International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Blockchain Technology and Cyber Security

Dr. Vishal Bharvesh

Abstract

In the digital age, cyber security has become a major concern for governments, organizations, and individuals. The rapid growth of data sharing and storage increases risks such as data breaches, identity theft, ransomware, and financial fraud. Traditional centralized systems are vulnerable, as a single point of failure can lead to massive damage.

Blockchain offers a strong alternative with its decentralized structure, immutability, and transparency, making systems harder to manipulate and more trustworthy. This paper explores its role in three key areas: securing digital transactions, protecting digital identity, and safeguarding data from tampering. It also examines real-world applications, challenges such as scalability and regulation, and future research directions.

The study concludes that blockchain extends beyond cryptocurrency, providing a powerful tool to strengthen cyber security and build a safer digital ecosystem.

Keywords: Blockchain, Cyber Security, Digital Identity, Data Protection, Secure Transactions, Decentralization.

1. Introduction

In today's highly digital and interconnected world, the importance of **cyber security** has grown more than ever before. Cyber security can be simply understood as the practice of protecting computer systems, networks, applications, and the data stored in them from different types of threats. It ensures that the information remains **confidential** (kept private and not leaked to unauthorised persons), **integral** (not changed or tampered with), and **available** (accessible whenever it is required). These three pillars – confidentiality, integrity, and availability – form the very foundation of any secure digital system.

However, with the rapid expansion of the internet, cloud computing, online banking, e-commerce, and social media platforms, the number of **cyber attacks** has also increased drastically. Threats like **ransomware attacks** (where attackers lock important files and demand money), **phishing** (where fake emails or websites trick users into sharing personal information), and **insider threats** (when employees or trusted people misuse their access) are becoming more common. The traditional defence methods, such as firewalls, anti-virus software, and centralised monitoring systems, are often unable to fully prevent or control these modern and sophisticated attacks. This shows that cyber security now requires new and advanced approaches.

In this situation, **Blockchain technology** has come into focus as a promising solution. Initially developed to power cryptocurrencies like Bitcoin, blockchain has now moved beyond financial transactions and is being considered as a transformative technology in many other fields. The main strength of blockchain lies in its **decentralised structure**, where data is not stored in one single server but distributed across a network of computers (nodes). This makes it extremely difficult for attackers to manipulate or hack the system, since there is no single point of failure. Another powerful feature is its **tamper-resistant design**, which means that once a record is entered into the blockchain, it cannot be altered or erased.

Because of these qualities, blockchain can offer new ways to **secure digital transactions**, **manage digital identities**, and **prevent unauthorised access** to sensitive information. For example, blockchain can be used to make online payments more secure, to ensure that personal identity information is safe from theft, and to protect critical databases from tampering.

Thus, blockchain is not just about digital money; it has the potential to **revolutionise the field of cyber defence** by introducing more reliable, transparent, and secure methods of data protection. This paper aims to study these possibilities in detail by examining the applications, challenges, and future scope of blockchain in strengthening cyber security.

2. Blockchain and Cyber Security

Blockchain is a modern digital technology that is best known for being the foundation of cryptocurrencies like Bitcoin. However, its usefulness goes much beyond digital money. At its core, blockchain is a type of **distributed ledger technology (DLT)**. This means that instead of storing information in a single central location, the data is stored in a network of computers (known as nodes). The data is arranged in the form of **blocks**, and each block is linked to the previous one through **cryptography**. Because of this cryptographic linking, the chain of blocks becomes highly secure, making it nearly impossible to change or delete any record once it has been added. This property makes blockchain both **immutable** (unchangeable) and **transparent** (open to verification).

The qualities of blockchain directly support and strengthen **cyber security** in several important ways:

1. Decentralization

In traditional security systems, data is stored and managed in a central server or authority. This creates a **single point of failure**, meaning that if the central system is hacked or compromised, the entire network can be damaged. Blockchain solves this problem through Decentralization. Since the information is distributed across many nodes, no single authority controls it completely. Even if one node is attacked, the system continues to function securely. This makes cyber attacks much harder to succeed.

2. Immutability

One of the most powerful features of blockchain is immutability. Once data is entered into a blockchain, it cannot be changed or erased without the agreement of the whole network. This ensures that **unauthorised modifications** are prevented. For cyber security, this means that important records such as financial transactions, identity proofs, or medical data cannot be tampered with by hackers or malicious insiders. It helps in building trust among users that their information will remain safe and original.

