Journal of Business and Management Studies
ISSN: 2709-0876
DOI: 10.32996/jbms
Journal Homepage: www.al-kindipublisher.com/index.php/jbms

JBMS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Blockchain Applications in Retail Cybersecurity: Enhancing Supply Chain Integrity, Secure Transactions, and Data Protection

Rejon Kumar Ray[1], Faiaz Rahat Chowdhury[2] and MD Rokibul Hasan MBA, PMP, CSM[3] ✉
[123]*Department of Business Analytics, Gannon University, Erie, Pennsylvania, USA*
Corresponding Author: MD Rokibul Hasan, **E-mail**: prorokibulhasanbi@gmail.com

| ABSTRACT
Blockchain technology has proven a powerful tool for reinforcing cybersecurity in the retail sector. This research offers an extensive overview of the applications of blockchain in retail cybersecurity, particularly, underscoring supply chain integrity, data protection, and transaction security. The research explored how blockchain can facilitate provenance and traceability well as prevent counterfeiting and enhance vendor management in the supply chain. It also explores how blockchain-based payment frameworks and fraud detection systems can boost transaction security. Moreover, the study assesses the capability of blockchain to safeguard data via privacy and consent management, and secure and immutable data storage. The findings outline the capability of blockchain technology to diminish risks, enhance transparency, and affirm trust in retail cybersecurity. While challenges are inevitable, such as regulatory and scalability considerations, the research infers that blockchain technology presents noteworthy opportunities for innovation and advancement in the retail industry's cybersecurity landscape.

| KEYWORDS

Retail cybersecurity; Blockchain technology; Data protection; Supply chain integrity; Transaction security

| ARTICLE INFORMATION

ACCEPTED: 15 January 2024 **PUBLISHED:** 10 February 2024 **DOI:** 10.32996/jbms.2024.6.1.13

1. Introduction

According to Ali et al. (2022), the retail sector has witnessed massive changes in the recent past as more organizations have moved online and digitally. While digital advancements have inspired new opportunities for organizations to reach prospective clients more easily, it has equally exposed them to more cybersecurity risks. Data thefts and breaches targeting retailers have become common as hackers take advantage of the vulnerabilities in legacy systems. Demirkan et al. (2020), contend that to resolve the escalating challenge, retailers are examining emerging technologies like blockchain to enhance security. Blockchain technology has proven to be a promising resolution for reinforcing cybersecurity in various sectors. In the retail domain, where secure transactions, data integrity, and supply chain transparency are pivotal, blockchain holds substantial possibility. This report explores the applications of blockchain technology in retail cybersecurity, particularly addressing secure transactions, supply chain integrity, and data protection.

1.1 Background

Alotaibi (2019), indicates that the retail sector functions in a complex and dynamic environment, with a multitude of shareholders encompassed in various phases of the supply chain. With the escalation of digitalization and the exponential dependence on technology, the retail industry has become susceptible to cybersecurity threats. These threats entail data payment fraud, breaches, supply chain vulnerabilities, and counterfeit products, among others. Mainstream centralized systems in the retail sector frequently struggle to efficiently resolve these cybersecurity obstacles. Centralized databases are vulnerable to single points of failure and can be exploited by malicious actors targeting to leverage vulnerabilities. As a consequence, there is an escalating need for innovative solutions that can reinforce cybersecurity measures and diminish risks in the retail sector.

Blockchain technology has arisen as a possible game-changer in the domain of cybersecurity. Initially crafted as the fundamental technology for cryptocurrencies like Bitcoin, blockchain provides an immutable and decentralized ledger that can transform the manner transactions and data are recorded, secured, and verified (Hasanova et al., 2023). By employing cryptographic methods and disseminated consensus mechanisms, blockchain offers transparency, immutability, and enhanced security.

In the setting of the retail sector, blockchain technology can resolve key cybersecurity matters. Supply chain integrity is a paramount component for retailers, as it affirms that products are traceable, authentic, and free from damage (Alotaibi, 2019). With blockchain, every item can be assigned a unique identifier, facilitating shareholders to track its journey from the producer to the end consumer. This traceability and transparency can assist in terms of combatting counterfeit products and affirming the authenticity of goods.

