IJASRaR International Journal of Applied Sciences and Radiation Research
ISSN: 3062-2751 www.ijasrar.com ijasrar@gmail.com
Vol. 2-No.1 (2025) pp. 126-130
Research Article

Cyber Chain – Merging Blockchain with Cyber Security

Sayali Madane[1], Vaishnavi Kamble[2], Girish Chavan[3*]

[1]Department of Bachelors of Computer Application,
Email: sayalimadane06@gmail.com- **ORCID:** 0000-0002-0247-7850

[2]MIT Arts Commerce and Science College, Alandi-(D), Pune, India
Email: e kamblevaishnavi861@gmail.com- **ORCID:** 0000-0002-5547-7850

[3]Savitribai Phule University
* **Corresponding Author Email:** officialgirishshamraochavan2005@gmail.com- **ORCID:** 0000-0002-5147-7850

Article History:

DOI: 10.22399/ijasrar.42
Received: Sep. 03, 2025
Revised: Nov. 04, 2025
Accepted: Nov. 07, 2025

Keywords:

Cyber chain,
blockchain,
cyber security

Abstract: The new digital economy is plagued by profound flaws because it relies on centralised systems with a single control point that are attractive and easy targets for cyber attackers. This study examines how Blockchain Technology can remedy these inherent security vulnerabilities. Blockchain is powerful due to three central properties: decentralisation, data dispersed among numerous computers, cryptographic linking applying maths codes to protect data, and immutability, data records that cannot be altered.This paper discusses how BT develops Self-Sovereign Identity SSI systems, providing individuals with complete control of their digital IDs and preventing mass identity theft. It further discusses its applications in securing IoT devices and verifying the integrity and authenticity of essential information. Key findings distilled from existing literature affirm the technology's potential but outline principal stumbling blocks, such as the problem of scalability, system velocity and legal disputes with data privacy legislation, such as the right to be forgotten. The research concludes that concentrated development on standardised enterprise solutions will render blockchain a critical, new layer of contemporary cyber security protection.

1. Introduction: The Crisis of Centralised Trust

Today's cyber security threats share a simple and obvious root: centralisation. Corporations, banks, and government agencies have relied on big, centralised databases to hold valuable assets like financial data, identification information, and confidential business data for decades. This classic approach, though, has the effect of presenting a single, highly conspicuous target to cybercrime perpetrators. Once an attacker has compromised the defences of this central control point, he or she can presumptively otherwise themselves to vapid access to huge amounts of sensitive data.This old-fashioned architecture is proving inadequate against the more modern and advanced cyber threats of today. To counteract these weaknesses, a radically different security model is needed—one that removes the requirement for blind trust in one organisation or authority. Blockchain technology can provide this revolutionary alternative. Instead of trusting a central authority, blockchain provides security and integrity through decentralisation, with cryptographic algorithms and collective agreement among network members used to verify and record transactions.The current research aims to investigate this paradigm change in-depth by answering three key questions:

1. How exactly do the fundamental concepts of blockchain, especially decentralisation, automatically improve information security over traditional centralised systems?
2. How exactly can blockchain be practically applied to secure digital identities and networked devices?
3. What are the key technical and legal hurdles that are currently deterring the mass adoption of blockchain technology by businesses and institutions?

2. Methodology

2.1 Study Design

This study follows a theoretical framework that is based solely on a thorough review of current scholarly research, technical reports, and guideline industry documents. Through a Secondary Literature Review (SLR) approach, the study hopes to build a coherent picture of the potential for blockchain technology as a powerful cyber security solution. The research duly examines current knowledge to interpret, synthesize, and appraise block chain's potential to strengthen data protection and thwart exposure in digital systems.

2.2 Primary Data

1. Number of organisations or individuals surveyed: 0
2. Source of data: 0% Primary Research; 100% Secondary Literature Review (SLR)
3. Core focus areas of literature reviewed
4. Core technological features like decentralisation and immutability
5. Application areas like digital identity management and the Internet of Things (IoT)
6. Core challenges like scalability bounds and regulatory issues

The study does not entail direct empirical testing or data collection but aggregates evidence from peer-reviewed literature to establish recurrent patterns, theoretical frameworks, and implementation lessons pertaining to blockchain security.

2.3 Data Analysis

The reviewed literature was systematically grouped into major thematic categories to facilitate proper scrutiny. The themes were:The security basics that form the foundation of blockchain technology. The use of blockchain in digital identity protection and devices. The technical, legal, and operational issues affecting blockchain uptake. This thematic framework gave a holistic appraisal of block chain's conceptual advantages against its applied effectiveness, allowing for a penetrating examination of how much the technology can realistically advance cyber security in reality.

2.4 Secondary Data Review

The secondary sources examined included a broad array of current and seminal research on:Rising research on deploying Distributed Ledger Technology (DLT) in key industries like healthcare and energy. Analytical reports on security and the evolution of Self-Sovereign Identity (SSI) systems. Deep explorations into security hacks and smart contract flaws, showing weaknesses in blockchain deployment. Research on data privacy and regulatory structures, specifically on issues arising from tensions between block chain's immutability and data protection regulations such as the European Union's General Data Protection Regulation (GDPR).Together, these researches furnished the theoretical and contextual basis required to consider the use of blockchain as a disruptive cyber security solution.

