International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0530
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3357 - 3363

Enhancing Cybersecurity with Blockchain Technology for Business Operations

Dr G A Pethunachiyar[1], Dr A Martina[2]
[1]Assistant professor, Dept. of Computer Applications, The Tamil Nadu Dr.Ambedkar Law University, Chennai-600113, Tamil Nadu, India.
[2]Assistant professor, Dept. of Management, The Tamil Nadu Dr.Ambedkar Law University, Chennai-600113, Tamil Nadu, India.
Emails: *apethu@gmail.com[1], martinamicheal@gmail.com[2]*

Abstract
The rapid growth of the digital economy has brought unprecedented advantages, enabling seamless transactions, real-time data exchange and global connectivity for the businesses. However, this digital expansion has also exposed businesses, governments and individuals to an evolving landscape of cyber threats. Traditional cybersecurity frameworks which rely heavily on centralized models are increasingly proving inadequate in the face of sophisticated cyber intrusions. Blockchain technology is a decentralized, cryptographically secure and immutable ledger system that introduces an innovative approach to cybersecurity. This research article examines the role of blockchain technology in enhancing cybersecurity, discussing its capabilities in securing online transactions, ensuring data integrity, preventing cyber threats and facilitating a proactive security mechanism against cyberattacks for businesses by integrating the CHIPS framework (Connect–Harness–Innovate–Protect–Sustain). This framework emphasizes the ability of blockchain to Connect stakeholders via trust less networks, Harness distributed ledgers to ensure data integrity, Innovate mechanisms for secure transactions, Protect digital assets with tamper resistant architectures and Sustain long term cyber resilience through scalable and adaptable systems. This study also highlights the effectiveness of this integration in securing digital transactions, thwarting cyberattacks and facilitating proactive cybersecurity strategies in business operations.

Keywords: *Blockchain; Business Operations; Cryptography; Cybersecurity; Data Integrity.*

1. Introduction
The swift growth of the digital economy has revolutionized organizational operations, facilitating real-time data sharing, effortless online transactions and operations on a global scale. Digital platforms have become pivotal to contemporary business ecosystems with almost all industries including finance, healthcare, government and supply chains by integrating it into interconnected cyber networks. As reported by the World Economic Forum (2024), more than 60% of global GDP is now digital or digitally influenced, propelling both economic expansion and cyber vulnerability [1]. Nevertheless, this rapid digitalization has concurrently resulted in a significant increase in cyber threats which urges towards the development of advanced, resilient security measures. In recent years, the occurrence and complexity of cyberattacks have increased dramatically. Ransomware incidents alone escalated by over 93% from 2021 to 2023, predominantly targeting critical infrastructure and business entities (IBM Security, 2023). AI-generated phishing, supply chain breaches and deepfake-based fraud have surfaced as significant security threats (McKinsey, 2024). Conventional cybersecurity framework predicated on centralized data storage, perimeter-based protection systems and password-based authentication are no longer adequate to combat sophisticated cyber criminals. Centralized systems

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0530
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3357 - 3363

create single points of failure rendering them highly susceptible to data breaches, insider threats and distributed denial-of-service (DDoS) attacks (NASSCOM, 2023). Blockchain technology has emerged as a viable alternative due to its decentralized, cryptographically secure and tamper-resistant framework. A blockchain operates as a distributed ledger where transactions are validated through consensus mechanisms and stored immutably across numerous nodes. This removes the dependence on centralized authorities by ensuring high levels of transparency, integrity and resilience. Research conducted by MeitY (2022) underscores blockchain's potential for securing digital identities and enhancing authentication systems. Furthermore, the immutability of blockchain presents significant challenges for attackers attempting to modify or erase transaction records without being detected. In light of the shortcomings of conventional security models, there is an urgent requirement for structured frameworks that facilitate the integration of blockchain into cybersecurity. This study employs the CHIPS framework as a strategic model for assessing the role of blockchain in business cybersecurity [2]. Even though, blockchain has numerous benefits, it has limitations while implementing in real-time Scalability problem exists when expanding network by adding nodes to the network (World Economic Forum, 2024). Finance and healthcare industries have regulatory mechanisms problem during its implementation. The smaller and startup companies face problem because of its execution cost (NASSCOM, 2023). Inspite of its disadvantages, the blockchain continues to be a revolutionary technology with the potential to transform digital security frameworks. This paper examines the potential of blockchain in enhancing cybersecurity through the CHIPS framework and evaluates case studies on blockchain-based security solutions which highlights implementation challenges and provides recommendations for organizations moving towards decentralized security models. By employing this comprehensive approach, the study can act as milestone in research on blockchain-enhanced cybersecurity within the digital economy.

