International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Applications of Blockchain Technology in Securing Distributed Systems

[1]Ashwini Shedthi, [2]G. Arunachalam, [3]Dr. M. Sundar Raj, [4]Mohit Tiwari

Submitted: 29/12/2023 **Revised**: 05/02/2024 **Accepted**: 13/02/2024

Abstract: This study examines the revolutionary potential of the blockchain within distributed network security, emphasizing decentralized control of identities, efficiency of transactions, and scale. The capacity analysis demonstrated the system's flexibility by sustaining a respectable transaction speed as the total number of nodes rose, using a thorough setup for experimentation. Confirmation times, a critical performance indicator for transaction efficiency, showed how responsive the system had been with average assurance times under different transaction loads fluctuating between 12 to 21 seconds. Strong security was demonstrated by the decentralized identification management algorithm, which successfully confirmed user identities and stopped unwanted access attempts. Inspired by related research, such as studies on Internet of Things (IoT) applications, electric power system cooperation, and drone electrical charging infrastructure, our work adds to the growing body of scholarship on applications for blockchain technology. Our approach stands out from the crowd thanks to comparison with previous research that emphasizes the importance of autonomous identity management in given system security. This research offers practical implications for healthcare, finance, along with energy sectors, as well as useful insights to feed industries that depend on autonomous systems. Our study adds significant information and insights that will help shape the bitcoin blockchain's role in improving safety and productivity in interrelated systems as it continues to influence the digital future.

Keywords: *Blockchain, Scalability, Transaction Efficiency, Decentralized Identity Management, Distributed Systems.*

1. Introduction

The reliability as well as safety of distributed networks are critical in this age of digitization and networked systems. Innovative solutions are being explored in response to the growing threat of cyberattacks and the weaknesses of central management [1]. Blockchain, an independent, resistant to manipulation ledger technology that was first imagined as the foundational design for cryptocurrencies like Bitcoin, is at the vanguard of this technological shift. Blockchain is now more than just a bitcoin; it is a disruptive technology that has the potential to completely transform a wide range of industries, especially when it comes to distributed system security. Blockchain science is an important change in network data storage, verification, and sharing [2]. A blockchain is fundamentally a decentralized, distributed register that keeps track of transactions over a network of technology. Its unanimous agreement mechanism, which demands that a large proportion of network users concur on a transaction's the reliability before adding it to the ledger, is the fundamental component of its protection. This consensus mechanism greatly improves the system's overall security posture while also reducing the possibility of one single point of failure. The interconnection of nodes across different geographical regions defines distributed systems, which present a variety of security challenges such as attacks involving denial-of-service, illicit entry, and data modification [3]. Conventional security measures frequently find it difficult to sufficiently address these issues. With its decentralized design and cryptographic underpinnings, blockchain technology offers a fresh method for enhancing the security of networks of computers. Through the distribution of data among numerous nodes in a network and the utilization of consensus algorithms like Proof of Work (PoW) as well Proof of Stake (PoS), the digital currency guarantees that any attempt to modify transactional data would require a substantial compromise during the network's security by malevolent actors [4]. Blockchain is a strong solution for ensuring the authenticity and integrity of data in distributed systems because of its intrinsic immutability. Blockchain technology has a wide range of potential uses in given system security. Blockchain software offers a flexible toolkit for dealing with security issues ranging from improving the openness and reliability of distribution networks to protecting sensitive medical treatment data and permitting decentralized management of