Hasan (2022), articulates that secure transactions are another imperative dimension of retail cybersecurity. Conventional payment systems frequently depend on intermediaries, such as payment processors, or banks which can present vulnerabilities and elevate the threat of fraud. Blockchain-based payment mechanisms reduce the need for intermediaries, hence, enabling peer-to-peer transactions that are secure, transparent, and efficient.

Data protection is also a noteworthy issue in the retail sector, provided the large volume of sensitive customer information that is gathered and stored. Data breaches can have detrimental implications, encompassing reputational damage, financial losses, and regulatory penalties (Hasan, 2022). Blockchain technology provides a possible solution by offering decentralized and encrypted data preservation, where sensitive info can be securely preserved and accessed only by authorized parties.

This research paper aims to examine how blockchain technology can fortify cybersecurity operations across different aspects of the retail industry. First, it assesses how blockchain can boost supply chain integrity by facilitating the traceability of items from origin to point of sale. Subsequently, this report explores how blockchain-oriented digital payments can assist in resolving issues like credit card fraud. Lastly, it evaluates blockchain's role in terms of safeguarding client data privacy and access controls. The research paper holds that employing blockchain-enabled resolutions can substantially reinforce retail cyber defenses and establish greater trust with stakeholders in today's digital marketplace.

1.2 Research Objectives

The principal objective of this study is to examine how blockchain technology can reinforce cybersecurity operations in the retail sector. By concentrating on secure transactions, supply chain integrity, and data safeguarding, the objective is to pinpoint the possible benefits and challenges related to implementing blockchain solutions in the retail context. The research objectives of this study are as follows:

- To explore how blockchain technology can strengthen supply chain integrity in the retail sector.
- To examine the role of blockchain in terms of securing transactions within the retail industry.
- To ascertain how blockchain technology contributes to data protection in the retail sector.
- To analyze and pinpoint the challenges and benefits associated with implementing blockchain technology in retail cybersecurity.

1.3 Research Questions

RQ*[1]*: How does blockchain technology reinforce supply chain integrity in the retail sector?

RQ[2]: What are the applications of blockchain in terms of safeguarding transactions within the retail industry?

RQ[3]: How does blockchain technology contribute to data safeguarding in the retail sector?

RQ[4]: What are the challenges and benefits of implementing blockchain in retail cybersecurity?

1.4 Significance of the research

This study holds substantial importance for the retail sector and its shareholders. The findings of this research will offer insights into the capability of blockchain technology in terms of resolving cybersecurity issues, enhancing transparency, and building trust among retailers, suppliers, and customers. By examining real-world use scenarios and initiatives, this research aims to illustrate the practical applications of blockchain in the retail sector, facilitating informed decision-making and potential employment of these solutions.

The significance of this study also lies in its contribution to the present body of research on blockchain technology and its deployment in the retail sector. By pinpointing the challenges and benefits related to deploying blockchain, this study will present crucial insights for researchers, policymakers, and industry practitioners targeting to leverage this technology to enhance cybersecurity in retail.

2. Conceptual Framework

2.1 Blockchain Technology: An Overview

Blockchain technology is gradually becoming a revolutionary force in various sectors, providing a secure and decentralized method of managing transactions and information (Taylor et al, 2020). At its center, a blockchain is an immutable and distributed ledger that records transactions across a network of computers. Unlike conventional centralized systems, blockchain functions on a peer-to-peer network, allowing security, transparency, and efficiency.

2.2 Distributed Ledger Technology

Distributed ledger technology (DLT) creates the pillar of blockchain. It comprises the imitation of a database across multiple computers or nodes, forming a decentralized network. Every participant in the network retains a duplicate of the entire ledger, and updates happen simultaneously via a consensus mechanism (Tezel et al., 2021). This decentralized aspect reinforces the security of the framework since there is no single point of failure. Distributed Ledger Technology has far-reaching repercussions, offering a solution to the obstacles of trust, data integrity, and cooperation in various sectors such as finance, supply chain, and healthcare.