2. Related Work

The growing complexity of cyber threats has exposed significant weaknesses in traditional centralized cybersecurity frameworks [3]. Contemporary attacks including AI-enhanced phishing, ransomware and supply chain breaches take advantage of deficiencies in standard methods thereby requiring the adoption of innovative technologies such as blockchain (IBM Security, 2023). The decentralized ledger of blockchain along with its cryptographic security and unchangeable transaction records presents considerable opportunities to increase cybersecurity by ensuring transparency, traceability and data management which are resistant to tampering (MeitY, 2022; Hossain et.al, 2024). Recent studies illustrate that the practical uses of blockchain in securing digital environments across various sectors. In the supply chain management, blockchain has proven to enhance cyber resilience by facilitating secure, real-time data exchange and incident recovery. Rezaeinejad.et.al2025 pointed out that blockchain reduces vulnerability to cyber threats by establishing distributed, verifiable records which increases trust among stakeholders. Industrial applications further substantiate blockchain's role in enhancing cybersecurity. Hossain et al. (2024) demonstrate that blockchain ensures immutable and traceable data flows in Industrial Cyber-Physical Systems (ICPS) protecting vital operational data from tampering and unauthorized access [4]. While the benefits of blockchain are evident, research has also highlighted significant challenges and vulnerabilities to address the necessity for effective threat detection and mitigation strategies within blockchain enabled supply chains. In spite of the benefits of blockchain demonstrated by numerous researchers, further investigation is required to establish a structured framework that facilitates the adoption of blockchain in organizations. The CHIPS framework plays a crucial role by providing a multidimensional approach to integrating blockchain with cybersecurity measures (Ayesha et al, 2024). Specifically, Connect evaluates how blockchain promotes decentralized trust among stakeholders by enabling secure peer-to-peer interactions (Rezaeinejad et al, 2025; Bayramova et al, 2021).

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0530
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3357 - 3363

Harness ensures that the immutable and auditable characteristics of blockchain data storage enhance operational transparency and integrity (Hossain et al, 2024; Fernandez-Carames et al, 2024). Innovate emphasizes automation through smart contracts and validation processes, which reduce human error and improve cybersecurity protocols (Al-Farsi et al, 2021; Shaikh et al, 2022) [5]. Protect highlights the inherent tamper-resistance of blockchain and its capacity to alleviate single points of failure (Islam et al, 2025). Sustain concentrates on the long-term resilience of blockchain systems by ensuring their adaptability to evolving cyber threats while maintaining regulatory mechanisms and operational efficiency (Ayesha et al, 2024).

3. Methodology

The methodology employed in this study is structured around a multi-layered integration of blockchain technology with the CHIPS framework to create a secure, resilient and scalable decentralized system. This approach conceptualizes the system into five interacting layers: Blockchain Layer, CHIPS Layer, Integration Layer, Application/Service Layer and Evaluation Layer. Each layer has its functionality to ensure its operational efficiency, data integrity and cybersecurity.

3.1. Blockchain Layer (Foundation Layer)

The Blockchain Layer serves as the foundation of the system. It establishes a decentralized ledger that links all participating nodes within the network. Transactions are cryptographically validated and recorded in an immutable manner by ensuring data integrity. Smart contracts are utilized to automate operational workflows, enforce business rules and reduce human errors [6]. This layer also integrates consensus mechanisms to securely validate transactions and ensure fault tolerance. By providing cryptographic security and tamper-resistant record-keeping, the Blockchain Layer guarantees that the fundamental reliability and trustworthiness of the system. CHIPS Layer (Security and Governance Layer)

3.2. The CHIPS Layer

This is built upon the foundational blockchain infrastructure to offer structured governance, security and operational control. Each component of CHIPS is aligned with the blockchain environment: Connect Specifies stakeholder access rights, network permissions and authentication protocols to facilitate secure collaboration. Harness organizes and manages blockchain data to enhance traceability, auditing and reliable information flow [7]. Innovate facilitates interoperability and integration across diverse platforms through standardized smart contracts and APIs. Protect enacts privacy-preserving mechanisms, continuous monitoring and intrusion detection to defend against cyber threats. Sustain develops governance protocols and scalability strategies.This layer guarantees that blockchain activities conform to established security standards, privacy obligations and operational efficiency objectives.