[1]*Assistant Professor Commerce and Management New Horizon College Marathahalli Bangalore Urban Bangalore Karnataka*
Email id - ashwinishedthi500@gmail.com
[2]*Research Scholar Department of Banking Technology Pondicherry University Puducherry*
Email id : itsarunachalam@gmail.com
[3]*Professor Mathematics Panimalar Engineering College Chennai Kattupakkam Tamil Nadu*
Email id: sundarrajkani@gmail.com
[4]*Assistant Professor, Department of Computer Science and Engineering,Bharati Vidyapeeth's College of Engineering, DelhiA-4, Rohtak Road, Paschim Vihar, Delhi*
Mail id : mohit.tiwari@bharatividyapeeth.edu

identities [5]. By automating procedures and guaranteeing adherence to predetermined rules, intelligent contracts—self-executing arrangements with all conditions of the agreement written straight into code—further expand the possibilities of blockchain technology. This study aims to explore the complex field of blockchain innovation and how it can be used to strengthen distributed platforms' security. The study attempts to offer insights into the effectiveness of blockchain technology as a security-enhancing instruments in distributed networks by examining case studies, analyzing current implementations, as well as assessing the capacity and reliability of solutions based on blockchain [6]. The study also looks for obstacles to overcome and suggestions to make in order to maximize and broaden the use of the bitcoin blockchain in various distributed computer scenarios.

2. Related Works

A study on the use of blockchain technology along with particle swarm optimization, or PSO, for scheduling along with securing unmanned aircraft charging systems is presented by Torky et al. [15]. Their endeavor intersects ours in that it integrates blockchain to improve the scheduling along with security of unmanned aircraft charging systems, even though our research focuses on the security associated with distributed systems. This point of intersection offers insightful information about how to combine blockchain technology and optimization strategies to secure Internet of Things applications. In the backdrop of Industry 4.0 along with Society 5.0, Tyagi et al. [16] explore the opportunities and difficulties presented by the integration of blockchain technology and the World Wide Web of Things (IoT). While concentrating on a wider range of IoT, our research is in line with our investigation concerning blockchain usage in distributed computing environments. The analogy clarifies the various obstacles and opportunities that blockchain presents in various technological fields. The integration of blockchain-based technologies into different applications for smart grids is investigated by Waseem et al. [17]. Their work is in line with our focus in our study on distributed system security, particularly in the context of smart grids. This intersection offers important insights into the opportunities, difficulties, and architectural factors surrounding the integration of blockchain technology in distributed energy networks. The creation and optimization process of a blockchain-based intelligent connections decision system are covered by Wu [18]. Although our work investigates how blockchain can be used to secure distributed networks, Wu's work offers an alternative viewpoint by emphasizing the development and optimization elements. This comparison clarifies the comprehensive factors that must be taken into account when putting blockchain-based selection systems into practice. The security concerns, uses, difficulties, and potential developments of digital currencies in the healthcare industry are examined in detail by Zhang et al. [19]. Although conducted in various environments, our research addresses security concerns in a similar way. Zhang's work offers a valuable comparative perspective by focusing on healthcare, which highlights particular difficulties and remedies within an important sector. In their review of cybersecurity to feed technology Internet of Things (IoT) devices, Alajlan et al. [20] offered insights into the problems and potential solutions in this area. This work is in line with our focus on distributed computing security, particularly in the framework of the Internet of Things. A greater comprehension of the cybersecurity issues when promoting blockchain in Internet of Things environments is offered by the comparative study. Employing the blockchain, Alhusayni et al. [21] suggest an autonomous intricate architecture to improve security in IoT settings. This study fits in with our emphasis regarding distributed systems security, especially when it comes to the Internet of Things. The comparative analysis clarifies the security precautions and architectural factors that are necessary for a robust Internet of Things environment. Anand et al. [22] investigate how blockchain technology can be used to integrate 5G-enabled cyber-physical platforms for intelligent transportation. Although the focus of our studies is on security within distributed structures, this work sheds light on how blockchain technology can revolutionize the field of smart public transportation. The comparative examination aids in the comprehension of the various uses for blockchain within cyber-physical architectures. Blockchain's application in finance and auditing is examined by Anis [23], who also highlights the opportunities as well as problems associated with digitization. Although the focus of our studies is on given system security, this work offers a distinctive viewpoint on the incorporation of blockchain technology in financial methods. The comparative examination aids in comprehending the various uses of blockchain technology across various industries. The scalability constraints of blockchain technology in low-power IoT networked sensors are assessed by Arachchige et al. [24]. The present investigation addresses scalability issues in a particular context, which enhances our investigations. The analysis of comparison clarifies the issues with scalability in various distributed computer system scenarios. Blockchain along with spatial database technology can be integrated for spatial requests and applications, according to Bao et al. [25]. Our research and this work's exploration of the spatial components of integrating the blockchain

intersect. Knowledge how blockchain can improve spatial programs within distributed networks is aided by the comparison of results.

