[1]Aifang Zhang

[2]Lingling Zhang

[3]Weiwei Zhu

Safety and Security of E-commerce Transactions Based on Blockchain Technology

JES
Journal of Electrical Systems

Abstract: - The safety and security of e-commerce transactions are critical in today's digital landscape, where cyber risks abound. Blockchain technology's decentralized, transparent, and immutable ledger system offers a viable solution to these concerns. This study investigates the use of Distributed Ledger Technology (DLT), specifically Decentralized Identifiable Distributed Ledger Technology (DIDLT), in conjunction with the innovative Blockchain Consent Algorithm (BCA), to improve the safety and security of e-commerce transactions. Secure data storage and retrieval in e-commerce can be achieved by accurate digital signature production, key generation, blockchain building, and validation. This paper investigates how DIDLT, which combines decentralized identity management with blockchain technology, and BCA, a cutting-edge consensus algorithm designed for blockchain environments, work together to protect e-commerce transactions from identity theft, payment fraud, and data manipulation. This paper throws insight into DIDLT and BCA's potential to transform the e-commerce safety and security market by providing an in-depth analysis of their implementation. Using the incorporated DIDLT-BCA model significantly improves the safety effectiveness of the network, resulting in 98% security, shorter performance times of as much as 150 milliseconds, and mining times of up to 0.98 s.

Keywords: Blockchain, Cybersecurity, E-commerce, Distributed Ledger Technology (DLT), Blockchain Consent Algorithm (BCA)

I. INTRODUCTION

Cybersecurity is a top priority for individuals, organisations, and governments globally. The internet has enhanced global connectivity, but it has also led to greater security dangers that are becoming more complicated. E-commerce has grown to play a significant role in today's digital industry and economy. Online enterprises must regard security as a critical factor [1]. As the e-commerce business grows, a safe form of communication between customers and sellers becomes increasingly important. As a result, cyberattacks have unexpectedly increased globally. Network architecture security is the most significant threat to future e-commerce platforms [2][3]. To solve these difficulties, various technologies that use blockchain technology have emerged as intriguing alternatives. Blockchain, a decentralized and immutable ledger system, has built-in security and transparency characteristics. Specifically, the integration of the Decentralized Identifiable Distributed Ledger Technology-Blockchain (DIDLT-BC) method presents a revolutionary technique for ensuring the safety and security of e-commerce transactions [4].

The DIDLT-BC architecture brings together the ideas of decentralized identity management with the immutability and transparency of blockchain technology. Using cryptographic techniques, each member in the e-commerce ecosystem is granted a unique decentralized identification (DID), which acts as a secure and verified digital identity [5]. These DIDs are stored on a distributed ledger, providing tamper-proof identity verification and validation throughout the transaction process. Furthermore, the ledger's decentralized design reduces the need for intermediaries, lowering the risk of single points of failure and the possibility of fraudulent activity [6]. Smart contracts, which are programmable self-executing agreements put on the blockchain, automate transaction processes while maintaining adherence to preset norms and circumstances, thereby improving security and efficiency.

In this research, it's time at the DIDLT-BC procedures, as well as the consequences for e-commerce transaction safety and security. The Blockchain Consent Algorithm (BCA) is used to offer exceptional reliability as well as safety features. They explore its potential to reduce common dangers such as identity theft, payment fraud, and data

[1] *Corresponding author: (1)School of Electronic Commerce, Luoyang Vocational College of Science and Technology, Luoyang, Henan, China, 471000; (2)Graduate school, University of Perpetual Help Systems DALTA, Las Piñas City, Metro Manila 0900, the Philippines; 15896603377@163.com

[2] College of Philosophy, Law & Political Science, Shanghai Normal University, Shanghai, China, 201418

[3] Business school, Luo Yang Polytechnic, Luoyang, Henan, China, 471099

manipulation, fostering increased trust and confidence among customers and businesses alike. Researchers evaluate the DIDLT-BC framework's effectiveness and scalability in various e-commerce situations using a thorough examination of empirical research and real-world deployments. In addition, we analyze the constraints and limitations connected with its implementation and provide solutions to overcome these obstacles. This study refers to the continuing conversation about using blockchain technology to improve the safety and security of e-commerce transactions. By explaining the DIDLT-BC framework and BCA algorithm, they hope to provide useful insights for stakeholders looking to embrace creative solutions in the ever-changing field of digital commerce.