3.3. Integration Layer

The Integration Layer acts as the link between the Blockchain Layer and the CHIPS Layer. It synchronizes transaction data from the blockchain with the operational guidelines and security protocols set by CHIPS. This layer promotes workflow automation, cross-platform compatibility and the enforcement of access controls and privacy safeguards. Furthermore, it enables real-time monitoring and analytics by allowing stakeholders to continuously assess transaction validity, compliance and system efficiency [8].

3.4. Application/Service Layer

The Application Layer is the end-user environment where the integrated system provides concrete services. The use cases of this layer supply chain management, industrial IoT operations and digital services for government. Transactions are processed, smart contracts are activated and data transparency is upheld in real time. Dashboards and reporting tools offer stakeholders insights into operational performance, traceability and adherence to security standards. The Application Layer also relays information back to the Integration Layer to enhance workflows and bolster system sustainability [9].

3.5. Evaluation Layer (Cross-Layer Monitoring and Validation)

The Evaluation Layer operates across all layers to oversee performance, security and operational efficiency. System testing entails simulating real-world conditions with varying transaction volumes

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0530
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3357 - 3363

and stakeholder interactions. Stress tests and hypothetical attack scenarios evaluate the importance of the blockchain-CHIPS system against cyber threats and operational disruptions. The performance evaluation metrics are throughput, latency, data integrity, interoperability and scalability. These metrics are assessed and compared with traditional centralized systems. This evaluation guarantees that the system fulfils the goals of trust, transparency and efficiency by specifying the areas for improvement.

4. Application of Cyber Security Using Blockchain for Businesses

As the businesses go digital, the risks for the business are also on the rise. The businesses has always been looking out for technologies and spending crores of rupees on technologies to improve business, safeguard their businesses from frauds and other threats. Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) are some of the technologies that are invested into sometime back by the businesses (Agarwal & Gupta, 2024). Similarly, to protect their data and other assets from frauds, businesses were using the firewalls, anti-virus softwares etc. As the technologies grow and innovations bloom, the businesses are also implementing new better technologies replacing the older technologies. One such technology that found a wide application is block chain technology. The advantages mentioned in the previous section of the paper like decentralization, immutability, transparency and low cost makes it a desired option among the businesses. In this section of the paper the researcher is going to discuss about the areas where the block chain technologies can be applied in the businesses to improve the security [10].

4.1. Financial Transactions

Since the block chain technology is tamperproof and secure, lots of business transactions happening on the day to day basis among the businesses can be encrypted with this technology. Currently, the crypto currency transactions are using this block chain technology and few businesses like Subway and Burgerking have started accepting crypto currencies in Europe as payment (Weldon & Epstein, 2019). Hence, it has become the need of the hour for the governments to use blockchain technology for their currency transactions. Once the governments make use of blockchain technology for the currency transactions, almost all the businesses will use block chain technology for business transactions due to its security [11].

4.2. Data Transfer

Next to financial transactions, the most shared item among the businesses are the data. Lots of confidential information is transferred among businesses, businesses and consumers, businesses and government etc. These data can be shared using the block chain network with limited cost and increased security. For example, the banks and other financial service providers like depositories, insurance agencies collect and store the data of consumers. Financial transactions of the consumers can be accessed by the consumers more securely if it is stored using the block chain technology (Laroiya et al., 2020). Another example where the data can be stored securely using blockchain technology is in the healthcare sector. The hospitals and government health centers can store the large volumes of data using blockchain technology in a more secure manner. Blockchain technology can be used by the property registration offices. Generally, the property registration happened at the local registration office and the records are maintained by the government offices. The blockchain technology makes this process simple for the government offices making it decentralized and more secure and easily accessible and verifiable by the users. Wherever the data is used and stored the block chain technology can be adopted by the businesses [12].

4.3. Automated Contract Management Systems

The contracts that are encrypted in the blockchain technology, verifies the terms of the contract and executes the contract only when the stated conditions are met by the parties. These contracts do away with the human intervention like the employees of the firm or third party. Hence it is less prone to manipulation, human errors and data theft. This offers more secutity to the business contracts.