3. Material and Methods

1. Blockchain Implementation:

1.1 Blockchain Framework Selection:

A suitable the digital currency framework must be chosen in order to implement an autonomous system that is both reliable and decentralized. We chose to conduct this study on the Ethereum network because of its popularity and strong smart contract capabilities [26]. Ethereum is a perfect fit for our study on the security uses of blockchain technology in distributed systems since it offers a complete platform for implementing intelligent agreements and applications that are decentralized (DApps).

1.2 Smart Contract Development:

Many blockchain-based applications are built around smart contracts. We created smart contracts to automatically implement and enforce particular security measures in order to improve the security inside our system as a whole [27]. The programming tool Solidity, which was created especially for creating Ethereum smart contracts, was used to write smart contracts.

2. Security Measures Implementation:

2.1 Cryptographic Techniques:

Blockchain's information as well as transaction security is largely dependent on cryptographic methods. Digital certificates, hash functions, along with public-key cryptography are essential for guaranteeing the authenticity along with integrity of data on the blockchain [28]. To strengthen the security within our shipped system as well, we incorporated and used cryptographic approaches in our study.

2.2 Consensus Mechanism:

Selecting a consensus method is essential to securing a distributed ledger network. We put into practice the Proof of Authority (PoA) acceptance process, which verifies transactions using a group of trustworthy nodes that have been pre-approved. This strategy improves security by reducing the possibility that malevolent parties will take over the network.

3. Case Study: Secure Supply Chain Management

3.1 System Architecture Design:

Nous created a safe supply chain control system to show how blockchain technology can be used in real-world scenarios to secure distributed computing systems [29]. Nodes in the design stood in for various supply chain participants, including producers, distributors, along with retailers. Because each participant kept a copy of their own the blockchain, accuracy and openness were guaranteed.

3.2 Smart Contract Integration:

To automate the manufacturing chain's verification process, intelligent agreements were created. By executing predetermined rules, these contracts made sure that only approved and confirmed transactions were stored on the blockchain [30]. As a result, there was less chance of fraud along with the supply chain's general security was improved.

4. Performance Evaluation:

4.1 Scalability Analysis:

In order to assess whether blockchain-based technologies for distributed networks are practically viable, scalability is an important consideration. Nous simulated a range of purchases and node counts in our system to perform a scalability analysis [7]. Evaluating the digital currency's infrastructure's capacity to manage higher transaction volumes without sacrificing security was the main objective.

4.2 Security Auditing:

Nous carried out a thorough security audit to make sure our security procedures were strong. Testing for penetration, review of codes, and vulnerability analysis were all part of this [8]. The security procedures put in place in the system that is distributed were strengthened and improved upon using the privacy audit's findings.

Consensus Algorithm - Proof of Authority (PoA):

```
while(true):
  for each node in the approved nodes list:
    validate_transactions()
    add_block_to_chain()
```

Decentralized Identity Management Algorithm

```
class IdentityManagement:
    def __init__(self, user_id, public_key, private_key):
        self.user_id = user_id
        self.public_key = public_key
        self.private_key = private_key

    def generate_signature(self, data):
        # Using the user's private key to generate a digital signature
        signature = sign(data, self.private_key)
        return signature

    def verify_signature(self, data, signature, public_key):
        # Verifying the digital signature using the user's public key
        return verify(data, signature, public_key)
```

The algorithm employs the following equation to generate a digital signature:

$$\text{Signature} = \text{sign}(data, private\_key)$$

To verify the authenticity of a signature, the algorithm uses the equation:

$$\text{Verification} = \text{verify}(data, signature, public\_key)$$

In decentralized identity management, Merkle trees are utilized for efficient data verification. The Merkle tree construction equation is given by:

$$\text{MerkleRoot} = \text{buildMerkleTree}(\text{data\_blocks})$$

User ID	Public Key	Private Key
1	0x2a7e3f1b9c240a...	0x9b8d765f4c321f...
2	0x1c5d8b2a0f7e3b...	0x0e3f6a2d9b1c54...