2.3 Consensus Mechanisms

As per Ali et al (2022), consensus mechanisms are the procedures that affirm all nodes in a blockchain network coincide with the state of the ledger. One of the most prevalent mechanisms is Proof of Work (PoW), where actors, such as miners, solve complicated mathematical puzzles to authorize transactions and add them to the blockchain. Another protocol is Proof of Stake (PoS), where validators are selected based on the amount of cryptocurrency they hold. Each consensus protocol comes with its merits and limitations, impacting factors such as energy efficiency, scalability, and security

2.4 Smart Contracts

Smart contracts revolve around self-executing contracts with the condition of the agreement explicitly written into code. These contracts instantly enforce and execute themselves when pre-set conditions are met (Alotaibi, 2019). Functioning on blockchain forums, such as smart contracts, and Ethereum, discards the need for intermediaries, minimizing costs and enhancing efficiency. They find applications in different domains, from financial services to supply chain management. Nevertheless, challenges, comprising the need for comprehensive programming and possible security vulnerabilities, underscore the significance of careful development and auditing (Ali, 2022).

2.5 Privacy and Security in Blockchain

Hasan (2022), conveys that while blockchain presents immutability and transparency, affirming security and privacy is pivotal. Privacy is frequently ensured via cryptographic methods that enable actors to engage with the blockchain while keeping their identities and transaction credentials confidential. Ring signatures and zero-knowledge proofs are illustrations of cryptographic tools deployed for privacy. On the other hand, security requires protection against attacks, such as the renowned 51% attack, where a single entity controls most of a network's mining power. Progressive advancements in consensus and encryption mechanisms contribute to the advancing landscape of blockchain security.

3. Cybersecurity Challenges in the Retail Industry

The retail domain, with its escalating dependence on digital technologies, is confronted with diverse cybersecurity challenges. As customers move towards online shopping and companies leverage digital platforms for different operations, the threat domain for retailers has expanded. This section examines three noteworthy cybersecurity challenges in the retail industry: Most notably, supply Chain Integrity, Secure Transactions, and Data Protection (Hasan, 2022).

3.1 Supply Chain Integrity

One of the instrumental cybersecurity issues in the retail sector is ensuring the integrity of the supply chain. Retailers depend on sophisticated networks of manufacturers, suppliers, distributors, and logistics partners. Cyber attackers frequently target the supply chain to manipulate the integrity of services and products (Demirkan et al, 2020). Interfering with the supply chain can cause the prevalence of counterfeit products, which not only undermines consumer trust but also presents substantial safety risks. Retailers should deploy robust cybersecurity activities via the supply chain, entailing secure communication channels, authentication procedures, and continued audits to detect and reduce potential vulnerabilities (Hasanova et al, 2023).

3.2 Secure Transactions

As the retail landscape evolves, so does the sophistication of cyber threats, particularly concerning financial transactions. Secure transactions are paramount in maintaining customer trust and protecting sensitive financial information. Point-of-sale (POS) systems, online payment gateways, and mobile payment apps are prime targets for cybercriminals aiming to steal payment card details and personal information (Hasanova et al, 2023). Retailers need to invest in advanced encryption technologies, secure payment gateways, and implement multi-factor authentication to fortify transaction security. Regular employee training on recognizing and thwarting phishing attacks also plays a crucial role in preventing unauthorized access to payment systems.

3.3 Data Protection

As per Miloslavskaya (2022), the retail sector is a treasure trove of customer data, making it a captivating target for cyber-attackers to abuse or sell confidential information. Data breaches not only culminate in financial losses but also destroy a retailer's reputation. Therefore, protecting client data is of utmost importance. Retailers ought to adhere to comprehensive data protection standards, deploy encryption procedures for preserved data, and undertake consistent security audits. Adhering to data protection regulations, such as the the Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR), is pivotal to avoid legal effects and maintain customer trust.

Considering everything, the cybersecurity obstacles confronting the retail sectors are multifactorial and demand an extensive approach to risk management. Supply chain integrity, data protection, and secure transactions are interconnected elements that demand continuous vigilance and adjusting to emerging threats. As retailers proceed to incorporate digital transformation, remaining ahead of cyber threats demands continuous investment in cybersecurity architecture, employee training, and cooperation with the sectors' experts to promote a secure and resilient retail ecosystem. Only via a proactive and holistic cybersecurity strategy can retailers maneuver the prevailing threat landscape and ensure the safety of their operations and the trust of their customers (Taylor et al 2020).

4. Blockchain Applications in Retail Cybersecurity

As per Hasan (2022), Blockchain technology, prominent for its tamper-resistant and decentralized attributes, has found promising roles in terms of addressing cybersecurity issues within the retail industry. This section examines how blockchain can reinforce secure transactions, and supply chain integrity, and protect sensitive data in the retail industry.