3. Transparency with Privacy

Blockchain offers a unique balance between **openness** and **privacy**. All transactions recorded in the blockchain can be verified, which provides transparency. At the same time, sensitive information can be shared in a controlled manner through encryption and permissioned blockchains. This means that while data remains verifiable, only authorised users can access or view private details. This dual feature makes blockchain very suitable for secure communication, safe data sharing, and regulatory compliance in sectors like banking, healthcare, and government services.

4. Smart Contracts

Another major innovation in blockchain is the concept of **smart contracts**. A smart contract is a self-executing digital agreement where the rules and conditions are written directly into code. Once the conditions are met, the contract automatically carries out the agreed actions without the need for third-

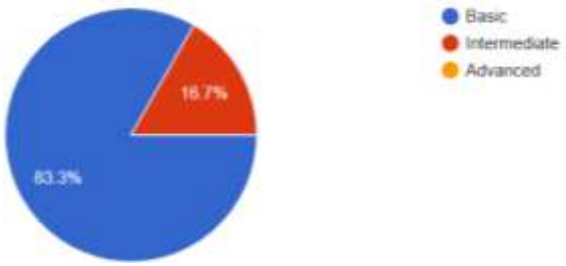
party involvement. In terms of cyber security, smart contracts can be used to **automate security policies**, such as granting or denying access to resources, validating digital identities, or ensuring compliance with data protection laws. This reduces the chances of human error and improves reliability.

In this way, blockchain combines its decentralised, tamper-proof, and transparent nature with advanced features like smart contracts to provide new and effective methods for enhancing cyber security. It has the potential to transform how digital systems are protected, making them more secure against modern cyber threats.

3. Research Survey Report on Blockchain and Cyber Security

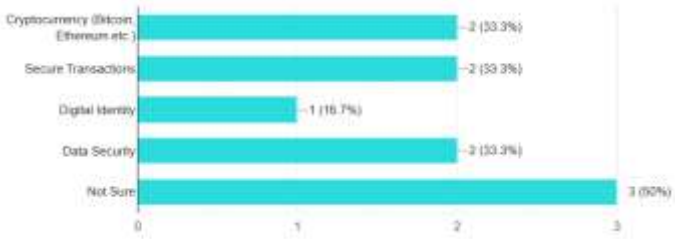
3.1 Awareness Levels

- Cyber security awareness: Mostly **Basic**, with some **Intermediate**.
- Blockchain awareness: Only **1 respondent had heard of Blockchain**, others said **No**.



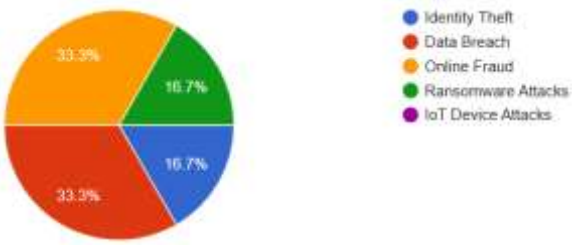
3.2 Understanding of Blockchain

- One respondent related it to **Cryptocurrency & Security**.
- Some linked it to **Data Security**.
- Majority were **Not Sure**.



3.3 Cyber Threats of Concern

- Data Breach
- Identity Theft
- Ransomware Attacks
- Online Fraud

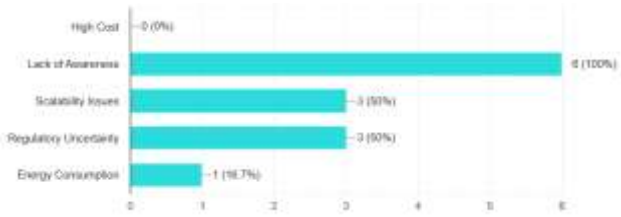


3.4 Blockchain for Cyber Security (Perceptions)

1. **Secure Transactions**: Mostly "Maybe", one clear "Yes".
2. **Digital Identity Management**: Mostly "Maybe", one "Yes".
3. **Data Protection**: Mostly "Maybe", one "Yes".

3.5. Barriers to Adoption

1. Lack of Awareness
2. Scalability Issues
3. Regulatory Concerns



4. Blockchain Applications

Blockchain is not limited to cryptocurrency alone; it has wide applications in strengthening cyber security across various domains. Its decentralised, transparent, and tamper-resistant nature makes it suitable for handling sensitive information and critical processes. Some of the key applications are discussed below:

4.1 Securing Transactions

One of the earliest and most widely recognized uses of blockchain is in securing financial transactions. The **double-spending problem**, which means spending the same digital currency twice, is eliminated because every transaction is validated and recorded permanently in the blockchain ledger (Nakamoto, 2008). Cross-border payments, remittances, and digital banking services can gain higher trust levels as blockchain prevents fraud and unauthorised manipulation (Fernandez-Carames & Fraga-Lamas, 2019). This ensures that customers and institutions both benefit from transparency and security.

