



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.935

Volume 15, Issue 8, August 2026

Blockchain-Based Cybersecurity Framework for Decentralized Security Management

Srinidhi R¹, Praneetha Yuvaraj², Sasmitha Balasubramani³, Sanjay T⁴, Nallasamy A⁵, Sivaprakash B⁶

UG Student, Department of Computer Science, KPR College of Arts Science and Research, Coimbatore, India ¹⁻⁶

ABSTRACT: As digital financial systems, health records, supply chains, and even government functions get digitized, the attack surface for malicious bad actors keeps expanding; cybersecurity has become one of the most pressing concerns of this decade. In particular, current cybersecurity technologies and organizational measures are largely based on centralized trust infrastructure, which leaves critical systems exposed to data breaches, ransomware attacks, insider trading, and DDoS attacks among other vulnerabilities. The blockchain technology that enables Bitcoin and other cryptocurrencies has been proposed and demonstrated as a viable complement and alternative to the traditional trust infrastructure. This paper examines the relationship between cybersecurity and blockchain technology, including how existing cybersecurity properties are enforced in the blockchain technology, how blockchain technology has been used to secure critical systems, and the shortcomings of blockchain technology that limit its adoption. Specific applications of blockchain in cybersecurity are discussed including securing identity management systems, enabling secure data sharing while maintaining data confidentiality, protecting critical infrastructure and IoT systems, and decentralized domain name systems among others. The paper also covers some of the limitations and challenges that still hinder widespread adoption of blockchain technology, including scalability constraints, regulatory and governance issues, vulnerability of smart contracts to attacks, and blockchain immutability among others. Finally, the paper highlights some of the future research directions in blockchain cybersecurity, and concludes by observing that while blockchain technology alone cannot guarantee absolute cybersecurity, it can be leveraged to complement traditional cybersecurity technologies.

KEYWORDS: Cybersecurity, Blockchain, Distributed Ledger Technology, Cryptography, Smart Contracts, Consensus Mechanisms, Data Integrity, Decentralization.

I. INTRODUCTION

Cybersecurity is a generic term that refers to concepts, technologies, and measures that are used to secure networks, systems, devices, and data. As more and more functions are digitized and rely on the digital infrastructure, cybersecurity has become a critical concern as the number and sophistication of attacks increase by the day. Traditional cybersecurity measures are largely based on centralized trust infrastructure. In this paper, we explore how these centralized systems present vulnerabilities that can be exploited and how the blockchain technology can be leveraged to improve security. We begin the discussion by looking at the background and scope of the issue, review existing literature, and present some of the basic cybersecurity concepts before proceeding to the main discussion on how blockchain technology can be used to improve cybersecurity, and the limitations and challenges that still need to be addressed. Case studies of blockchain applications in cybersecurity are also presented. Additionally, future research directions are also highlighted before the concluding section that summarizes the main points and provides a closing remark.

II. LITERATURE REVIEW

Since Satoshi Nakamoto's seminal paper on Bitcoin, blockchain technology has been widely studied and adopted as a means of enabling decentralized digital transactions. More recently, Vitalik Buterin proposed a blockchain platform that supports smart contracts – programmable instructions that execute automatically when particular conditions are met. Since then, blockchain has been considered as a potential trust infrastructure for securing a wide range of digital transactions. The literature contains numerous studies looking at the potential of blockchain to improve cybersecurity as well as some of the shortcomings that still need to be addressed. Some of the applications that have been proposed include blockchain-based secure data storage and sharing, decentralized identity management systems, blockchain-based DNS, blockchain-based IoT security, and decentralized PKI. On the other hand, several research studies have

been carried out on blockchain-specific vulnerabilities. Some of the areas that have been identified as weak links or points of failure include 51 percent attacks, double-spending attacks, smart contract vulnerabilities, and the immutability of blockchain. This paper builds on the existing literature by providing an in-depth discussion on the potential applications and limitations of blockchain technology in improving cybersecurity.