4.1 Enhancing Supply Chain Integrity

In the retail domain, supply chain integrity is instrumental in affirming the authenticity and quality of items. Blockchain presents a decentralized and transparent ledger that can be optimized to elevate various aspects of supply chain management (Hasan, 2022). Supply chain integrity is integral in the retail sector to affirm the traceability, authenticity, and transparency of Items. Blockchain technology can play a fundamental role in this regard.

4.1.1 Traceability and Provenance

Blockchain's capability to develop an unalterable record of transactions enables provenance and traceability in the supply chain. Each step of the product's journey, from production to distribution, can be detailed on the blockchain (Tezel et al., 2021). This transparency not only facilitates retailers to locate the source of products in scenarios of recalls but also empowers customers to verify the authenticity and ethical sourcing of the items they purchase.

4.1.2 Counterfeit Prevention

Counterfeit products present a substantial threat to both clients and retailers. By leveraging blockchain, retailers can deploy mechanisms that verify and track the authenticity of products. This is accomplished via unique identifiers or QR codes that are tagged on the blockchain (Demirkan et al., 202). As such, customers can scan these codes to access a product's entire history, hence affirming that they are purchasing genuine items.

4.1.3 Vendor Management

As per Alotaibi (2019), blockchain can also simplify vendor management by offering a secure and decentralized forum for verifying and documenting vendor information. Smart contracts can computerize processes, affirming that vendors adhere to the predefined standards and security protocols. This not only mitigates the risk of unauthorized access but also reinforces the overall integrity of the supply chain ecosystem.

4.2 Securing Transactions

Securing financial transactions is pivotal in retail, and blockchain brings innovative resolutions to fortify transaction security. Securing transactions is a fundamental component of retail cybersecurity. Blockchain technology provides several key advantages in this regard (Ali et al, 2022).

4.2.1 Payment Systems

Blockchain enables transparent and secure payment systems. Cryptocurrencies, which function on blockchain technology, can offer an extra layer of security by discarding the need for conventional financial intermediaries. Smart contracts within blockchain facilitate computerized and secure payment processes, therefore, minimizing the risk of fraud and unauthorized access to payment information (Hasanova et al, 2023).

4.2.2 Fraud Detection and Prevention

Blockchain's immutability and decentralized nature make it difficult for cybercriminals to hack transaction records. This inherent security attribute assists in fraud detection and prevention. Any attempt to interfere with transaction data would demand consensus from most of the network, making suspicious activities more difficult to execute and conceal (Miloslavskaya et al, 2022)

4.3 Protecting Data

Data protection is a pivotal component of retail cybersecurity, and blockchain provides innovative resolutions to safeguard sensitive information. Data safeguarding is a substantial matter in the retail sector, provided the large volume of sensitive client information that is gathered and preserved. Blockchain technology presents several mechanisms to protect data (Hasan, 2022).

4.3.1 Data Privacy and Consent Management

Blockchain can be deployed to strengthen data privacy by providing customers more control over their private and confidential information (Taylor et al., 2022). Via the application of self-sovereign identity on the blockchain, clients can manage and provide consent for the utilization of their data. This decentralized method minimizes the risk of centralized data breaches and boosts consumer trust.

4.3.2 Immutable Data Storage

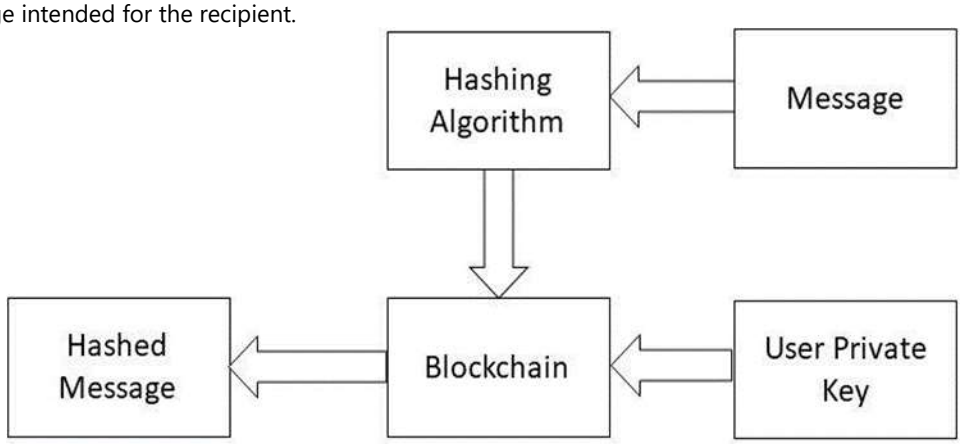
The immutability of data preserved on the blockchain affirms that once information is documented, it cannot be deleted or altered. This feature is specifically valuable in safeguarding client data from unauthorized alterations or deletions (Taylor et al., 2022). Retailers can adopt blockchain for secure and tamper-proof preservation of client profiles, transaction histories, and other sensitive data.