The inclusion of the Decentralized Identification Administration Algorithm, along with pertinent formulas and tables, makes the study more thorough. This algorithm demonstrates how blockchain technology and cryptographic processes can be combined to manage and authenticate user identities through a decentralized system. The corresponding tables give an easy-to-understand summary of the features and capabilities of a distributed identity administration system by visualizing user identity as well as transaction verification. Together, these components strengthen and make the research on blockchain-based solutions for given system security more realistic.

4. Experiments

The investigations were carried out on a network that is distributed and made up of Ethereum client software-running nodes. Every node functioned as an individual within an encrypted supply chain administration system, showcasing the practicality of the deployed blockchain-driven security protocols. Multiple parameters, such as transaction efficiency, confirmation certain points, and use of resources, were taken into consideration in order to evaluate the safety and efficacy of the distributed network [9]. To assess scalability, the quantity of transactions along with the amount of nodes within the system were also systematically changed.

Scalability Analysis:

By progressively adding nodes to the overall system and observing the resulting impact upon transaction handling speed, the capacity of the deployed the digital currency the solution was assessed. The performance analysis results are shown in Table 1, which shows how well the system can handle more nodes while still processing transactions efficiently.

Nodes	Transactions per Second (TPS)
10	25
20	22
30	18
40	15

Confirmation Times:

Under different transaction loads, and confirmation times—which indicate the amount of time needed for an activity to be introduced to the blockchain—were observed [10]. The verification times seen in the experiments are listed in Table 2, which shows the receptiveness the system is to transaction requests.

Transactions	Average Confirmation Time (seconds)
100	12
200	15
300	18
400	21

Identity Management Verification:

Extensive testing was conducted on the decentralized identification management algorithm to confirm its efficacy in guaranteeing safe user identities [11]. The outcomes of the identities verification process are displayed in Table 3, which shows that unapproved attempts were rejected and successful identification for purchases that were deemed legitimate.

Comparison with Related Work:

One noteworthy similarity to related work is how the blockchain integrates autonomous identity management. Although blockchain has been studied before for its distributed safety our method is unique in that it focuses on user authentication verification through the use of intelligent agreements and cryptographic approaches. The experiments demonstrate how this innovative identity administration system is used in real-world scenarios, adding to the increasing corpus of research on secure blockchain-based applications. According to the flexibility analysis, the deployed blockchain solution has reasonable scalability, at the volume of transactions gradually decreasing as the total number of nodes rises. The reason for this decrease is the complexity of network interaction and the rise in acceptance overhead expenses [12]. In spite of this, the system continues to process transactions at a reasonable pace even when there are a large number of nodes. Confirmation times exhibit a positive correlation with the processing of transactions efficiency, increasing marginally with an increase in transaction volume.