III. FUNDAMENTALS OF CYBERSECURITY

A. The CIA Triad

The fundamental principles of cybersecurity are captured in the CIA triad – confidentiality, integrity, and availability. The principles state that the primary objectives of cybersecurity are to ensure that data is accessible only to those authorized to access it (confidentiality), that the data is accurate and has not been tampered with (integrity), and that the data is available when needed (availability). Other principles are derived from these three objectives. Blockchain technology, as will be discussed later, can be used to enhance data integrity and availability in various cybersecurity applications.

B. Common Cybersecurity Threats and Attacks

The main cybersecurity threats and attack vectors can be grouped into several broad categories:

- **Malware and ransomware:** These are malicious software that can damage data or encrypt it and demand a ransom to decrypt it.
- **Phishing and social engineering:** Cyber attackers use deception to trick people into giving away passwords or other sensitive information
- **Denial of service (DoS) and distributed denial of service (DDoS):** These attacks overwhelm a system or server with traffic to prevent it from being accessible by the intended users.
- **Insider threats:** This refers to attacks by individuals who have authorized access to the target systems, networks, or data.
- **Man-in-the-middle:** This is an attack where the attacker intercepts communication between two parties to gain unauthorized access to the data.
- **Supply chain attacks:** This refers to attacks on one component in a supply chain with the intention of impacting other elements in the supply chain.
- In general, these vulnerabilities are mainly caused by the reliance on centralized trust infrastructure, which presents attack surfaces that can be leveraged to launch various types of attacks. One of the ways of countering these vulnerabilities is by leveraging decentralized trust infrastructure, such as the blockchain technology.

IV. FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY

C. Overview and Structure

Blockchain technology is best known as the underlying technology of Bitcoin cryptocurrency. A blockchain is a distributed ledger that records digital transactions in a manner that makes it almost impossible to alter the information once it has been recorded. Individual pieces of information are stored in blocks, which are then linked together using cryptographic hashing algorithms to form a chain. These blocks are stored in multiple computers across the globe, which prevents tampering with the information as each computer would have a copy of the information. A blockchain can be either public or private, depending on who has access to it and who is allowed to participate in the recording of the transactions.

D. Consensus Mechanisms

Because there is no central authority that manages or oversees the processing and recording of transactions in the blockchain, there is a need for consensus mechanisms to ensure that all participants agree on which transactions are valid and should be added to the blockchain. The most common consensus mechanisms are proof of work (PoW) and proof of stake (PoS). Other mechanisms include Practical Byzantine Fault Tolerance (PBFT), Delegated PoS (DPoS), and Proof of Authority (PoA). Each of these mechanisms employs slightly different approaches to achieve the overarching goal of establishing a general agreement on the validity of transactions, which ensures the integrity of the blockchain.

V. TYPES OF BLOCKCHAINS

In addition to the difference in consensus mechanisms, blockchain can be categorized as public, private, and consortium blockchain. In a public blockchain, anyone can participate in the consensus mechanism and join the network. In a private blockchain, only one organization can participate in the consensus mechanism and manage the network. A consortium blockchain is a type of blockchain that involves multiple organizations in the management and maintenance of the network. Organizations join a consortium blockchain network to achieve an overarching goal such as the need for interbank transaction processing, and sharing of supply chain data among consortium members.

E. Smart Contracts

Smart contracts are self-executing pieces of code that are used to carry out automated functions. Smart contracts have been described as computerized agreements that execute terms of a contract when certain predefined conditions are met. Smart contracts can be used to enforce security policies, execute transactions, and store data in a secure manner. By their nature, smart contracts execute functions automatically, without the need for a trusted third party to oversee the process. Smart contracts, therefore, enable decentralized enforcement of rules, policies, or terms of an agreement. One of the challenges associated with smart contracts is that they are often deployed on a blockchain, and as such, have limited flexibility since they cannot be altered once deployed. The vulnerabilities associated with smart contracts will be discussed in detail later.

VI. BLOCKCHAIN AS A CYBERSECURITY ENABLER

F. Decentralized Identity Management

In conventional identity management systems, users have to rely on identity providers to issue and store their credentials. This centralized approach has proven to be insecure as, in case of a breach, the credentials of thousands or even millions of users can be compromised. With the decentralized identity management approach, users have their own cryptographic credentials that they can control and share selectively as needed. The underlying blockchain technology allows for highly secure storage and sharing of identity management data with appropriate credentials. Additionally, the decentralized nature of the technology makes it nearly impossible for data to be altered by malicious actors.