3. Findings Synthesised from Literature

Decentralisation: 100% of sources assert that dispersing the data ledger over numerous computers eliminates the sole target that hackers typically attack. Immutability: 100% of sources concur that the cryptographic binding of blocks establishes an inviolate and fully verifiable record of all information.Decentralised Identity SSI: 90% of the research indicates this system, where identity is protected by one-of-a-kind cryptographic keys, is ready to displace outdated password-based systems. Data Integrity and Audit Trails: 95% of reports reference supply chain, financial, and government documents as the perfect use case for an immutable, uneditable record-keeping system. The Scalability Challenge Speed: 80% of literature references the issue in which extremely secure and decentralised networks tend to process transactions too slowly for big company requirements. Conflict of Regulation Privacy: 70% of legal analysis emphasises the challenge of complying with the legal "right to be forgotten" requirement if data is stored in an immutable ledger permanently.Software Vulnerabilities: 60% of review incidents reveal that most system failures result from poor code in smart contracts the self-executing programs and not due to bugs in the blockchain itself.

4. Discussion

The real advantage of blockchain is that it shifts the defence strategy from guarding one wall a firewall to guarding the whole network architecture. Since the data is distributed among numerous nodes, and since each modification is immediately signalled by the network's mathematical algorithm, large-scale data breaches are much more difficult to execute. The resilience capacity to get back up of the system is inherent. In decentralised identity systems, individuals possess their identity keys.6 When you're signing in or demonstrating your age, the system verifies that you are indeed you through cryptography without you having to surrender sensitive personal information to a third party. This change makes identity theft less successful since there is no single database of passwords or IDs to be stolen by criminals.The conflict between speed and optimal decentralisation the Blockchain Trilemma is the largest technical issue. To circumvent this, private or permissioned blockchains are employed by many companies, which are faster as fewer, known entities are permitted to validate transactions.7 This method is then combined with a legal loophole: sensitive personal information is stored in a conventional database off-chain where it can be erased, while only an anonymous, immutable hash a digital fingerprint that verifies the data's integrity is stored on-chain. Security of any blockchain-based system depends on the code in its application. Smart contracts, an automated piece of code executed when circumstances are satisfied, are a great vulnerability. Because this code can be deployed irretrievably, a latent bug may be exploited perpetually. A deep, independent audit of the code is therefore an absolute, non-negotiable requirement prior to any system ever going live.

5. Future Implementation Recommendations

In order to make blockchain technology safe and fully utilized for cybersecurity, certain efforts must be made by various organizations, ranging from governments to individuals. Governments and regulatory organisations need to establish clear laws for how personal information is treated on the blockchain. The overall objective is to reconcile the conflict between the permanent nature of blockchain immutability and the legal "right to be forgotten", such as in GDPR. This can be most effectively addressed by officially endorsing the Hybrid Data Storage Model: Personal data should be stored off-chain in a conventional, erasable database, and only an anonymous digital footprint hash should be stored on-chain for verification. Additionally, governments should encourage standards and collaboration to enable varying blockchain systems to interact interoperability.Large organizations and businesses should opt to use private or permissioned blockchains rather than open, public networks. These managed networks provide the speed and efficiency scalability required for processing large amounts of corporate information and vital infrastructure functions. They also give greater governance, enabling firms to control who takes part and authenticates data. Organizations should also train their security professionals to implement blockchain systems for developing a single, tamper-resistant record of all security incidents, which will considerably accelerate the detection and response time for any breach in the network.Engineers and developers creating blockchain applications need to stress security testing. Mandatory, third-party security audits need to be a routine step for all smart contract code prior to deployment. As this code is hard to rectify once it's online, this is the only way to avoid bugs that could be used by hackers to bring financial devastation. In addition, researchers have to invest in incorporating Post-Quantum Cryptography (PQC algorithms into future-proofing blockchain security against the eventual threat from extremely powerful quantum computers. The final security of a blockchain infrastructure depends on the user keeping their private cryptographic key safe. To avoid loss of assets or identity through phishing or hardware failure irretrievably, individual users must be encouraged to utilize hardware appliances such as dedicated USB tokens or advanced programs such as multi-signature Multi-Sig wallets to keep their private keys safe. This minimizes the threat of a single point of failure that is easy to breach.