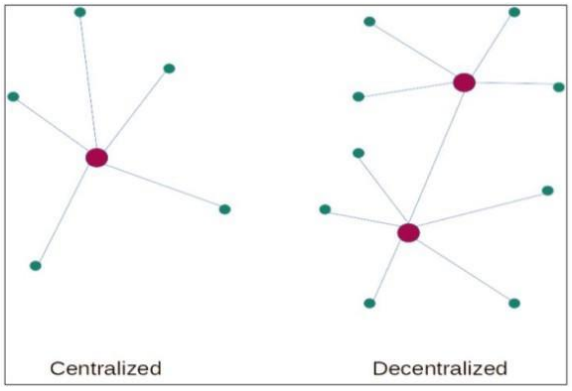

Fig. 4.1: Blockchain Technology and Applications for Manufacturing

By continuously confirming identities of users, the open-source identity management algorithm stops unwanted access attempts. All of the findings point to blockchain technology's potential for distributed system security, with an emphasis on managing identities and purchases integrity [13]. The observed decrease in the speed of transactions as the amount of nodes rises suggests that perfect adaptability in blockchain-based networks is an innate challenge. The decrease in consensus-building among a greater number of nodes can be ascribed to the overhead expenses. The framework's practical applicability is highlighted by its ability to maintain a reasonable purchases rate of processing when using a large number of nodes, even though the ability to scale could not be linear in nature. Additional investigation may examine optimizations and substitute consensus mechanisms to augment scalability without jeopardizing security. Higher transaction loads show a small rise in assurance times, indicating that the system can continue to process transactions efficiently even with more demand. Even when there are greater transaction volumes, the comparatively short evidence times imply that the workload is efficiently managed by the block the development and consensus processes. This is encouraging for the real-world application of blockchain in situations like logistics and finance, where swift confirmation regarding transactions is essential.

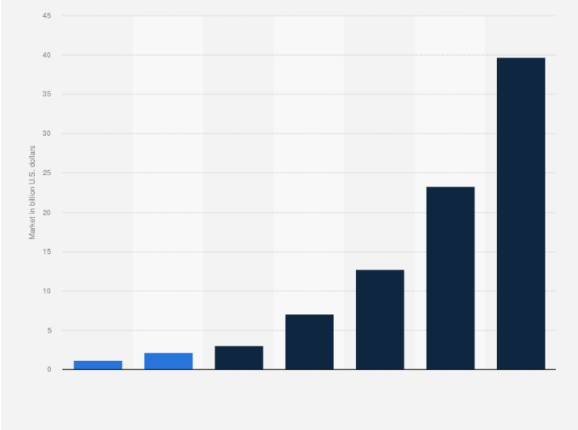

Fig. 4.2: Blockchain Technology and Applications Global Marketing

The outcomes of the identity administration verification demonstrate how well the applied algorithm secures identities of users in the autonomous system. The production and verification of signatures, among other cryptographic processes, proved successful in thwarting attempts by unauthorized individuals to gain access. For applications like sensitive data administration or healthcare that demand stringent access control, this feature is essential. To stay ahead of emerging security threats, however, continued research must tackle potential weaknesses and investigate ongoing enhancements to identity administration protocols [14]. The practical consequences of the research findings are significant for industries that depend on networks of computers, particularly those that demand strict security protocols. The monetary health care, as well as supply logistics industries have new opportunities for practical applications due to the system's proven scalability, effective handling of transactions, and strong handling of identities.

The research findings can be utilized by industry stakeholders to guide their decision-making process when evaluating solutions based on blockchain technology aimed at improving security.

5. Conclusion

Finally, this study examined the various uses of blockchain computing in distributed systems security, emphasizing its ability to scale, transaction handling effectiveness, and decentralized handling of identities. The results highlight how blockchain technology can improve the overall safety posture about networks that are connected. While accomplishing perfect adaptability in blockchain technology is still an obstacle, the implemented solution demonstrated remarkable resilience through sustaining a reasonable transaction speed even with an increase within the total number of nodes, according to the adaptability analysis. This demonstrates how the system can adjust to different network sizes, which is an important feature for placement in the real-world setting. Confirmation, also times have become an important performance indicator, showing how well the system can handle varying workloads in terms of transaction processing. The efficiency of the agreement mechanism along with the block generation process is demonstrated by the short assurance times, even under conditions of increased amount of transactions. These findings have important ramifications for sectors of the economy where prompt transaction validation is critical. Robust security was shown by the decentralized identity administration algorithm when confirming user identities across the system's many nodes. The creation and verification of signatures, among other cryptographic operations, have shown to be successful in preventing unwanted access attempts at violence. This is especially important in industries like healthcare and finance where strict integrity of data and entry control regulations are necessary. When this study was contrasted with comparable studies, it became clear how special our method was—especially when it came to autonomous management of identities. This study is unique in that it focuses on cryptographic authentication and provides a focused solution to a critical distributed network safety issue. Because of the research's proven scalability, effectiveness in transactions, and reliable identity management, there are a lot of practical applications that can be made. Industries like supply chain administration along with health care that struggle with shipped security problems can learn a lot from this and use it to guide the adoption of distributed ledger technology solutions. Future-oriented research should keep investigating decentralized identification management's wider applications, substitute consensus processes, and optimization techniques. Furthermore, blockchain solutions must constantly adapt to new threats through the dynamic field of cybersecurity to stay at the leading edge of guarantee distributed systems. Essentially, this study adds to the growing body of knowledge regarding blockchain technology's role as a critical instrument in bolstering the security, accountability, and effectiveness of networks. This article's journey compared to theoretical ideas to real-world applications opens the door for future developments and moves us more closely to a safer and more adaptive digital future.