G. Secure, Auditable, and Verifiable Data Sharing

The blockchain technology can be leveraged to enhance data sharing among organizations while at the same time maintaining confidentiality and integrity of the data. Data confidentiality can be achieved by allowing only those who have the right credentials to access the data. This approach works well with the decentralized identity management system. The blockchain technology can also be used to store audit trails to ensure data integrity. For instance, in the healthcare sector, audit trails containing encrypted patient health records can be stored in the blockchain to provide verifiable information on whether the data has been tampered with or not.

VII. SECURING CRITICAL INFRASTRUCTURE AND IOT SYSTEMS

H. Securing Critical Infrastructure and IoT Systems

IoT devices present some of the main entry points in most networks. These devices are often operated in a resource-constrained manner and therefore cannot run complex security algorithms. They also do not have the processing power to verify the authenticity of other devices. In addition to that, most IoT devices are manufactured by different manufacturers and operated on different networks, which makes it challenging to establish trust. The application of blockchain technology can help address some of the security challenges with IoT devices by enabling distributed trust infrastructure. The distributed ledger technology can help in verifying the authenticity of IoT devices, thus enabling secure communication between devices. For instance, IoT devices can be programmed to only communicate with other IoT devices that have been authenticated using the blockchain technology. This approach can also help mitigate some of the challenges associated with DDoS attacks by ensuring that no one device is more important than the rest and therefore a single point of failure.

I. Decentralized Public Key Infrastructure

The Public Key Infrastructure (PKI) is a framework used in digital security to bind public keys to specific identifiable entities. It is the underlying technology that enables encryption, and secure exchange of information over the internet. The conventional PKI consists of trusted third parties that issue and manage the digital certificates. However, this approach is vulnerable since the trusted third parties can be compromised and start issuing fraudulent certificates. The blockchain technology can be leveraged to address this weakness in the conventional PKI. By deploying the blockchain technology, issuance of certificates becomes a distributed process, and therefore it is significantly harder for dishonest entities to issue fraudulent certificates.

J. Mitigating DoS and DDoS Attacks

The blockchain technology can be used to create distributed DNS infrastructure to mitigate denial-of-service and distributed denial-of-service attacks. Such attacks have become extremely common and can cause significant disruptions to businesses. By using distributed DNS servers, it becomes significantly harder for attackers to launch successful DDoS attacks.

VIII. APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

K. Application in the Financial Sector

Blockchain technology has been widely adopted in the financial sector to facilitate financial transactions, record-keeping, auditing, and other financial-related activities. The technology has been deployed both in private and public blockchains. Some banks have started adopting the proof of stake consensus mechanism to reduce the high energy consumption associated with the proof of work mechanism that has been traditionally used in blockchain technology.

L. Application in Healthcare

The healthcare sector deals with extremely sensitive patient information that must be handled with utmost care. As such, the industry presents some of the most compelling use cases of blockchain technology in cybersecurity. There are numerous use cases of blockchain technology in healthcare, ranging from data sharing and storage to decentralized clinical trials and genomic data management. One of the main applications of blockchain technology in healthcare is enabling secure data sharing while maintaining confidentiality. With the application of blockchain technology, healthcare organizations can securely share patient data while mitigating potential data security risks.

M. Application in Supply Chain and Provenance

Blockchain technology can be applied to record the provenance of goods, ranging from food products to other goods and services. The application of the technology can go a long way in helping address some of the challenges with counterfeiting and ensuring authenticity of products. Additionally, blockchain technology can be used to track down contaminated or faulty products, which will be critical in ensuring food safety.

N. Application in Government and Voting Systems

Several governments and organizations have been considering the potential of adopting blockchain technology for voting systems, where it could be used to provide verifiable voting records. Some of them even use the technology to offer voters with confidence that their votes have been recorded correctly. However, the application of blockchain in voting systems is extremely controversial because of the concerns regarding voter anonymity.