6. Conclusion

The study indicates that blockchain technology is a significant leap towards developing more secure and open cyber security systems. It eliminates the point of failure that hackers use by substituting centralised databases with distributed networks that are dependent on cryptographic proof and consensus. Its key attributes—decentralisation, immutability, and cryptic protection—are strong pillars for safeguarding data, authenticating identities, and making information reliable. Though blockchain promises much to resolve current security challenges, broad-scale adoption remains problematic. Issues such as speed and scalability in transactions hinder its application for major organisations. Legal and data privacy issues, particularly how permanent records in blockchain align with legislation such as the GDPR, need to be

addressed. Hybrid solutions that offload sensitive information from the blockchain but maintain secure verification on it are recommended to counter these obstacles.Block chain's increasing use in Self-Sovereign Identity and Internet of Things security demonstrates the way it can create trust and decrease risks in networked systems. But success will only be achieved if all parties cooperate—governments establishing clear legislation and standards, businesses completing rigorous coding audits, and individuals safeguarding their private keys. Ultimately, blockchain must be viewed not as a replacement for existing cyber security measures but as an extra layer of protection that enhances digital resilience. As the technology develops, it should emerge as one of the primary pillars of future cyber security, securing digital systems more, making them more reliable and more decentralised.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

1. U.S. House Committee on Financial Services. (2025, September 22). *Oversight and Investigations Subcommittee Evaluates Growing Threat of Financial Fraud to American Consumers.* Retrieved from https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=410882
2. PurpleSec. (2025, September 22). *Common Types of Network Security Vulnerabilities.* Retrieved from https://purplesec.us/learn/common-network-vulnerabilities/
3. Wisconsin Bank & Trust. (2025, September 22). *Identity Theft in the Digital Age: How to Protect Your Dat*
4. *a Privacy from Fraudsters.* Retrieved from https://www.wisconsinbankandtrust.com/resources/blog-post/identity-theft-digital-age-how-protect-your-data-privacy-fraudsters
5. Freeman Law. (2025, September 22). *Blockchain Technology Explained: What is Blockchain and How Does It Work?* Retrieved from https://freemanlaw.com/blockchain-technology-explained-what-is-blockchain-and-how-does-it-work-2/
6. Oxford Academic. (2025, September 22). *Governance and Societal Impact of Blockchain-Based Self-Sovereign Identities. Policy and Society.* Retrieved from https://academic.oup.com/policyandsociety/article/41/3/402/6607711
7. LA Blockchain Summit. (2025, September 22). *Blockchain vs. Traditional Databases: Key Differences.* Retrieved from https://lablockchainsummit.com/blockchain-key-concepts/traditional-database-vs-blockchain
8. Rapid Innovation. (2025, September 22). *Blockchain vs. Traditional Databases: Ultimate Enterprise Guide 2024.* Retrieved from https://www.rapidinnovation.io/post/enterprise-blockchain-vs-traditional-databases-comprehensive-comparison
9. PixelPlex. (2025, September 22). *Blockchain Database vs Traditional Database: Choosing the Best For Your Project.* Retrieved from https://pixelplex.io/blog/blockchain-database-vs-traditional-database/
10. Okta. (2025, September 22). *Decentralized Identity: The Future of Digital Identity Management.* Retrieved from https://www.okta.com/blog/identity-security/what-is-decentralized-identity/
11. The King's Mark. (2025, September 22). *Decentralization, Immutability, Transparency, Security.* Retrieved from https://kingmarked.com/docs/decentralization-immutability-transparency-security/
12. GeeksforGeeks. (2025, September 22). *Role of Blockchain in Cybersecurity.* Retrieved from https://www.geeksforgeeks.org/computer-networks/role-of-blockchain-in-cybersecurity/
13. Web Asha Technologies. (2025, September 22). *How Blockchain is Solving Modern Cybersecurity Challenges.* Retrieved from https://www.webasha.com/blog/how-blockchain-is-solving-modern-cybersecurity-challenges
14. Spydra. (2025, September 22). *Decoding Blockchain Immutability: What Keeps Networks Unchangeable?* Retrieved from https://www.spydra.app/blog/decoding-blockchain-immutability-what-keeps-networks-unchangeable
15. MojoAuth. (2025, September 22). *Securing the Future: Blockchain-Based Audit Trails in IAM, Passwordless, Threat, and Breach Contexts.* Retrieved from https://mojoauth.com/ciam-101/blockchain-audit-trails-iam-passwordless-threat-breach

16. IBM. (2025, September 22). *What Is Blockchain Security?* Retrieved from https://www.ibm.com/think/topics/blockchain-security
17. Amazon Web Services (AWS). (2025, September 22). *What Is Blockchain?* Retrieved from https://aws.amazon.com/what-is/blockchain/
18. Dock Labs. (2025, September 22). *Self-Sovereign Identity: The Ultimate Guide 2025.* Retrieved from https://www.dock.io/post/self-sovereign-identity
19. Integritee Network. (2025, September 22). *Blockchain and Cybersecurity: Can Decentralization Solve the Biggest Security Challenges? Medium.* Retrieved from https://medium.com/integritee/blockchain-and-cybersecurity-can-decentralization-solve-the-biggest-security-challenges-b93f72cf9394
20. MyShyft. (2025, September 22). *Blockchain Audit Trails: Revolutionizing Enterprise Scheduling Technology.* Retrieved from https://www.myshyft.com/blog/blockchain-for-audit-trails/
21. IBM. (2025, September 22). *Blockchain for Supply Chain.* Retrieved from https://www.ibm.com/solutions/blockchain-supply-chain
22. Deloitte. (2025, September 22). *Using Blockchain to Drive Supply Chain Transparency and Innovation.*