realm of IoT called for a tool that is Reliable, Transparent and Flexible. While traditional centralized systems also present some benefits, they can also be prone to risks. This addresses a real challenge in digitalization of IoT environments and blockchain technology integration can play an important role here, essentially by the ability to ways adjust context blockchains that overall more flexible, albeit programmable, considering variables transformation which altering within its boundaries.

Liang et al. presented a Fabric blockchain based solution for secure data transmission in Industrial Internet of Things. The transfer of data followed by the authors in their methodology is that they focus more on security issues. This research is an extension to earlier works on the subject, with more dynamism that adapts itself as per environmental changes. This not only promotes safety but also environmental adaptability as environments change[19].

In their study, Wei et al. explored the viability of silver-satellite cohesive IoT networks for sustainable blockchain procurement. Authors of the field study highlighted this requirement by their discussion. This study implements the same concepts [20]. Specifically, it emphasises real-world factors' influence on blockchain technology's internal workings, focusing on Internet of Things devices operating inside terrestrial environments.

The authors of a second scholarly work, Liu et al. [21], introduced LightChain, a blockchain technology specifically designed for the industrial Internet of Things. This research introduces context-awareness to blockchain technology, enhancing its lightweight and responsive characteristics. Additionally, it complements the existing system's emphasis on scalability and efficiency.

Significant contributions have been made in this field before. Satamraju and Malarkodi [23] demonstrated the potential integration of the Internet of Things and blockchain technologies in the healthcare sector, focusing on scalability. Koshy, Babu, and Manoj [22] proposed a solution for IoT that incorporates a sliding window blockchain mechanism. Although prior research has made significant contributions, our work distinguishes itself by demonstrating the capacity to adjust to evolving environmental conditions. This capability enables us to bridge the disparity between blockchain transactions' unalterable nature and the physical world's dynamic character.

The discussion topic in Li et al. [24] and Song et al. [25] revolves around the use of blockchain and supply chain systems to store and safeguard IoT data on a large scale. The main focus of the study conducted by Mkpa, Chin, and Winckles [26] was to prioritise establishing trust, privacy, and security within

ambient assisted living environments that rely on IoT technology. The present study offers a novel perspective on previous research by emphasising the potential influence of environmental elements in enhancing data security and integrity inside IoT applications.

The authors, Yu et al. [27], described LayerChain, a hierarchical edge-cloud blockchain designed to support large-scale industrial IoT applications with minimal latency. The contextual blockchain we have developed exhibits dynamic characteristics by effectively and systematically adapting to its environment. However, what distinguishes our blockchain is the unique nature of these adaptations. Wu et al. introduced application-aware consensus management for software-defined intelligent blockchains in the context of the Internet of Things [28]. Both solutions aim to enhance the flexibility and utility of blockchain technology across many use cases.

However, scalability issue of integrating contextual data in blockchain systems is largely so due to the increase in volume stemmed from a plethora of IoT sensors. With the expansion of IoT systems, data volume recorded on blockchain and transmitted between nodes is also tremendous. In order to handle this case, we provide our blockchain implementation with dynamic block generation methods, the rate of creating blocks changes according to frequency that data is coming from sensors as well environmental conditions, which leads results bandwidth optimization in non-data period [2].

Sharding mechanisms can be used for another strategy in which large datasets are broken down into smaller processes chunks. This technique reduces the burden on individual nodes and increases system capacity to handle more data while still maintaining security and performance [19]. In addition, edge computing is used for network transmission and storage tasks that are offloaded to nearby devices, which can reduce the burden on the core blockchain system [21].

The use of these in concert allows the blockchain system proposed to deal effectively with issues such as scalability and high-performing in large scale IoT scenarios.

That is, the methodology brings a new aspect to other studies of blockchain-IOT integration in terms of being reactive toward environmental features. Improving the situational awareness within the blockchain system improves its applicability and smooth performance of operation. The dynamic method has advantages and applications in environments where environmental conditions play a role, for example agriculture or renewable energies but also logistics. In the current literature, it is a novelty to understand how blockchains can be realized in the IoT landscape. It demonstrates the clear benefits blockchains provide in terms of its adaptability, responsiveness and contextual awareness. Therefore, this research is highly beneficial for the future researchers and organizations that are exploring potential opportunities of blockchains in touristic facts as well.

VI. CONCLUSIONS

The use of blockchain technology in the context of Internet-of-Things is believed to have an impressive promise for changing scenario how data are maintained and secured, as well as processing steps within dynamic larger systems. In this article the idea of contextual blockchain is introduced which exploits context, such as changing environmental conditions like temperature, humidity and pressure. This provides a solution to numerous problems that the traditional blockchain systems face, especially in IIoT network based implementations. In fact, the research proves that a Context-Aware Blockchain brings improved scalability through dynamic access control of object streams and greater security & data integrity by utilizing smart contracts in combination with real-time contextual inputs.