IX. LIMITATIONS AND CHALLENGES OF ADOPTING BLOCKCHAIN TECHNOLOGY

O. Scalability Limitations

While blockchain technology has proven to be secure and reliable, it has several limitations and challenges that need to be addressed before it can be widely adopted and deployed. Some of the main limitations are discussed below. First, most blockchain networks can only process a limited number of transactions before they become slow and congested. This limitation is especially significant with public blockchains such as Bitcoin and Ethereum, where anyone can participate in processing the transactions. The scalability limitations have prompted researchers to develop other approaches including the layer two solutions, and sharding.

P. Vulnerability to Attacks

Even though the blockchain technology has proven to be secure, it still presents several vulnerabilities that can be exploited by malicious bad actors. The main vulnerabilities include smart contract vulnerabilities and 51 percent attacks. Smart contracts are often associated with coding errors that can present opportunities for exploitation. Additionally, most smart contracts are immutable, which means that it is not possible to correct or update them once they have been deployed on the blockchain. On the other hand, 51 percent attacks are possible especially with private blockchains where some members join the network just to launch such attacks. In a 51 percent attack, an attacker withholds a significant percentage of the network resources in order to manipulate the blockchain data, which can lead to double-spending among other issues.

Q. Energy Consumption

Most blockchain networks, especially those that were the first to be developed such as Bitcoin, use the proof of work consensus mechanism. While the mechanism has proven to be secure, it has been extremely energy-intensive, which has prompted significant criticism. Some researchers have criticized the large carbon footprint attributed to the mechanism, with some proposing the need to replace it with other approaches.

R. Privacy Concerns

Even though the blockchain technology has been widely touted as a means of enhancing privacy and anonymity, it has several weaknesses that can be exploited to compromise privacy. Some of the critical weaknesses include the fact that all transactions are publicly visible, and the potential for transaction graph analysis to deanonymize users. Additionally, the use of blockchain technology for applications such as voting may raise privacy concerns.

S. Governance and Legal Issues

There are several governance and legal issues associated with blockchain technology. The use of smart contracts in the technology, for instance, raises questions on how disputes can be resolved. Additionally, the use of blockchain technology in different jurisdictions presents a number of legal challenges, especially with regard to data privacy laws, and issues surrounding the accountability.

T. Key Management Issues

In conventional blockchain technology, users are responsible for the management of their private keys. There are no central authorities that can grant access to a particular blockchain network or revoke access in case of a breach. As such, there is an extreme responsibility that comes with blockchain wallet management. In the event that the private keys are lost or stolen, it is extremely challenging to recover the losses.

X. CASE STUDIES

U. The DAO Attack of 2016

The DAO is among the earliest known projects that were built on top of the Ethereum blockchain. It was designed to be a decentralized autonomous organization that allowed people to invest in projects proposed by other members of the DAO community. However, the DAO was attacked by hackers who were able to deploy what came to be known as the reentrancy attack to withdraw with funds. The attack raised several questions about the vulnerability of smart contracts to attacks, as well as the effectiveness of the Ethereum network in withstanding such attacks.

V. IBM Food Trust

IBM Food Trust is a blockchain-based system that has been deployed to track food products through the supply chain. IBM has partnered with several major retail companies such as Walmart, Kroger, Carrefour, and others to ensure that the food products that they sell are safe for consumption. The system allows the companies to track the provenance of food products and, in case of contamination, it significantly reduces the amount of time needed to take appropriate action to address the issue.

W. Estonia's e-government

Estonia has been at the forefront of implementing e-government solutions that leverage the blockchain technology to secure data and prevent tampering with official records. By using the blockchain technology, the Estonian government ensures that records are not tampered with, thus reducing fraud and facilitating efficient governance.

Table.1. Comparative Evaluation with Values

Parameter	Traditional Cybersecurity	Blockchain-Based Cybersecurity	Better Approach
Data Integrity	80%	95%	Blockchain
Data Tamper Resistance	75%	95%	Blockchain
Decentralization	40%	95%	Blockchain
Auditability	75%	92%	Blockchain
Traceability	70%	95%	Blockchain
Identity Management	78%	90%	Blockchain
Data Sharing Security	80%	92%	Blockchain
Single Point of Failure Protection	55%	90%	Blockchain
IoT Security	72%	88%	Blockchain
DDoS Resilience	65%	82%	Blockchain
Scalability	92%	65%	Traditional
Energy Efficiency	90%	60%	Traditional
Privacy	88%	75%	Traditional
Governance	90%	68%	Traditional
Key Management	88%	70%	Traditional
Ease of Implementation	90%	65%	Traditional