4.4. Raw Materials Procurement

Many businesses are integrating Block chain technology in the procurement processes. The data of

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0530
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3357 - 3363

the different suppliers, their quality, grading, rates and cost of transportation kind of information can be collected and stored in the block chain networks so that the purchase department can use these data for the effective purchase decisions (Rijanto, 2021). This data is secure and is not susceptible for cybersecurity threats over traditional ERP platforms which uses old security features. This is effectively used by IBM in their supply chain management process.

4.5. Human resource management

The employee records like recruitment, training and performance appraisal reports and disciplinary records can be kept in the block chain technology for the top level HR executives to take decisions and for the employees to have a feedback on their performances. The qualification and other records of the employees can also be stored in a more secured manner using block chain technology [13].

5. Advantages of Integration Blockchain with Chips

The combination of blockchain technology and the CHIPS framework offers organizations a comprehensive strategy for enhancing digital security. A key advantage is the improved protection of data. The distributed ledger of blockchain guarantees that all records are secure from tampering and are cryptographically protected while the governance protocols based on CHIPS implement access controls and operational oversight thereby decreasing the chances of breaches and unauthorized alterations. This integration enhances operational visibility. Organizations can track transactions and data flows among various stakeholders in real time by facilitating the swift identification of discrepancies or irregularities. This feature not only fosters trust among partners but also allows for prompt action in response to operational risks. Additionally, the automation of smart contracts enables routine business activities such as executing contracts, granting approvals and transferring assets o be initiated automatically once specific conditions are satisfied. This reduces reliance on manual processes, lessens the potential for human error and guarantees consistent execution of processes. Another notable benefit is the interoperability across platforms. The CHIPS framework facilitates smooth interactions between blockchain networks and existing enterprise systems and digital services. This enables organizations to implement blockchain solutions without the need for a complete structure. This integration encourages long-term adaptability and continuity. The decentralized structure of blockchain combined with CHIPS-directed governance and sustainability initiatives allows organizations to efficiently scale their operations respond to changing security threats and sustain uninterrupted business activities. This methodology shifts cybersecurity from a reactive stance to a proactive and strategically integrated capability [14].

6. Challenges and Limitations

There are numerous advantages gained by the organization after the integration of blockchain within the CHIPS framework. There are some limitations faced regardless of its benefits. Scalability is a significant issue particularly for networks that manage extensive transaction volumes which may lead to a decrease in processing speed and an increase in energy consumption which affects the efficiency of its execution. The technical complexity is another major issue because the effective implementation needs a deep understanding of blockchain technology, cryptography and network management which is a major challenge for smaller industries or industries with limited IT Personnels. The next issue is the legal compliance as different regions require different data privacy techniques. This integration also leads to deployment cost problem; this integration cannot be adopted with existing configuration [15 - 18].

7. Future Directions

The blockchain technology with the CHIPS framework leaves numerous pathways for both research and practical application. The blockchain and artificial intelligence (AI) can be used combinedly for the prediction of threat detection, automate the identification of anomalies and enhance decision-making processes by improving proactive cybersecurity measures. The broader adoption of blockchain-CHIPS in sectors such as Industrial IoT, smart manufacturing and logistics can lead to enhanced operational reliability, secure real-time data exchanges and the optimization of intricate

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0530
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3357 - 3363

workflows. The blockchain enabled decentralized identity management systems to enhance user privacy, mitigate identity fraud and ensure secure authentication across various digital platforms. The organizations can utilize blockchain not just as a technological revolution but as a strategic enabler for adaptive, resilient and future-oriented cybersecurity.

Conclusion

The adoption of blockchain technology in cybersecurity is not an option. it is a necessity in today's digital economy. Its ability to provide decentralized, trustless security mechanisms makes it a powerful tool against cyber threats. The CHIPS framework provides a roadmap for organizations to integrate blockchain into digital security strategies, ensuring scalability, adaptability and resilience. By focusing on connectivity, security, innovation and sustainability, Blockchain will continue to redefine how cybersecurity threats are managed in the digital economy. Governments, enterprises and security firms must collaborate to implement blockchain-based cybersecurity frameworks by ensuring future-proof protection against evolving cyber threats. While challenges like scalability, regulatory compliance and implementation costs exist, blockchain's long-term benefits outweigh the initial hurdles. The future of cybersecurity is no longer about reacting to cyber threats. It's about anticipating, preventing and neutralizing them before they occur. Blockchain offers a transformational shift in how digital security is managed, eliminating vulnerabilities and inherent in centralized systems.