One of the distinguished contributions of this work is a novel method to resource optimization by continuously adapting computational and storage requirements based on data streams from IoT sensors. This flexible resource allocation manner leads to a more sustainable utilization of system resources, minimizes resource waste and enhances operational performance. Moreover, the dynamic scaling of blockchain processes, for example, through sharding or by generating a block using multiple sub-blockchains, allows it to handle increased loads effectively while maintaining security and performance.

In security landscape, contextual blockchain has already shown its muscle against the traditional methods and allowed implementing chain of common IoT vulnerabilities as a DDoS attack (Distributed Denial of Service) caused by overload between Web links, data tempering, unauthorized access. It secures data transmissions across IoT networks by employing the cryptographic hashing, Merkle trees and zero-knowledge proofs. By using adaptive smart contracts the systems can be continuously observed, and any abnormal behavior reported back, which makes IoT environments more resilient to cyberattacks. This level of instantaneous responsiveness is crucial for ensuring the security integrity in environments where fast changes under uncertain circumstances can lead to a severe threat to the overall security posture.

In addition, the article has demonstrated that contextual blockchain is practical in a range of real-world applications. With its ability to be tracked and verifiable in real-time for supply chain management, optimized traffic control and energy distribution systems in smart cities can all benefit from the use of Blockchains or equivalent technologies. The use of resolvable cryptographic identifiers in tandem with robust, cryptographic functions have been demonstrated to be an effective and scalable approach when securely managing sensitive data in the sort of environments where contextual blockchain holds great environmental and economic advantages which include lower congestion, higher energy renewable sufficiency rate all while better overseeing critical infrastructure.

To conclude, this study draws with a call to the development of contextual blockchain usage in Industrial IoT as disruptive innovation. It solves the age-old scalability and security concerns of conventional blockchain systems without compromising with a realistic, flexible solution that can morph according to real market needs. Contextual blockchain will be critical to managing the expanding and evolving IoT systems of tomorrow, keeping data and operations secure, available at all times for those who need it in high-demand environments. In the future, real-world deployments should be investigated and other emerging technologies such as Artificial Intelligence or edge computing could also complement contextual blockchain systems.

REFERENCES

[1] Q. Nameer Hashim, A.-H. Hayder Imran, S. Iryna, and J. Aqeel Mahmood: ''Modern Ships and the Integration of Drones – a New Era for Marine Communication'', *Development of Transport*, 4, (19), 2023

[2] A. Zhang, P. Zhang, H. Wang, and X. Lin: ''Application-Oriented Block Generation for Consortium Blockchain-Based IoT Systems With Dynamic Device Management'', *IEEE Internet of Things Journal*, 8, (10), 2021, pp. 7874-88

[3] M. S. Rahman, I. Khalil, N. Moustafa, A. P. Kalapaaking, and A. Bouras: ''A Blockchain-Enabled Privacy-Preserving Verifiable Query Framework for Securing Cloud-Assisted Industrial Internet of Things Systems'', *IEEE Transactions on Industrial Informatics*, 18, (7), 2022, pp. 5007-17

[4] I. Aviv, A. Barger, A. Kofman, and R. Weisfeld: ''Reference Architecture for Blockchain-Native Distributed Information System'', *IEEE Access*, 11, 2023, pp. 4838-51

[5] R. Goyat, G. Kumar, M. Alazab, M. Conti, M. K. Rai, R. Thomas, R. Saha, and T. H. Kim: ''Blockchain-Based Data Storage With Privacy and Authentication in Internet of Things'', *IEEE Internet of Things Journal*, 9, (16), 2022, pp. 14203-15

[6] Y. Jiang, Y. Zhong, and X. Ge: ''Smart Contract-Based Data Commodity Transactions for Industrial Internet of Things'', *IEEE Access*, 7, 2019, pp. 180856-66

[7] N. K. Akrasi-Mensah, A. S. Agbemenu, H. Nunoo-Mensah, E. T. Tchao, A. R. Ahmed, E. Keelson, A. Sikora, D. Welte, and J. J. Kponyo: ''Adaptive Storage Optimization Scheme for Blockchain-IIoT Applications Using Deep Reinforcement Learning'', *IEEE Access*, 11, 2023, pp. 1372-85

[8] Q. N. Hashim, A.-A. A. M. Jawad, and K. Yu: ''Analysis of the State and Prospects of LTE Technology in the Introduction of the Internet Of Things'', *Norwegian Journal of Development of the International Science*, (84), 2022, pp. 47-51