II. Literature Survey

This section covers recent studies on e-commerce security and blockchain integration, highlighting major findings and potential mitigating strategies.

Dahal, et al. [7]. This study examines how blockchain technology can secure e-commerce transactions and reduce fraud. This study examines how blockchain can improve transaction security and reduce fraud risks on various e-commerce platforms. The report demonstrates blockchain's potential for protecting e-commerce transactions. Blockchain records are immutable, which prevents tampering with transaction data. This property prevents fraudulent manipulation and ensures data integrity.

Deshmukh et al., [8]. This research provides a rigorous assessment of blockchain's core properties and architecture in e-commerce. Researchers proposed an application using blockchain technology as part of their investigation.

Treiblmaier et al. [9]. The goal of the research is to ask systematic questions about how blockchain affects e-commerce. This requires aligning e-commerce essentials with blockchain technology's disruptive potential. This article discusses the key elements of e-commerce and blockchain technology. Finally, a detailed research framework is developed for each question. The report examines the ramifications for academics and industry but also highlights several limits. Furthermore, it provides brief insights into future study directions.

Jiang et al., [10]. This study aims to address privacy concerns regarding the disclosure of sensitive information such as identities, addresses, and phone numbers during e-commerce transactions. They created a mechanism to safeguard privacy in e-commerce systems with blockchain technology. The researchers use zk-SNARKs, a cryptographic approach for securing user identities and validating ownership [11].

E.Cristina's [12]. paper on "Blockchain in e-commerce" provides a short definition of blockchain and highlights its significance. The core features of blockchain architecture are blocks, hashes, transactions, chains, and nodes. The report explains how blockchain technology works and its benefits for e-commerce, including security, cost-effectiveness, speed, tracking, reliability, and transparency.

Xuan T., Alrashdan T., and Al-Maatouk Q. (2020) [13]. The writers emphasize the importance of implementing blockchain technology into e-commerce. The study emphasizes the importance of blockchain in protecting sensitive business information, preventing data breaches, and preventing unwanted access to databases.

Bulsara, H. and Vaghela, P. [14]. found that traditional e-commerce faces several obstacles, including transaction processing, data security, order and payment procedures, and transparency issues. The study explores how blockchain technology might successfully address difficulties in e-commerce. Their research focuses on blockchain applications in payment systems, security, supply chain management, and e-commerce transparency [15]. The study concludes that blockchain technology promotes transparency and trust, providing customers with anti-fraud protection on e-commerce platforms.

III. Methodology

A. Blockchain in E-commerce

Blockchain technology enables secure and transparent digital information storage and transfer through decentralization and distribution. Blockchain technology uses a consensus mechanism to validate transactions and add them to a digital ledger. Blockchain technology uses linked blocks to create an immutable record of transactions, protected by cryptographic hashes. Blockchain's decentralized structure eliminates the need for a central authority, promoting transparency and security.

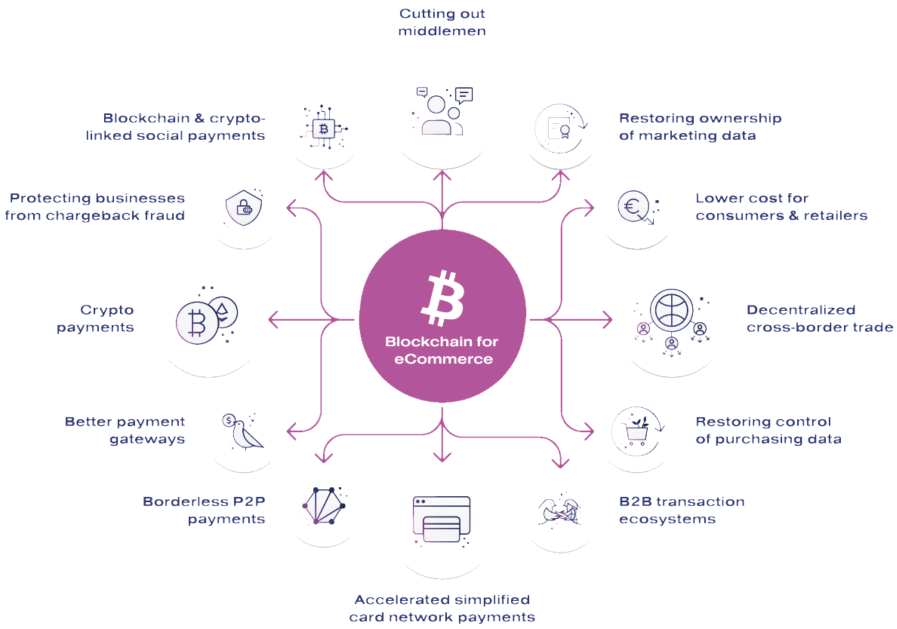
Cutting out middlemen
Blockchain & crypto-linked social payments
Restoring ownership of marketing data
Protecting businesses from chargeback fraud
Lower cost for consumers & retailers
Crypto payments
Blockchain for eCommerce
Decentralized cross-border trade
Better payment gateways
Restoring control of purchasing data
Borderless P2P payments
B2B transaction ecosystems
Accelerated simplified card network payments