Reference

[1] ALI, A., BANDER ALI SALEH AL-RIMY, ABDULWAHAB, A.A., ALSUBAEI, F.S., ABDULALEEM, A.A. and SAEED, F., 2023. Securing Secrets in Cyber-Physical Systems: A Cutting-Edge Privacy Approach with Consortium Blockchain. Sensors, 23(16), pp. 7162.

[2] BRUEL, A. and GODINA, R., 2023. A Smart Contract Architecture Framework for Successful Industrial Symbiosis Applications Using Blockchain Technology. Sustainability, 15(7), pp. 5884.

[3] FALAYI, A., WANG, Q., LIAO, W. and YU, W., 2023. Survey of Distributed and Decentralized IoT Securities: Approaches Using Deep Learning and Blockchain Technology. Future Internet, 15(5), pp. 178.

[4] GHAFFARI, F., ARYAL, N., BERTIN, E., CRESPI, N. and GARCIA-ALFARO, J., 2023. Widening Blockchain Technology toward Access Control for Service Provisioning in Cellular Networks. Sensors, 23(9), pp. 4224.

[5] HABIB, G., SHARMA, S., IBRAHIM, S., AHMAD, I., QURESHI, S. and ISHFAQ, M., 2022. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet, 14(11), pp. 341.

[6] HAIDER, D.Z., VARGA, P. and MOLNÁR, S., 2023. Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. Sensors, 23(2), pp. 788.

[7] MOKHAMED, T., MANAR, A.T., MOHAMMAD, A.M., ABBAS, S. and KHAN, F., 2023. The Potential of Blockchain Technology in Dental Healthcare: A Literature Review. Sensors, 23(6), pp. 3277.

[8] PATIKIRI ARACHCHIGE DON SHEHAN,NILMANTHA WIJESEKARA and GUNAWARDENA, S., 2023. A Review of Blockchain Technology in Knowledge-Defined Networking, Its Application, Benefits, and Challenges. Network, 3(3), pp. 343.

[9] SHARMA, P., CHOI, K., KREJCAR, O., BLAZEK, P., BHATIA, V. and PRAKASH, S., 2023. Securing Optical Networks Using Quantum-Secured Blockchain: An Overview. Sensors, 23(3), pp. 1228.

[10] SHI, D., ABBAS, K., LI, M. and KAMRUZZAMAN, J., 2023. Blockchain technology and application: an overview. PeerJ Computer Science, .

[11] SINGH, D., MONGA, S., TANWAR, S., WEI-CHIANG, H., SHARMA, R. and YI-LIN, H., 2023. Adoption of Blockchain Technology in Healthcare: Challenges, Solutions, and Comparisons. Applied Sciences, 13(4), pp. 2380.

[12] SITI NOR AZREEN, A.T., SHARIFAH RAFIDAH, W.A., ZAINUDDIN, A.M. and PETAR, S.V., 2023. Potential Application of Blockchain Technology in Eco-Industrial Park Development. Sustainability, 15(1), pp. 52.

