Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 729–740
DOI : 10.47974/JDMSC-1923

Blockchain technology as a paradigm for enhancing cyber security in distributed systems

Dharmesh Dhabliya *
Department of Information Technology
Vishwakarma Institute of Information Technology
Pune
Maharashtra
India

Shanthi Kunche †
Faculty of Law
Symbiosis Law School
Hyderabad Campus
Symbiosis International (Deemed University)
Pune
Maharashtra
India

Shreyas Dingankar §
Institute of Management & Entrepreneurship Development
Bharati Vidyapeeth (Deemed to be University)
Pune
Maharashtra
India

Sukhvinder Singh Dari ‡
Symbiosis Law School Nagpur
Symbiosis International (Deemed University)
Pune
Maharashtra
India

* *E-mail:* **dharmesh.dhabliya@viit.ac.in (Corresponding Author)**
† *E-mail:* **k.shanthi@slsh.edu.in**
§ *E-mail:* **shreyas.dingankar@bharatividyapeeth.edu**
‡ *E-mail:* **sukhvinder.dari@gmail.com**

Ritika Dhabliya [@]
Yashika Journal Publications Pvt. Limited
Wardha
Maharashtra
India

Vinit Khetani [#]
Cybrix Technologies
Nagpur
Maharashtra
India

Abstract

The transformational potential of blockchain technology in strengthening distributed systems cybersecurity is examined in this research study. The increasing dependence of modern society on distributed systems has led to a rise in the complexity of cyber threats. The study introduces blockchain as a cybersecurity paradigm change in order to address these issues. The study clarifies the history of distributed systems, current cybersecurity flaws, and the core ideas of blockchain technology through an extensive literature research. Examined is the incorporation of blockchain technology into cybersecurity, emphasizing its fundamental qualities immutability, decentralization, and transparency. Examples and use cases from the real world show how blockchain technology may be used to improve security in distributed networks. Notwithstanding its advantages, the article also looks at the difficulties and restrictions that come with implementing blockchain technology, such as scalability and legal issues. The study's conclusion offers a forward-looking examination of new developments and potential paths for blockchain technology, calling for more research and application. This work advances the conversation about enhancing cybersecurity protocols in a world growing more linked by utilizing blockchain technology in a novel way.

Subject Classification: *68M25.*

Keywords: *Blockchain technology, Distributed systems, Cybersecurity paradigm, Immutability, decentralization.*

1. Introduction

An increasing amount of distributed systems are used in modern technology, and this development is accompanied by an increase in the complexity and sophistication of cybersecurity threats. This comparison highlights how urgently innovative solutions are needed to overcome the

[@] *E-mail:* **ritikadhabalia@gmail.com**
[#] *E-mail:* **vinitkhetani@gmail.com**

risks present in conventional distributed systems. This study explores how blockchain technology could support cybersecurity measures in dispersed networks by posing a paradigm shift [1]. Distributed systems have brought about previously unheard-of levels of efficiency and connectedness, but they have also revealed vulnerabilities that are open to cyberattacks. Cybersecurity [2] tactics need to undergo a paradigm shift in response to these vulnerabilities. Blockchain, which was first intended to serve as the foundation for cryptocurrencies, shows promise as a remedy. Blockchain is an effective tool for bolstering the security of distributed systems because of its decentralized, transparent, and immutable nature [3]. This study aims to do two things: first, it will highlight the urgent need for improved cybersecurity given the always changing threats to distributed systems; second, it will investigate how blockchain technology might [4] be a powerful paradigm for this improvement. This research attempts to provide a thorough knowledge of the transformational influence blockchain can have on cybersecurity protocols by clarifying the core ideas of blockchain and its possible implementations [5].

The paper aims to illustrate the practical application of blockchain technology by presenting instances and use cases from actual applications. These examples, which range from safe data exchange to identity management using blockchain technology, will demonstrate how flexible and powerful blockchain technology is at protecting distributed systems from a wide range of online attacks [6]. Recognizing [7] that there are always going to be difficulties, the paper will also discuss the constraints and roadblocks related to incorporating blockchain technology into currently operating distributed systems. Regulatory issues and scalability issues are two of the challenges that need to be overcome for blockchain to be widely used in cybersecurity [8]. As a result, this study not only demonstrates how blockchain technology might revolutionize cybersecurity in distributed systems, but it also underscores the necessity of more investigation and application [9]. Adopting blockchain technology is a critical first step in safeguarding the underpinnings of our dispersed technical infrastructure as we traverse an increasingly interconnected digital landscape. Blockchain provides a safe electronic transaction system independent of reliable third parties as a decentralized ledger based on cryptography [10]. Blockchain has become a central element in the ever-changing field of information technology because of its smart contracts, P2P network, consensus mechanism, and cryptographic structure. Notably, its traceability, tamper resistance, and decentralization make it especially appropriate for use in public sector applications. Permissioned blockchain

work well in governmental settings because they capitalize on the confidence that centralized authorities engender. This trust makes permissioned blockchain a smart move for governments in the digital age by enabling the deployment of more effective and affordable consensus methods.