Fig 1: Blockchain in E-commerce.

Blockchain technology improves e-commerce platforms' security, simplicity, and transaction speed. Users may conduct safer transactions and securely keep their digital assets. Blockchain offers a secure alternative to typical online transactions that rely on third-party validation, such as credit cards or banks. User data leaks pose a risk to traditional e-commerce systems. Integrating blockchain technology enhances the security of e-commerce systems. Blockchain's distributed ledger prevents tampering and ensures transaction integrity. Integrating blockchain-based applications has numerous benefits, including streamlining company operations, lowering costs, decreasing security threats, and increasing efficiency in Fig 1.

B. Proposed Methods

This section introduces the proposed Distributed Ledger Technology (DLT) based blockchain method for improving the security of e-commerce transactions. This study uses Decentralized Identifiable Distributed Ledger Technology-Blockchain (DIDLT-BC) technology and Rabin's digital signature generate technique to safeguard data saved in cloud-IoT systems. The optimization-based BCA is used to provide very high reliability while utilizing Blockchain Technology. Figures 2 illustrate the suggested method of operational movement.

This framework has the following stages:

- Digital signature generation
- Key pair generation
- Block construction using DIDLT
- Block validation and formation

Initially, the system is initialized with a set of IoT users, and the transaction is initiated with the digital signature-generating procedure. Based on this, authentication is carried out using the private and public key pairs. The DIDLT approach creates data blocks with headers, hash codes, timestamps, nonce messages, and transaction lists. After finishing blocks, validation was performed to ensure the accurate receipt of transaction IoT users.

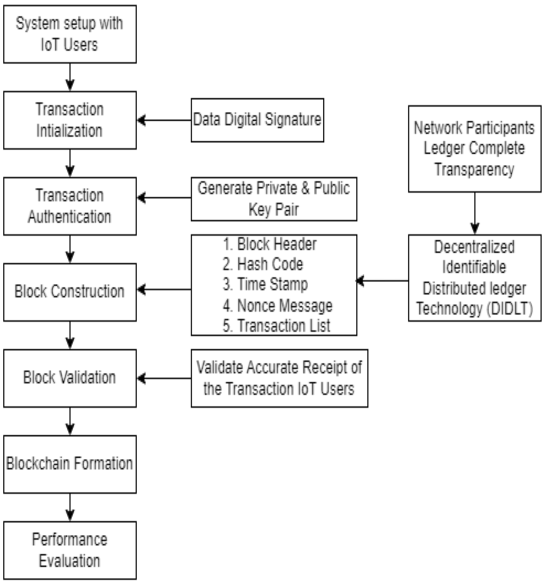
System setup with IoT Users
Transaction Intialization
Transaction Authentication
Block Construction
Block Validation
Blockchain Formation
Performance Evaluation
Data Digital Signature
Generate Private & Public Key Pair
1. Block Header
2. Hash Code
3. Time Stamp
4. Nonce Message
5. Transaction List
Validate Accurate Receipt of the Transaction IoT Users
Network Participants Ledger Complete Transparency
Decentralized Identifiable Distributed ledger Technology (DIDLT)

Fig 2: Workflow of the proposed DIDLT-BC model.

This framework provides high security for IoT data against malicious users. The suggested DIDLT-BC model has several advantages, including excellent reliability, resilience, reduced complexity and the amount of time and assured data confidentiality.