References

[1]. IBM Security. (2023). IBM X-Force threat intelligence index 2023. IBM. https://www.ibm.com/security/data-breach/threat-intelligence

[2]. MeitY. (2022). Blockchain in government and enterprise: Enhancing digital security. Ministry of Electronics and Information Technology, Government of India. https://www.meity.gov.in/writereaddata/files/Blockchain_Report_2022.pdf

[3]. NASSCOM. (2023). Cybersecurity in India: Market trends and insights. NASSCOM Research Reports. https://nasscom.in/knowledge-center/publications/cybersecurity-india-market-trends-and-insights

[4]. World Economic Forum. (2024). Global risks report 2024. World Economic Forum. https://www.weforum.org/reports/global-risks-report-2024

[5]. UNCTAD. (2023). Digital economy report 2023: Blockchain and sustainable development. United Nations Conference on Trade and Development. https://unctad.org/webflyer/digital-economy-report-2023

[6]. Ben Hmaida, M. A. (2024). The Role of Blockchain Technology in Enhancing Cybersecurity: Emerging Trends and Future Perspective. Journal of Reproducible Research, 2(2), 144–152. Retrieved from https://journalrrsite.com/index.php/Myjrr/article/view/83Siam,

[7]. Siam, M. K., Saha, B., Hasan, M. M., Hossain Faruk, M. J., Anjum, N., Tahora, S., Siddika, A., & Shahriar, H. (2025). Securing Decentralized Ecosystems: A Comprehensive Systematic Review of Blockchain Vulnerabilities, Attacks, and Countermeasures and Mitigation Strategies. Future Internet, 17(4), 183. https://doi.org/10.3390/fi17040183

[8]. Hossain, M. I. et.al (2024). Enhancing data integrity and traceability in Industry Cyber-Physical Systems through blockchain technology: A comprehensive approach. arXiv preprint. https://arxiv.org/abs/2405.04837

[9]. Rezaeinejad, S., Rayman, K., Sauser, B. et al. How can Blockchain Contribute to Cyber Resilience? Supply Chain Analytics and Digitalization Benefits. Inf Syst Front (2025). https://doi.org/10.1007/s10796-025-10651-w

[10]. Islam, M. J., Islam, S., Hossain, M., Noor, S., & Islam, S. M. R. (2025). Securing Blockchain Systems: A Layer-Oriented Survey of Threats, Vulnerability Taxonomy, and Detection Methods. Future Internet, 17(5),205.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0530
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3357 - 3363

https://doi.org/10.3390/fi17050205

[11]. Bayramova, A., Edwards, D. J., & Roberts, C. (2021). The Role of Blockchain Technology in Augmenting Supply Chain Resilience to Cybercrime. Buildings, 11(7),283. https://doi.org/10.3390/buildings11070283

[12]. Fernandez-Carames, T. M., Blanco-Novoa, O., Froiz-Miguez, I., & Fraga-Lamas, P. (2024). Towards an autonomous Industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability. arXiv https://arxiv.org/abs/2402.00709

[13]. Ayesha, I., et al. (2024). A review on blockchain impact in cybersecurity: Current applications, challenges, and future trends. International Journal of Scientific Research in Engineering & Management (IJSRA)

[14]. Shaikh, A. K., Al-Alawi, L. R., Al-Busaidi, R., & Shaikh, A. (2022). Towards security enhancement of blockchain-based supply chain management. arXiv https://arxiv.org/abs/2209.04917

[15]. Agarwal, P., & Gupta, A. (2024). Harnessing the power of enterprise resource planning (ERP) and customer relationship management (CRM) systems for sustainable business practices. International Journal of Computer Trends and Technology, 72(4), 102-110.

[16]. Weldon, M. N., & Epstein, R. (2019). Beyond Bitcoin: leveraging blockchain to benefit business and society. Transactions: The Tennessee Journal of Business Law, 20(3), 837.

[17]. Laroiya, C., Saxena, D., & Komalavalli, C. (2020). Applications of blockchain technology. In Handbook of research on blockchain technology (pp. 213-243). Academic press.

[18]. Rijanto, A. (2021). Blockchain technology adoption in supply chain finance. Journal of Theoretical and Applied Electronic Commerce Research, 16(7), 3078-3098.