4.3.4 Benefits and Challenges of Blockchain in Retail Cybersecurity

Blockchain technology has become a game-changer in terms of fortifying cybersecurity within the retail sector. While it brings forth tremendous benefits, it also provides unique challenges that should be addressed entirely to realize its potential.

5. Conceptual Framework

This research is premised on the Blockchain conceptual framework, which holds that it is an indisputable digital ledger adept at recording activities, not confined to financial transactions. The effect of this assertion is that Blockchain technology can be adopted to enhance cybersecurity, and supply chains and safeguard systems against phishing attacks. To assess the conceptual framework efficiency in strengthening supply-chain cybersecurity, the methodology of this research will be underpinned by the conceptual framework showcased in the following Figure 1. The procedure comprises inserting an electronic message into a hashing algorithm, which in turn produces a unique fixed-length hash to minimize the message's size. Consequently, the message, coupled with a private key presented by the authorized user, will be incorporated into the blockchain to facilitate other users to validate the message's authenticity. Once a new message is integrated into the blockchain, a unique hash ID will be produced and appended to the final message intended for the recipient.



In the setting of this research, the message denotes the raw and unsecured data that is required to be processed, such as instant messages or emails. To process this raw data, a hashing algorithm is employed. A hashing algorithm refers to a cryptographic algorithm that inputs data and generates a distinct series of characters portraying that data. There are different hashing algorithms accessible, each offering various levels of security and demanding different processing power. Hashes are mostly employed to sign text files or data files to combat tampering.

To insert authenticity into every message, users are anticipated to present a private key that will be adopted by the hashing algorithm. The user's private key is a distinct key identified only to the user and is employed to encrypt the message. It is mathematically irreversible, affirming that the subsequent hash message cannot be overturned back to its initial form. Once the message is safeguarded, it is attached to the blockchain and instilled into other blockchain networks.

The blockchain acts as a progressively intensifying list of records deemed as blocks, which are connected and secured adopting cryptographic hashes grounded on available hashing algorithms. The hashed message portrays the output of the freshly generated block within the up-to-date blockchain. Every generated block has a distinguished hash ID that is attached to the final message before sending it to the intended recipient.