In the developed DIDLT-BC framework, transaction initiation is accomplished by the Rabin digital signature creation procedure. The authentication method uses a private and public key pair, ensuring safe data storage. The DIDLT approach is used to create data blocks with headers, hashes, timestamps, nonce messages and transaction lists. After the blocks have been built, the information is saved in the cloud with the information blocks. When the recipient accesses the data, the transaction signature is verified to validate the block. Additionally, BCA ensures reliability, security, and robustness. In this distributed system, the blockchain technique is mostly used for one value for data expression. A Blockchain Consent Algorithm (BCA) has been developed to improve dependability in blockchain technology by controlling faulty nodes with different hash values. Due to Blockchain technology. There is no centralized validation system, thus each new block must be checked at random using hash values. BCA provides additional benefits for this type of part. In comparison with different models, the BCA stands out for its ease of implementation, fast processing time, and reduced complexity.

1) Rabin Digital Signature and Key Generation: The transaction is initiated by the Rabin Digital Signature generation method after the system configuration has been simulated. This public-key cryptography technology enhances communication security between participants. This cryptography algorithm is lightweight and faster than others, making it ideal for developing intelligent applications. The following are the primary benefits of using this technique:

- It efficiently eliminates duplicate data storage.
- No additional parts are required.
- Computation efficiency has grown.
- Simpleness.

Because of these issues, the suggested study seeks to use the Rabin signature generation algorithm to improve information security.

2) Rabin Digital Signature and Key Generation: Participants in the network are assigned unique decentralized identifiers (DIDs), which are cryptographic keys that allow them to establish and verify their identities without the need for a centralized authority. Transactions are rigorously validated to ensure their validity and integrity by checking the digital signatures associated with each transaction, which are connected to each participant's DID. When creating a new block, these DIDs are included in the block header, together with transaction information and metadata such as timestamps and references to prior blocks. This inclusion enables the transparent identification of the persons involved in each transaction, hence improving accountability and traceability across the network. This inclusion enables the transparent identification of the persons involved in each transaction, hence improving accountability and traceability across the network. Before being added to the blockchain, created blocks are validated and agreed upon by network nodes, assuring transaction authenticity and order. Consensus mechanisms like as Proof of Work (PoW) and Proof of Stake (PoS) are used for this purpose. Once added to the blockchain, the block becomes an immutable record of transactions, with DIDs securely recorded in the block headers, resulting in a visible and tamper-proof audit trail. The DIDLT paradigm improves the security, transparency, and integrity of blockchain networks by incorporating decentralized identity management concepts into block construction, making them suited for many applications like as banking, supply chain management, and digital identity verification.

3) Block Validation: Block validation is an important step in blockchain technology that ensures the legitimacy and integrity of freshly manufactured blocks before they are added to the network. This procedure starts with methodically checking the transactions in the block, confirming the validity of the digital signatures linked with each transaction, and assuring compliance with consensus rules to prevent double-spending and maintain network protocol standards. Following individual transaction verification, the block goes through consensus verification, in which all network nodes agree on its validity using processes like Proof of Work or Proof of Investment. Once consensus is reached, the block's integrity is rigorously checked, including comparing the cryptographic hash of the block header to the network's difficulty target, confirming references to prior blocks to maintain chronological order, and ensuring timestamps are within acceptable ranges. If the block passes validation, it is disseminated to other nodes in the network to maintain consensus and prevent invalid blocks from being added to the blockchain.

4) Blockchain Consent Algorithm: Blockchain technology is utilized to create a single data value notation for distributed processes. To provide the highest level of consistency in blockchain technology, a Blockchain Consent Algorithm (BCA) has been developed. This provides solutions for operating many faulty nodes with varying hash values.