4.2 Digital Identity Management

Identity theft is a serious problem in the digital world. Traditional identity systems are centralised and vulnerable to hacking. Blockchain introduces the concept of **self-sovereign identity (SSI)**, where users have complete control over their digital identity without depending on centralised authorities (Proctor, 2024). This approach not only reduces the risk of unauthorised access but also ensures safer authentication processes for services such as e-governance, banking, and online platforms (Chongqing University of Posts and Telecommunications, 2019).

4.3 Data Protection

Sensitive data such as **medical records, supply chain information, and government documents** require strong protection. With blockchain, such records can be stored in a tamper-proof way, ensuring both **integrity and auditability** (Stephen & Alex, 2018). For example, in healthcare, blockchain prevents unauthorised changes to patient histories and allows only authorised doctors or institutions to access the

records. Similarly, supply chains benefit by being able to trace goods securely at every stage, reducing fraud and counterfeit risks.

4.4 IoT Security

The rapid growth of the **Internet of Things (IoT)** has created new security challenges, such as vulnerability to botnet attacks. Blockchain can provide decentralised authentication and secure device-to-device communication, reducing single points of failure (Ballamudi, 2016). By enabling distributed trust, blockchain helps prevent large-scale cyber-attacks that exploit weak IoT devices.

5. Blockchain and Security Case Studies

5.1 Estonia's E-Government: Estonia is one of the first countries in the world to implement blockchain at a **national governance level**. Since 2008, Estonia has been using blockchain-based systems to secure its government databases, including **healthcare records, judicial data, and national registries** (Mahmood, 2022). The technology ensures that records cannot be tampered with, and every change is visible and auditable. For example, in healthcare, blockchain protects patient records, giving patients and doctors confidence in the integrity of data. In governance, it improves transparency and reduces the possibility of corruption or unauthorised changes to government documents. This model has made Estonia a **global leader in digital governance**, often cited as an example for other nations to follow.

5.2 IBM & Maersk TradeLens (Global Supply Chain): Global trade involves many parties such as shipping companies, customs authorities, and financial institutions. Traditionally, data in supply chains is siloed, and this makes it vulnerable to **fraud, document manipulation, and inefficiency**. IBM and Maersk developed **TradeLens**, a blockchain-based platform, to tackle these issues. TradeLens provides a **shared, tamper-proof digital ledger** where all stakeholders can track the movement of goods, shipping documents, and customs records in real time (Wylde, 2022). This system increases transparency, reduces paperwork, prevents fraud, and improves efficiency in global trade. By 2022, over 150 organisations, including port operators and logistics companies, joined the platform, showing its acceptance and effectiveness.

5.3 Decentralised Finance (DeFi): The rise of **Decentralised Finance (DeFi)** demonstrates blockchain's role in reshaping financial systems. Unlike traditional finance, where banks or central authorities control transactions, DeFi uses **smart contracts** on blockchains to automate financial services such as lending, borrowing, insurance, and trading (Taherdoost, 2023). These services are highly secure, transparent, and open to anyone with internet access. Since transactions are recorded on blockchain, risks like fraud, double-spending, or manipulation are reduced. However, challenges like coding vulnerabilities in smart contracts remain. Despite this, DeFi has become a multi-billion-dollar ecosystem, showing how blockchain can create trust in financial systems without intermediaries.

5.4 Healthcare Data Security (Example: MediLedger Project): Healthcare is a critical area where data security is very important. The **MediLedger Project** uses blockchain to secure pharmaceutical supply chains and prevent **counterfeit drugs** from entering the market (Stephen & Alex, 2018). By tracking every stage of a medicine's journey, from manufacturer to pharmacy, blockchain ensures authenticity and patient safety. Similarly, storing **patient medical records** on blockchain gives patients more control over their data while ensuring doctors have access to accurate and tamper-proof histories. This improves both security and healthcare quality.

5.5 Voting Systems (Blockchain-Based E-Voting): Blockchain has also been tested in **electronic voting systems**, aiming to improve transparency and prevent fraud. For instance, some pilot projects in the United

States and other countries have used blockchain-based voting platforms for overseas citizens (Chongqing University of Posts and Telecommunications, 2019). These systems allow votes to be recorded securely, ensuring that they cannot be altered or deleted. This builds public trust in election processes and reduces the risk of hacking centralised voting databases. While large-scale adoption is still in the experimental stage, blockchain e-voting shows promise for the future of democratic processes.