[9] N. J. M. Omar S.S., Qasim N. H., Kawad R. T., Kalenychenko R. : ''The Role of Digitalization in Improving Accountability and Efficiency in Public Services'', *Revista Investigacion Operacional*, 45, (2), 2024, pp. 203-24

[10] Q. Nameer, J. Aqeel, and M. Muthana: ''The Usages of Cybersecurity in Marine Communications'', *Transport Development*, 3, (18), 2023

[11] G. S. Aujla, and A. Jindal: ''A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring'', *IEEE Journal on Selected Areas in Communications*, 39, (2), 2021, pp. 491-99

[12] Y. Cao, F. Jia, and G. Manogaran: ''Efficient Traceability Systems of Steel Products Using Blockchain-Based Industrial Internet of Things'', *IEEE Transactions on Industrial Informatics*, 16, (9), 2020, pp. 6004-12

[13] A. Lucas, D. Geneiatakis, Y. Soupionis, I. Nai-Fovino, and E. Kotsakis: ''Blockchain Technology Applied to Energy Demand Response Service Tracking and Data Sharing'', *Energies*, 14, (7), 2021

[14] V. Puri, I. Priyadarshini, R. Kumar, and C. Van Le: ''Smart contract based policies for the Internet of Things'', *Cluster Computing*, 24, (3), 2021, pp. 1675-94

[15] Q. N. H. Sieliukov A.V., Khlaponin Y.I.: ''Conceptual model of the mobile communication network'', *The Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things «TTSIIT»*, 2022, pp. 20-22

[16] P. Wang, N. Xu, H. Zhang, W. Sun, and A. Benslimane: ''Dynamic Access Control and Trust Management for Blockchain-Empowered IoT'', *IEEE Internet of Things Journal*, 9, (15), 2022, pp. 12997-3009

[17] T. Li, H. Wang, D. He, and J. Yu: ''Permissioned Blockchain-Based Anonymous and Traceable Aggregate Signature Scheme for Industrial Internet of Things'', *IEEE Internet of Things Journal*, 8, (10), 2021, pp. 8387-98

[18] N. H. Qasim, V. Vyshniakov, Y. Khlaponin, and V. Poltorak: ''Concept in information security technologies development in e-voting systems'', *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS)*, 3, (9), 2021, pp. 40-54

[19] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K. C. Li: ''A Secure FaBric Blockchain-Based Data Transmission Technique for Industrial Internet-of-Things'', *IEEE Transactions on Industrial Informatics*, 15, (6), 2019, pp. 3582-92

[20] H. Wei, W. Feng, C. Zhang, Y. Chen, Y. Fang, and N. Ge: ''Creating Efficient Blockchains for the Internet of Things by Coordinated Satellite-Terrestrial Networks'', *IEEE Wireless Communications*, 27, (3), 2020, pp. 104-10

[21] Y. Liu, K. Wang, Y. Lin, and W. Xu: ''$\mathsf{LightChain}$: A Lightweight Blockchain System for Industrial Internet of Things'', *IEEE Transactions on Industrial Informatics*, 15, (6), 2019, pp. 3571-81

[22] P. Koshy, S. Babu, and B. S. Manoj: ''Sliding Window Blockchain Architecture for Internet of Things'', *IEEE Internet of Things Journal*, 7, (4), 2020, pp. 3338-48

[23] K. P. Satamraju, and M. B: ''Proof of Concept of Scalable Integration of Internet of Things and Blockchain in Healthcare'', *Sensors*, 20, (5), 2020

[24] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun: ''Blockchain for Large-Scale Internet of Things Data Storage and Protection'', *IEEE Transactions on Services Computing*, 12, (5), 2019, pp. 762-71

[25] Q. Song, Y. Chen, Y. Zhong, K. Lan, S. Fong, and R. Tang: ''A Supply-chain System Framework Based on Internet of Things Using Blockchain Technology'', *ACM Trans. Internet Technol.*, 21, (1), 2021, pp. Article 13

[26] A. Mkpa, J. Chin, and A. Winckles: ''Holistic Blockchain Approach to Foster Trust, Privacy and Security in IoT Based Ambient Assisted Living Environment'', *2019 15th International Conference on Intelligent Environments (IE)*, 2019, pp. 52-55

[27] Y. Yu, S. Liu, P. L. Yeoh, B. Vucetic, and Y. Li: ''LayerChain: A Hierarchical Edge-Cloud Blockchain for Large-Scale Low-Delay Industrial Internet of Things Applications'', *IEEE Transactions on Industrial Informatics*, 17, (7), 2021, pp. 5077-86

[28] J. Wu, M. Dong, K. Ota, J. Li, and W. Yang: ''Application-Aware Consensus Management for Software-Defined Intelligent Blockchain in IoT'', *IEEE Network*, 34, (1), 2020, pp. 69-75