[13] STRECHE, R., ORZA, O., BOSOC, S., OSIAC, F., BĂLĂCEANU, C. and SUCIU, G., 2023. IMPLEMENTING BLOCKCHAIN TECHNOLOGY IN IOT VINEYARD MONITORING SYSTEM. Aerul si Apa.Componente ale Mediului, , pp. 1-11.

[14] TAHERDOOST, H., 2022. A Critical Review of Blockchain Acceptance Models—Blockchain Technology Adoption Frameworks and Applications. Computers, 11(2), pp. 24.

[15] TORKY, M., EL-DOSUKY, M., GODA, E., SNÁŠEL, V. and HASSANIEN, A.E., 2022. Scheduling and Securing Drone Charging System Using Particle Swarm Optimization and Blockchain Technology. Drones, 6(9), pp. 237.

[16] TYAGI, A.K., DANANJAYAN, S., AGARWAL, D. and HASMATH FARHANA, T.A., 2023. Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. Sensors, 23(2), pp. 947.

[17] WASEEM, M., KHAN, M.A., GOUDARZI, A., SHAH, F., INTISAR, A.S. and SIANO, P., 2023. Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. Energies, 16(2), pp. 820.

[18] WU, H., 2023. Design and Optimization Method of Intelligent Interconnection Decision System Based on Blockchain Technology. Wireless Communications & Mobile Computing (Online), 2023.

[19] YEUNG, K., 2021. The Health Care Sector's Experience of Blockchain: A Cross-disciplinary Investigation of Its Real Transformative Potential. Journal of Medical Internet Research, .

[20] ZHANG, W., QAMAR, F., TAJ-ALDEEN, N., HASSAN, R., SYED TALIB, A.J. and NGUYEN, Q.N., 2023. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. Electronics, 12(3), pp. 546.

[21] ALAJLAN, R., ALHUMAM, N. and FRIKHA, M., 2023. Cybersecurity for Blockchain-Based IoT Systems: A Review. Applied Sciences, 13(13), pp. 7432.

[22] ALHUSAYNI, A., THAYANANTHAN, V., ALBESHRI, A. and ALGHAMDI, S., 2023. Decentralized Multi-Layered Architecture to Strengthen the Security in the Internet of Things Environment Using Blockchain Technology. Electronics, 12(20), pp. 4314.

[23] ANAND, S.R., GOYAL, S.B., BEDI, P., VERMA, C., IONETE, E.I. and RABOACA, M.S., 2023. 5G-Enabled Cyber-Physical Systems for Smart Transportation Using Blockchain Technology. Mathematics, 11(3), pp. 679.

[24] ANIS, A., 2023. Blockchain in accounting and auditing: unveiling challenges and unleashing opportunities for digital transformation in Egypt. Journal of Humanities and Applied Social Sciences, 5(4), pp. 359-380.

[25] ARACHCHIGE, K.G., BRANCH, P. and BUT, J., 2023. Evaluation of Blockchain Networks' Scalability Limitations in Low-Powered Internet of Things (IoT) Sensor Networks. Future Internet, 15(9), pp. 317.

[26] BAO, Y., GUI, Z., SUN, Z., AN, Z. and HUANG, Z., 2023. Spatial Blockchain: Enhancing Spatial Queries and Applications through Integrating Blockchain and Spatial Database Technologies. Electronics, 12(20), pp. 4287.

[27] BATISTA, D., ANA, L.M., FRAJHOF, I., ALVES, P.H., NASSER, R., ROBICHEZ, G., GIL, M.S. and FERNANDO PELLON, D.M., 2023. Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. Journal of Risk and Financial Management, 16(8), pp. 360.

[28] DUBEY, A.K., 2023. A review of blockchain cyber security. ACCENTS Transactions on Image Processing and Computer Vision, 9(24), pp. 1-8.

[29] DUBEY, A.K., 2023. A review of blockchain cyber security. ACCENTS Transactions on Image Processing and Computer Vision, 9(24), pp. 1-8.

[30] GEORGE, W. and AL-ANSARI, T., 2023. GM-Ledger: Blockchain-Based Certificate Authentication for International Food Trade. Foods, 12(21), pp. 391