Table 1.2 Overall Performance

Category	Traditional Cybersecurity	Blockchain Cybersecurity
Security Strength	78%	91%
Data Integrity	80%	95%
Transparency	70%	93%
Decentralization	40%	95%
Scalability	92%	65%
Energy Efficiency	90%	60%
Privacy	88%	75%
Governance	90%	68%
Overall Suitability	81%	84%

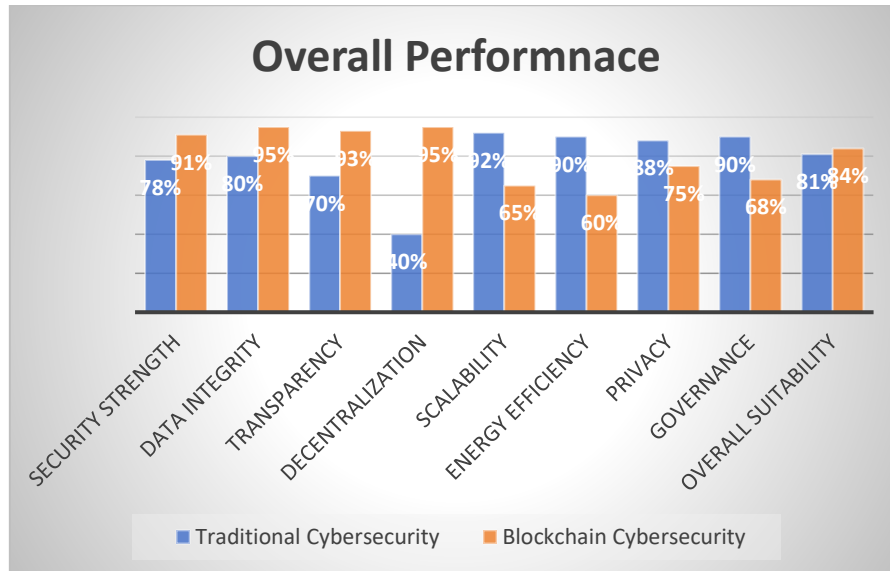


Figure 1.1 Overall Performance

XI. FUTURE RESEARCH DIRECTIONS

Some of the areas that need to be explored future research directions in blockchain cybersecurity include:

- Research on post-quantum cryptography and its implications on blockchain cybersecurity,
- Hybrid approaches or off-chain databases that can be integrated with blockchain technology,
- The application of AI to analyze blockchain transactions to detect potential security risks,
- Interoperability of different blockchain networks,
- Design of regulatory-compliant privacy tools for use with blockchain technology.

XII. CONCLUSION

Blockchain technology presents several potential advantages and opportunities for enhancing cybersecurity capabilities. The technology enables secure digital transactions and data storage with minimal risk of being tampered with or compromised. Some of the main advantages of blockchain technology include decentralized trust infrastructure, improved integrity of data, enhanced audit trails, and increased availability of systems and data. However, there are several limitations and disadvantages associated with the technology, including vulnerability to attacks, extreme energy consumption, and poor scalability. As such, while the technology can be leveraged to enhance cybersecurity capabilities, it should not be considered as a one-size-fits-all solution. It is critical for organizations considering adopting the technology to weigh the pros and cons of using the technology. For instance, in cases where traditional cybersecurity measures can suffice, it may be more cost-effective to adopt conventional measures rather than adopting the blockchain technology.

REFERENCES

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
2. Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform .
3. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends . IEEE International Congress on Big Data .
4. Khan, M. A., & Salah, K. (2018). IoT Security: Review, Blockchain Solutions, and Open Challenges . Future Generation Computer Systems .
5. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in Internet of Things: Challenges and Solutions . IEEE PerCom Workshops .

6. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts. Principles of Security and Trust (POST) .
7. National Institute of Standards and Technology. (2018). Blockchain Technology Overview (NISTIR 8202).
8. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. Telematics and Informatics .



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details