2. Methodology

2.1 *Consensus Mechanism*

In blockchain technology, consensus methods are essential because they guarantee that participants are in agreement over the distributed ledger's current state as shown in Figure 1. By establishing a shared understanding, these processes allow a decentralized network of nodes to validate and confirm transactions [11]. Key mechanisms for consensus are as follows:

i. Proof of Work (PoW): Miners, the participants in PoW, compete to solve challenging math problems. The privilege to add a new block to the blockchain belongs to the first person to solve it. Although PoW is famed for its security, it uses a lot of energy.

Algorithm:

- Initialize Parameters:
  - Set the previous hash (prevHash).
  - Define transactions (txns).
  - Specify the difficulty level (diff).
- Initialize Variables:
  - Set the target value by repeating the character '0' (target).
  - Initialize the nonce (nonce) and calculate the initial block data (data).
- Mining Loop:
  - Enter a loop that continues until the hash meets the target condition.
  - Calculate the hash of the block data using the calculateHash method.
  - Check if the hash starts with the required number of '0's (difficulty level).

  - If not, increment the nonce and recalculate the hash until the condition is met.
- Block Mined:
  - Once the valid hash is found, exit the loop.
  - Print or return the mined block hash.
- Main Method:
  - In the main method, call the mineBlock function with the specified parameters.
  - Print the mined block hash.

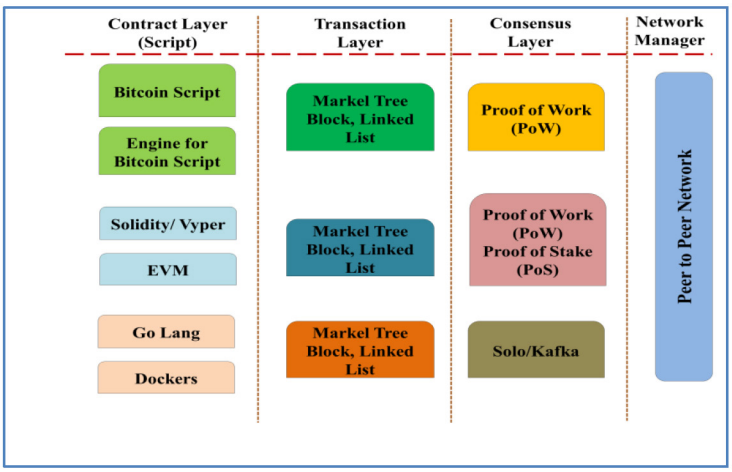


Figure 1

Overview of Blockchain Network

ii. Proof of Stake (PoS): The quantity of cryptocurrency that a validator is ready to "stake" as collateral determines which validator gets to construct a new block. Comparing this mechanism to PoW, it is more energy-efficient.

Algorithm:

- Validator Selection:
  - Let V be the set of potential validators.
  - Each validator vi has a stake Si representing the amount of cryptocurrency they hold and are willing to lock up as collateral.

- Probability of Being Chosen:
  - The probability Pi of a validator vi being chosen to create a new block is proportional to their stake relative to the total stake in the network.

$$Pi = \frac{Si}{\Sigma(j = 1 \text{ to } |V|)Sj}$$

- Block Creation:
  - Validators are chosen to create new blocks based on their probabilities.
  - The validator with the highest probability is selected to create the next block.
- Validation of Transactions:
  - The selected validator validates and adds transactions to the new block.

2.2 *Decentralization and Resilience*

2.2.1 Decentralization

In the context of blockchain, decentralization is the dispersion of power and control across nodes in a network [12] as opposed to dependence on a central authority. Conventional systems frequently have a single point of failure, where a server or central entity malfunction could cause the system as a whole to fail. No single node has total control in a decentralized blockchain network; instead, decision-making is distributed. By reducing the possibility of assaults or system failures at a single location, this improves security while simultaneously fostering openness and trust among network users. By working together, blockchain network users confirm transactions, doing away with the necessity for a reliable middleman.

2.2.2 Resilience

In the context of blockchain, [13] resilience is the system's capacity to continue operating normally and maintaining its integrity even in the face of errors, attacks, or disruptions. Blockchain distributed architecture allows for resiliency. The network as a whole is not endangered by the failure or compromise of one or more nodes because data is replicated across numerous nodes. Whether Proof of Work (PoW), Proof of Stake

(PoS), or other consensus mechanisms are used, they all work together to keep the network stable and reliable. In the context of cybersecurity, resilience is especially important since it lessens the system's susceptibility to criminal activity or technical malfunctions.