5.1 Research Methodology

5.1.1Research Design

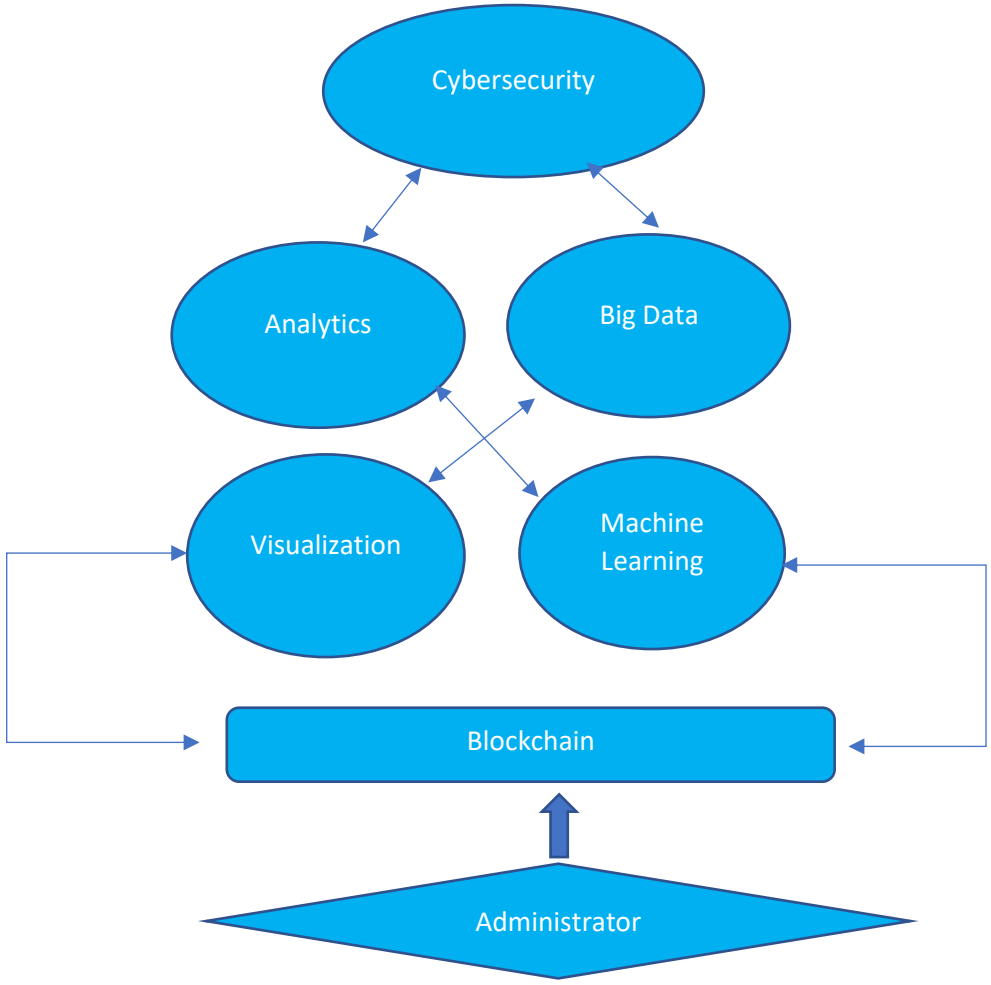
In this research, a programming simulation and descriptive research design will be employed to achieve the research goals. The simulation comprises the employment of a Mersenne Twister pseudorandom number generator crafted by Matsumoto et al. (2017). This generator will be employed to present randomness into the test code, facilitating the simulation of both invalid and valid messages, repeating the characteristics of a phishing attack. The Mersenne Twister pseudorandom number generator is an extensively renowned and proven algorithm in the domain of computer science. It is recognized for its supreme-quality random number production capacities, affirming that the simulation generates reliable and realistic results. By utilizing this generator, the investigation can accurately imitate the unpredictable characteristics of phishing attacks and examine the efficiency of the proposed methodology in detecting and preventing such attacks.

5.1.2 Research Method

A careful choosing process was undertaken to pinpoint a hashing algorithm that is suitable for the execution of the blockchain. Manifold hashing algorithms were imposed for benchmarking, assessing their security grounded on the number of hash possibilities and the sophistication of the produced hashes. Following this choosing process, the SHA256 algorithm was ascertained to be the most appropriate hashing algorithm for the blockchain implementation.

To create a simulated climate for the research, a computer-oriented simulation was crafted. This simulation targeted to reproduce the conduct of both legitimate recipients and email senders as well as phishing email recipients and senders. To affirm a straight and user-friendly code execution, the simulation was designed using JavaScript as the underlying runtime environment.