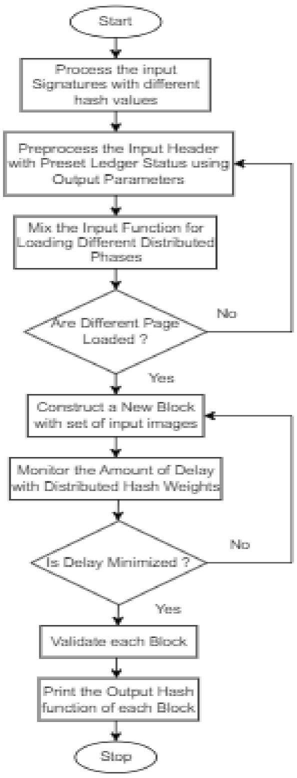
Start
Process the input Signatures with different hash values
Preprocess the Input Header with Preset Ledger Status using Output Parameters
Mix the Input Function for Loading Different Distributed Phases
Are Different Page Loaded ?
No
Yes
Construct a New Block with set of input images
Monitor the Amount of Delay with Distributed Hash Weights
Is Delay Minimized ?
No
Yes
Validate each Block
Print the Output Hash function of each Block
Stop

Fig 3: Steps in Blockchain Transactions Using Blockchain Consent Algorithm.

Because of the absence of a centralized validation method. In Blockchain technology, every new block must be verified with random hash values. BCA offers a further benefit in this function. BCA enables high-security characteristics by allowing for easy monitoring of current operations, even with unknown earls in the approach.

IV. Result And Discussion

This section evaluates the proposed blockchain model based on security, throughput, time, latency, and cost. The suggested methodology improves security, and accuracy and simplifies data access e-commerce transactions based on user roles. Figure 4 shows that the recommended security level has been validated. The model demonstrates the tremendous influence of security policies in e-commerce transactions. Comparing cutting-edge security models such as Stochastic Diffusion Search (SDS), Merkle Hashing Tree (MHT), Linear Elliptical Curve Digital Signature (LECDS) and Auth Privacy Chain.

Figures 6 confirm the digital signature validation times of the present RSA and developed Rabin Signature-generating techniques for various numbers of endorsers. Typically, signature creation and confirmation time are characterized by how much time spent making and confirming created digital signatures earlier permitting transactions.

Furthermore, all signers in a system can produce the signature concurrently, which can be utilized to validate one signer. Furthermore, signature generation.

Table 1: Security Evaluation.

Methods	**Nature**	**Identity with more than one signature**	**Tolerance for faults**	**Complexity of Time**	**Security as well as reliability**
CT	Central	No	1	O (1)	Poor
PHP	Central	No	1	O (1)	Poor
Sanda et al.	Distributed	No	2f + 1 ≤ n	O (n)	Medium
Duard et al.	Distributed	No	2f + 1 ≤ n	O (n)	Medium
Block Auth	Distributed	Yes	3f + 1 ≤ n	O (n2)	Strong
Proposed	Distributed	Yes	3f + 1 ≤ n	O (n2)	Very Strong

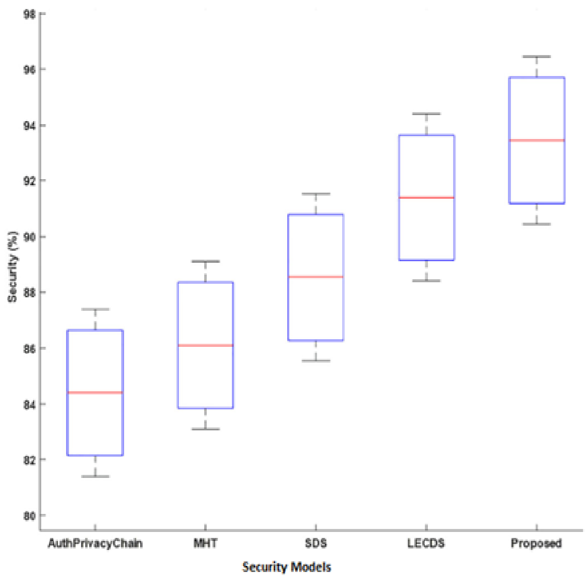

Fig 4: Analysis of the level of security (%).

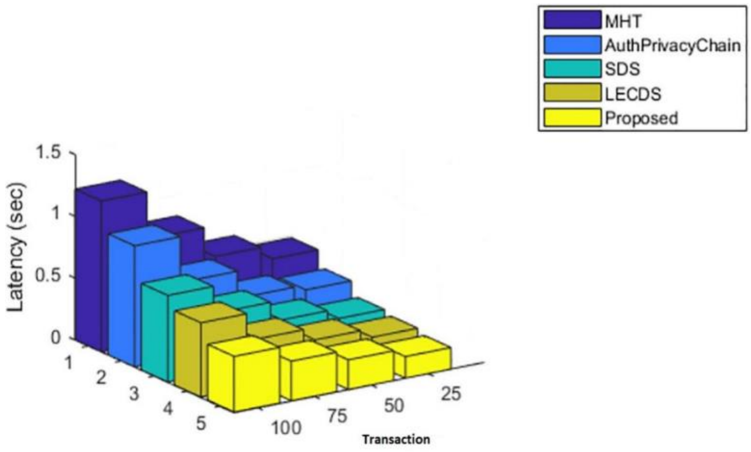

Fig 5: Latency.