6. Challenges

Despite many advantages, blockchain adoption in cyber security is not free from challenges:

1 **Scalability**: Public blockchains often face slow transaction speeds, making them difficult to use for large-scale enterprise solutions (Homoliak et al., 2019).
2 **Energy Consumption**: Consensus mechanisms like proof-of-work demand high energy, raising environmental concerns (Fernandez-Carames & Fraga-Lamas, 2019).
3 **Legal & Regulatory Barriers**: Many countries do not yet have clear laws and regulations for blockchain, slowing down adoption (Chongqing University of Posts and Telecommunications, 2019).
4 **Interoperability**: Different blockchain platforms lack common standards, making it difficult for them to work together seamlessly (Elisa et al., 2020).

7. Future Directions

To make blockchain more effective for cyber security, future research can focus on:

1 **Post-Quantum Cryptography with Blockchain**: To create **quantum-safe security systems** resistant to future quantum computing threats (He et al., 2024).
2 **AI-Enhanced Blockchain**: Artificial Intelligence (AI) can help detect anomalies and prevent attacks in real time (Tariq, 2025).
3 **Hybrid & Consortium Blockchains**: Enterprise-level security solutions can be developed by combining public and private blockchain models (Fernandez-Carames & Fraga-Lamas, 2019).
4 **Zero Trust Architecture Integration**: Blockchain can be merged with zero trust frameworks to strengthen identity management and reduce risks from insider threats (Proctor, 2024).

8. Conclusion

In conclusion, blockchain presents a powerful framework for addressing major challenges in cyber security. Its ability to provide secure transactions, protect digital identities, and safeguard sensitive data makes it an important tool in building trust in digital ecosystems. Although there are barriers such as scalability, energy consumption, and unclear regulations, ongoing innovation and global policy development are expected to overcome these issues. With advancements such as AI integration, post-quantum cryptography, and hybrid models, blockchain is likely to become a **cornerstone of future cyber security architectures** (Mahmood, 2022; Wylde, 2022).

References and Bibliography

1. Ballamudi, K. R. (2016). Blockchain as a type of distributed ledger technology. **Asian Journal of Humanity, Art and Literature, 3**(2), 127–136.
2. Stephen, R., & Alex, A. (2018). A review on blockchain security. **IOP Conference Series: Materials Science and Engineering, 396**, 012030.
3. Proctor, K. (2024, January). Decentralization, immutability, and integrity: The role of blockchain tech-

nology in enhancing cybersecurity. **University of the Cumberlands**.
4. Chongqing University of Posts and Telecommunications. (2019). A systematic literature review of blockchain cyber security. **Digital Communications and Networks, 6**(2), 147–156.
5. Taherdoost, H. (2023, February 13). Smart contracts in blockchain technology: A critical review. **Information, 14**(2), Article 117.
6. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2019, February 25). A review on the application of blockchain for the next generation of cybersecure Industry 4.0 smart factories.
7. He, Z., Li, Z., Yang, S., Qiao, A., Zhang, X., Luo, X., & Chen, T. (2024, March 21). Large Language Models for blockchain security: A systematic literature review.
8. Tariq, A. (2025, April 3). Blockchain and distributed ledger technologies for cyberthreat intelligence sharing.
9. Mahmood, (2022). Cybersecurity challenges in blockchain technology: A scoping review. **Human Behavior and Emerging Technologies**.

Web Links

1. Blockchain: A new safeguard to cybersecurity. In Blockchain Technology: Applications and Challenges (pp. 271–284). https://doi.org/10.1007/978-3-030-69395-4_15SpringerLink
2. Leveraging blockchain technology for cyber security: A comprehensive review. Retrieved from Preprints.org. https://www.preprints.org/manuscript/202409.0407/v1 Preprints
3. Blockchain solutions for enhancing security and privacy in industrial IoT. Retrieved from Preprints.org. https://www.preprints.org/manuscript/202504.2178/v1 Preprints
4. Blockchain and how it relies on cryptographic methods. Retrieved from Preprints.org. https://www.preprints.org/manuscript/202504.1170/v1 Preprints
5. Blockchain and Internet of Things: A bibliometric study. **Computers & Electrical Engineering, 81**, Article 106525. https://doi.org/10.1016/j.compeleceng.2019.106525 ScienceDirect
6. A survey on the application of blockchain in cryptographic protocols. **Cybersecurity**. https://doi.org/10.1186/s42400-024-00324-7