5.2 Proposed Model

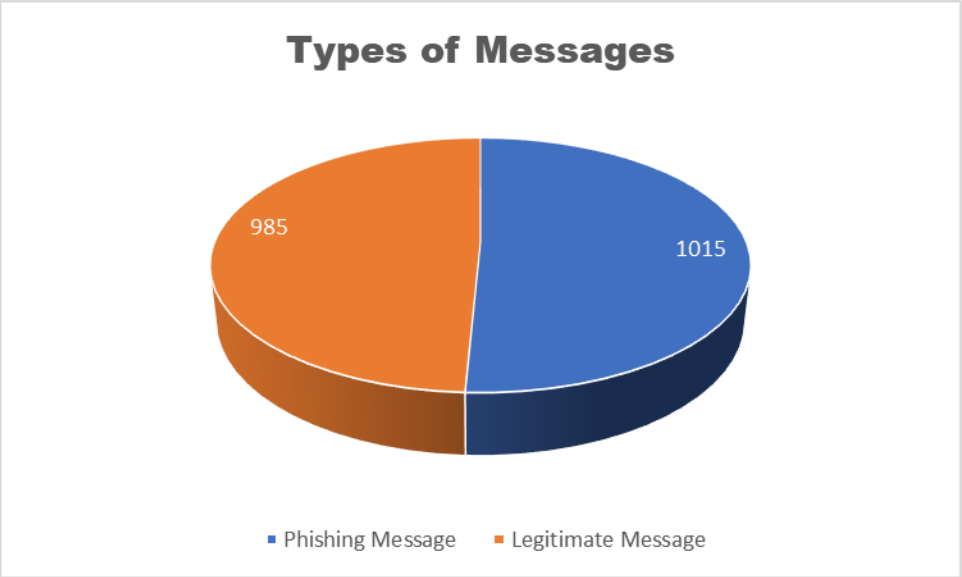


The elements in the above flowchart display components of a blockchain system which can be articulated as follows:

- ***Blockchain administrator***: The blockchain administrator is in charge of maintaining and setting up the blockchain system.
- ***Analytics:*** Blockchain data should be analyzed to pinpoint patterns and trends.
- ***Big data:*** Blockchain frameworks should be designed in such a way that they can store and process large volumes of data.
- ***Visualization***: Blockchain data ought to be visualized to make it easier to understand.
- ***Machine learning***: Machine learning should be employed to reinforce the security and efficiency of the blockchain systems.
- ***Cybersecurity:*** Blockchain frameworks are susceptible to cyberattacks, so it is pivotal to execute appropriate cybersecurity security measures to mitigate all possible threats.

5.2.1 Case Scenario

According to an experiment conducted by Ogdol & Samar (2018), where they blockchain simulation as a reference to pinpoint manipulated phishing attacks. Upon adding a new block successfully to the blockchain, a sequence of randomly produced messages, entailing both phishing and legitimate data, were inserted for testing purposes. The simulation acted as a mode to verify the conceptual application of blockchain technology in terms of pinpointing phishing content. Via the deployment of the simulation for an overall of 2000 iterations, the program documented the outcomes, enabling the measurement of the performance of the blockchain concept in combating phishing attacks. According to the 2,000 iterations, the following pie chart showcases that approximately 985 messages, representing 49.25% of the total, were produced as legitimate and valid messages by the test simulation. On the other hand, 1,015 messages, exemplifying 50.75% of the total, were detected as invalid and classified as phishing attacks.



In the executed simulation experiment, all 1,015 simulated phishing cyber-attacks were successfully interjected and mitigated. This result indicated that by deploying blockchain technology, the supply chain system accomplished a 100% detection and mitigation rate for the simulated phishing cyber-attacks. In the setting of this study, it is presumed that the theoretical framework suggested by Tapscott et al. in 2016 holds, since blockchain technology efficiently accomplished its role in terms of pinpointing phishing activities. As a consequence, this technology can be employed in various aspects of cybersecurity, including addressing the issue of phishing.

5.3 Benefits

5.3.1 Transparency and Trust

One of the noteworthy benefits of executing blockchain in the retail cybersecurity domain is the transparency it affords to the entire supply chain and transaction process. The immutable and decentralized nature of blockchain affirms that every transaction and interaction is documented on a visible shared ledger, to all authorized shareholders (Taylor et al., 2022). This transparency not only inspires trust among shareholders but also offers a verifiable trail of every item's journey, affirming customers' authenticity and ethical sourcing. Retailers can utilize this transparency to promote a better connection with customers who are increasingly conscious of the source of the products they purchase

5.3.2 Improved Security

According to Alotaibi (2019), blockchain's comprehensive security attributes significantly elevate the overall cybersecurity position of the retail sector. The decentralized aspect of blockchain makes it immune to conventional cyber-attacks, such as denial-of-service attacks or data breaches as there is no single point of failure. Furthermore, the cryptographic methods adopted in blockchain strengthen the confidentiality and integrity of data. For example, public and private keys in blockchain-oriented transactions add an extra shield of protection, making it hard for cyber criminals to forge and manipulate information. By employing blockchain, retailers can substantially minimize the risk of unauthorized access, and data breaches and fortify the security of both client and business data.