Researchers analyze the throughput rate of current and proposed security methods depending on the total amount of transactions. The Rabin signature generation procedure can effectively reduce user time for searching, resulting in higher throughput. In comparison to existing approaches, the suggested DIDLT-BC could significantly increase throughput for all data transactions.

The performance times of current and developed security models for different bytes of data (1000, 3000, and 6000 bytes). The suggested system uses a decentralized blockchain paradigm based on Distributed Ledger Technology (DLT) to create a safe and secure channel of communication for each Connected user, enhancing data security. As a result, the DIDLT-BC technique outperforms other methods by requiring less execution time.

Figure 5 compares the average delay of current and planned models for increasing numbers of transactions. This investigation shows that the suggested DIDLT-BC has lower latency than alternative approaches. The proposed methodology requires only 0.5 seconds for 25 data transactions, compared to competing systems that need 0.6, 0.98, 1.22, and 0.7 seconds. The assessment shows that the suggested model's average latency is decreased compared to additional approaches.

To validate the signers, verification is performed consecutively. This evaluation considers keys with differing sizes, such as 1024, 2048, and 3027 bits. The Rabin digital signature system outperforms the RSA algorithm in terms of signature generation and verification speed.

Figure 7 compares the mining period of the current qTESLA + IPFS (Zhang et al., 2021) and proposed DIDLT-BC techniques with different block sizes. Based on this evaluation, mining time increases linearly with block size. After generating every block, the miner validates sequential information transactions. The study revealed that the mining time of the suggested approaches is more efficient and performs better than the current qTESLA model for all block sizes.

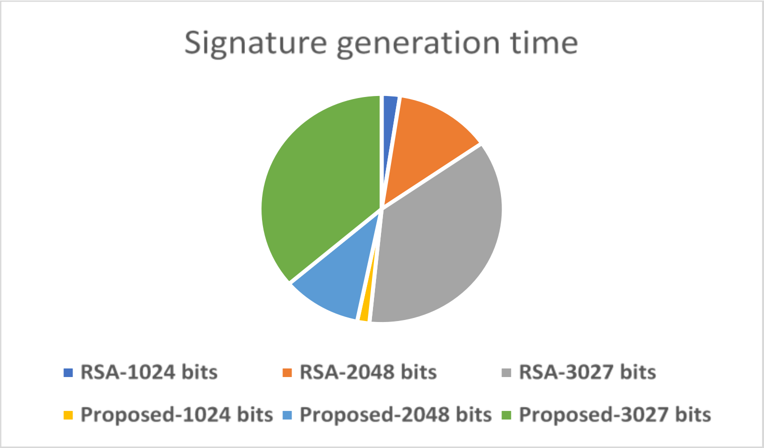

Fig 6: Signature generation time.

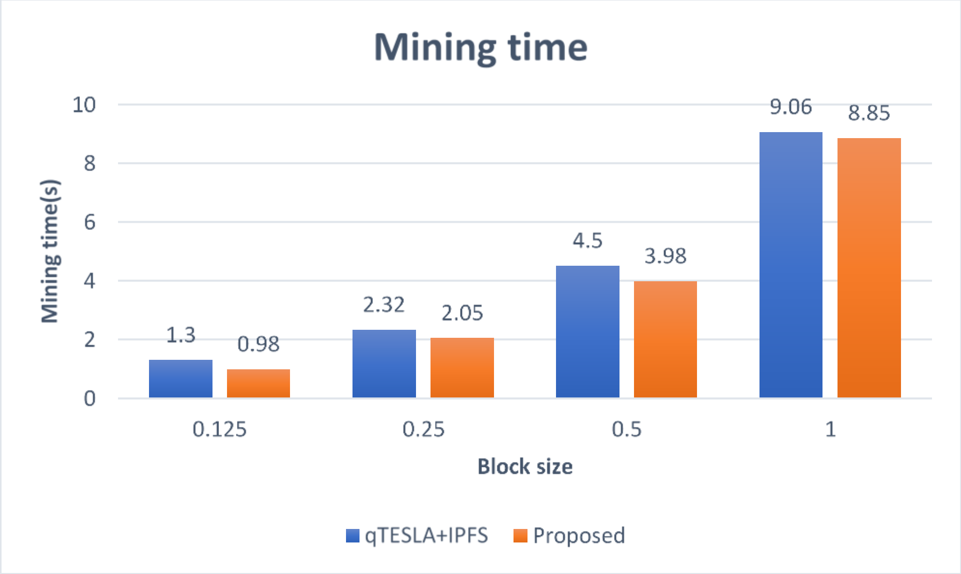

Fig 7: Mining time.

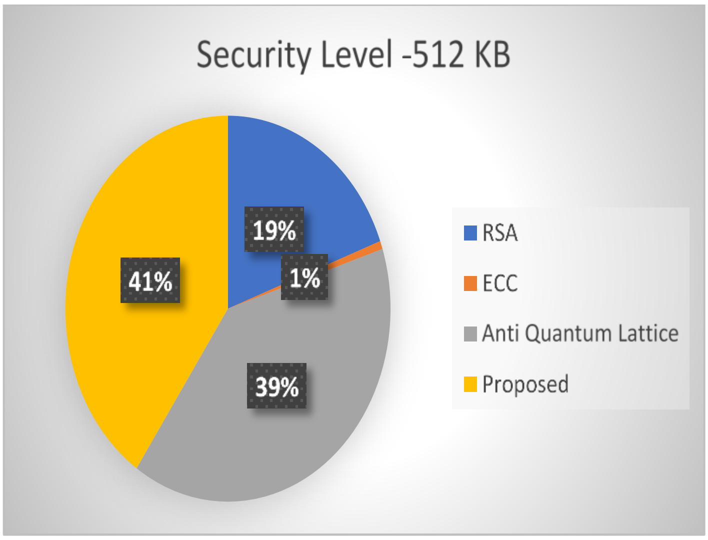

Fig 8: Security level.

Figure 8 assesses the current degree of security (Li et al., 2021) RSA, ECC, and anti-quantum lattices and shows DIDLT-BC models for the security of 512 KB.

This investigation estimated the level of security based on signature size, using the Rabin Signature Algorithm (RSA) at 28.7 KB, ECC at 1.024 KB, and anti-quantum lattice at 58.7 KB. The proposed technique effectively increased security to 60.2 KB, surpassing previous models. The security level for current and potential cryptography methods in terms of varied. Signature sizes in units of KB. The suggested methodology improves security for all signature sizes, outperforming other techniques.

Table 2: Security criteria for DIDLT.

Parameters	**Description**
Privacy	Very high
Security	Very high
Scalable	High
Authenticate	Yes
Confidential	Very high

Accuracy	Very high
Reliability	High
Exactness	High
Runtime	Low

The amount of time used by the proposed DIDLT-BC on key creation, encryption, and decryption. Analysis of key length (bits) reveals that the DIDLT-BC model uses less time for security procedures overall. Table 2 lists several safety measures that are efficiently met by the proposed DIDLT-BC approach.

V. Conclusion

The inclusion of the DIDLT-BC model marks a significant step forward in improving the safety and security of e-commerce transactions. By seamlessly merging decentralization, cryptographic identity management, and distributed ledger technology, DIDLT-BC addresses the long-standing issues of fraud, data breaches, and unauthorized access that plague traditional e-commerce platforms. DIDLT-BC offers tamper-proof identity verification and authentication throughout the transaction lifecycle by combining blockchain's transparent and immutable properties with decentralized identity management protocols. This comprehensive architecture not only protects transactions but also promotes confidence and openness in the digital marketplace. As blockchain technology evolves, frameworks like DIDLT-BC have enormous potential to transform the e-commerce sector. They lay the groundwork for a future in which transactions are handled with greater security, integrity, and transparency, resulting in a more robust digital economy. However, the full realization of DIDLT-BC benefits necessitates continued research, collaboration, and development. Addressing issues and maximizing the framework's capabilities will be critical to realizing its full potential, spurring more innovation, and fostering wider acceptance in the changing world of e-commerce. DIDLT-BC is an important step forward in the growth of e-commerce, providing a path to safer, more secure, and transparent transactions. DIDLT-BC has the potential to define the future of digital commerce by being dedicated and innovative, ushering in an era of trust, efficiency, and honesty.