5.3.3 Efficiency and Cost Reduction

Blockchain presents cost reduction and efficiency by enhancing various processes within the retail framework. Smart contracts, designed to deploy instantly when specific conditionalities are met, diminish the need for mediators in transactions and agreements. This computerization not only elevates processes but also minimizes the costs related to compliance and manual verification (Miloslavskaya et al, 2022). In the supply chain, blockchain's capability to offer real-time visibility into the transportation of goods enhances overall efficiency, diminishes delays, and reduces errors. This elevated efficiency not only profits the retailer but also contributes to a more smooth and satisfactory experience for the end client.

5.4 Challenges

5.4.1 Scalability

As per Hasan (2023), despite its transformative capability, blockchain technology confronts scalability issues that prevent its widespread application in the retail sector. As the volume of transactions on a blockchain network escalates, the scalability of the

network becomes a noteworthy matter. Scalability issues can culminate in a slower transaction processing timeline and higher fees. Resolving scalability is pivotal for blockchain to achieve the demands of large-scale retail surroundings with millions of transactions happening daily. Endeavors are underway, with proceeding research and development concentrated on streamlining blockchain protocols and consensus mechanisms to enhance scalability while maintaining security.

5.4.2 Interoperability

Interoperability is another noteworthy challenge in the application of blockchain in the retail sector. Different blockchain forums may use distinct standards and protocols, making smooth communication between them hard. This lack of interoperability can prevent the development of a solid and interconnected blockchain ecosystem across the retail supply chain (Ali et al, 2022). Industry-wide coordination and the development of standardized procedures are paramount to combating interoperability challenges, ensuring that different blockchain networks can seamlessly exchange information and transactions.

6. Conclusion

In conclusion, the deployment of blockchain technology in retail cybersecurity has tremendous capabilities for streamlining supply chain integrity, safeguarding transactions, and protecting data. By leveraging blockchain, retailers can achieve end-to-end traceability and provenance, combat counterfeiting, and streamline vendor management processes. The adoption of blockchain-based payment mechanisms and fraud detection systems diminishes vulnerabilities and fortifies security in retail transactions. Besides, blockchain affords resolutions for consent management, data privacy, and safe data storage, ensuring the safeguarding of sensitive information. These deployments of blockchain technology in the retail sector pave the way for elevated efficiency, transparency, and trust among suppliers, retailers, and consumers. While challenges persist, such as scalability and regulatory considerations, the advantages of blockchain technology in retail cybersecurity are significant, making it a promising source for future innovation and enhancement in the industry.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Ali, İ., Jhanjhi, N. Z., & Laraib, A. (2022). Cybersecurity and blockchain usage in contemporary business*. In Advances in Information Security, privacy, and ethics book series* (49–64). https://doi.org/10.4018/978-1-6684-5284-4.ch003
[2] Alotaibi, B., (2019). Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things*: A Review, in IEEE Sensors Journal.* 10953-10971, doi: 10.1109/JSEN.2019.2935035.
[3] Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189–208. https://doi.org/10.1080/23270012.2020.1731721
[4] Hasan, M. R. (2022). Cybercrime Techniques in Online Banking. *Journal of Aquatic Science.* Retrieved from https://www.journal-aquaticscience.com/article_158883.html
[5] Hasan, M. R. (2023). NetSuite's Next Frontier: Leveraging AI for Business Growth. *International Journal of Science, Engineering and Technology,* 6. Retrieved from: https://www.ijset.in/volume-11-issue-6/
[6] Hasanova, H., Baek, U., Mu-Gon, S., Cho, K., & Kim, M. (2023). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management, 29*(2). https://doi.org/10.1002/nem.2060
[7] Miloslavskaya, N., Tolstoy, A., Budzko, V., & Das, M. (2022). Blockchain application for IoT Cybersecurity Management. In Chapman and Hall/CRC eBooks (141–168). https://doi.org/10.1201/9780429674457-7
[8] Ogdol, J. M. (2018). Enhancing cybersecurity through blockchain technology. https://www.academia.edu/81375019/Enhancing_Cybersecurity_Through_Blockchain_Technology
[9] Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147–156. https://doi.org/10.1016/j.dcan.2019.01.005
[10] Tezel, A., Papadonikolaki, E., Yitmen, İ., & Bolpagni, M. (2021). Blockchain Opportunities and Issues in the Built Environment: Perspectives on trust, transparency and cybersecurity. *In Structural integrity* (569–588). https://doi.org/10.1007/978-3-030-82430-3_24