References

[1] S. M. Alrubei, E. Ball, and J. M. Rigelsford, “A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer,” IEEE Access, vol. 10, pp. 18583–18595, 2022, doi: 10.1109/ACCESS.2022.3151370.

[2] R. Apau, F. Koranteng, S. G.-J. of Information, and U. 2019, “Cyber-crime and its effects on E-commerce technologies,” Acad. Apau, FN Koranteng, SA GyamfiJournal Information, 2019•academia.edu.

[3] A. Kharche, S. Badholia, and R. K. Upadhyay, “Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India,” Blockchain Res. Appl., p. 100188, 2024, doi: 10.1016/j.bcra.2024.100188.

[4] Rangga Gelar Guntara, Muhammad Naufal Nurfirmansyah, and Ferdiansyah, “Blockchain Implementation in E-Commerce to Improve The Security Online Transactions,” J. Sci. Res. Educ. Technol., vol. 2, no. 1, pp. 328–338, 2023, doi: 10.58526/jsret.v2i1.85.

[5] H. Guo, X. Y.-B. research and applications, and undefined 2022, “A survey on blockchain technology and its security,” ElsevierH Guo, X YuBlockchain Res. Appl. 2022•Elsevier.

[6] H. Taherdoost and M. Madanchian, “Blockchain-Based E-Commerce: A Review on Applications and Challenges,” Electronics (Switzerland), vol. 12, no. 8. 2023. doi: 10.3390/electronics12081889.

[7] S. B. Dahal, “Enhancing E-commerce Security: The Effectiveness of Blockchain Technology in Protecting Against Fraudulent Transactions,” Int. J. Inf. Cybersecurity, vol. 7, no. 1 SE-Articles, pp. 1–12, 2023.

[8] S. Deshmukh Bharati Vidyapeeth et al., “Blockart: The Blockchain Solution to E-Commerce,” Res. Deshmukh, S Chaudhary, Y Kulkarni, G Bhole, S Jadhav, T Suryawanshi, M KasarEur. Chem. Bull, 2023•researchgate.net, vol. 2023, pp. 5505–5513, 2023, doi: 10.48047/ecb/2023.12.si5a.0469.

[9] H. Treiblmaier and C. Sillaber, “The impact of blockchain on e-commerce: A framework for salient research topics,” Electron. Commer. Res. Appl., vol. 48, 2021, doi: 10.1016/j.elerap.2021.101054.

[10] Y. Jiang, C. Wang, Y. Wang, and L. Gao, “A Privacy-Preserving E-Commerce System Based on the Blockchain Technology,” in IWBOSE 2019 - 2019 IEEE 2nd International Workshop on Blockchain Oriented Software Engineering, 2019, pp. 50–55. doi: 10.1109/IWBOSE.2019.8666470.

[11] Z. Hongmei, “A Cross-Border E-Commerce Approach Based on Blockchain Technology,” Mob. Inf. Syst., vol. 2021, 2021, doi: 10.1155/2021/2006082.

[12] M. C. Enache, “Blockchain in Ecommerce,” Risk Contemp. Econ., vol. 1, no. 1, pp. 254–260, 2021, doi: 10.35219/rce20670532118.

[13] T. Xuan, M. Alrashdan, … Q. A.-M.-I. J. of, and U. 2020, “Blockchain technology in E-commerce platform,” Acad. Xuan, MT Alrashdan, Q Al-Maatouk, MT AlrashdanInternational J. Manag. 2020•academia.edu.

[14] H. Bulsara, P. V.-I. J. of Advanced, and U. 2020, “Blockchain technology for e-commerce industry,” Res. Bulsara, PS VaghelaInternational J. Adv. Sci. Technol. 2020•researchgate.net, vol. 29, no. 5, pp. 3793–3798, 2020.

[15] S. Selvarajan et al., “An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems,” J. Cloud Comput., vol. 12, no. 1, Dec. 2023, doi: 10.1186/s13677-023-00412-y.