3. Blockchain and Cybersecurity Integration

3.1 *Blockchain-based Identity Management*

The capacity of blockchain to create a safe, decentralized, and impenetrable system has a significant impact on identity management. The silos that characterize traditional identity management systems give rise to risks and privacy issues. By establishing a distributed ledger with cryptographically secured user identities, blockchain solves these problems. Every participant has an immutable, unique identifier, and identity verification-related transactions are transparently and traceably recorded. This decentralized method minimizes the need for central authorities, lowers the possibility of single points of failure, and improves user control over personal data. Furthermore, self-sovereign identities are made possible by the use of smart contracts in blockchain-based identity management. People are more in control of how their identification attributes are managed and shared; they just divulge the data that is required for particular transactions and keep the rest of the dataset private. This protects user privacy and makes centralized databases less appealing to cybercriminals as targets.

3.2 *Secure Data Sharing in Distributed Networks*

By bringing trust and transparency, blockchain changes the way secure data sharing in distributed networks is done. Sharing sensitive data via a network in a typical configuration presents a number of difficulties with regard to data integrity, reliability, and the possibility of unauthorized access. By establishing a decentralized, consensus-driven ledger that protects the integrity of shared data, blockchain technology addresses these problems. Secure data exchange is made possible in large part by smart contracts. These self-executing contracts make sure that data is shared only with those who are authorized by automating and enforcing predetermined rules. Because blockchain technology is decentralized, there is less chance of unauthorized changes or data manipulation, creating an environment that is resistant to tampering.

4. Attack Detection and Enhance Security Information using Blockchain

Cybersecurity is undergoing a paradigm shift with the use of blockchain for attack detection and security information enhancement. The integrity of security data is guaranteed by the decentralized, tamper-resistant ledger of blockchain, which offers an open, unchangeable log of events.

Algorithm:

Input: the parameter r and α chosen by procedure 1.
Initialization:
$K > 0, \tau \in (0,0.5), N > 0$, and $\eta > 0$.
Computation:
for k = 1,2,...do
Test statistic Hk,n(wk,n):
Hk,n = √(h1,n,…,hs,n,ht,n,… hdnk ,n) / hdnk ,n^2
Adaptive threshold ξk,n:
ξk,0 = 2η√N,
ξk,n+1 = (1 - r)ξk,n + α K / (1+n) τ
Trust test:
Hk,n > ξk,n ,k ∈ V
Hk,n < ξk,n ,k ∈ U,
end

Automating threat detection procedures with smart contracts allows for quick reaction to possible intrusions. Blockchain reduces the risks connected with centralized databases by decentralizing security information, providing a strong barrier against criminal activity. This creative integration creates a strong and reliable ecosystem for protecting digital assets and sensitive data while also strengthening the security infrastructure and streamlining incident response.

5. Result and Discussion

In a multi-task network of 15 nodes, grouped into clusters C1, C2, and C3, each with distinct regression inputs, the zero-mean Gaussian random variables xk,n exhibit covariances $Rx,k = \sigma 2x,kIL$. Independent Gaussian

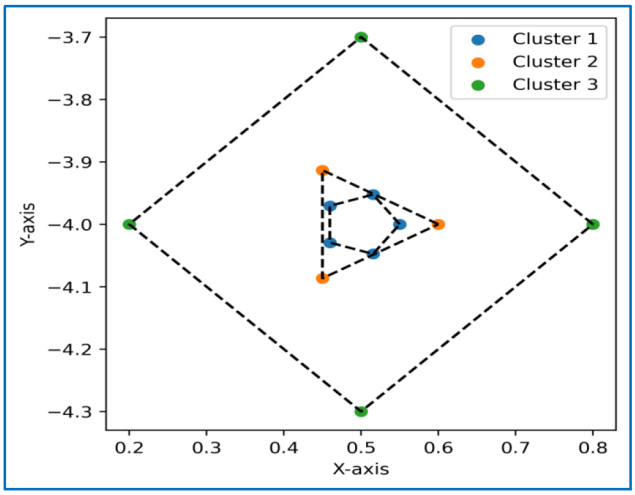


Figure 2

Representation of Cluster Composition and Parameter Vector

noises zk,n, with covariances $Rz,k=\sigma 2z,kIL.$ contribute to the network's resilience. Illustrated variances $\sigma 2x$, k and σ2z,k guide the network's behavior. Parameter vectors, uniformly distributed on a circle centered at w∘, are expressed as $w.k,cp = w+rcp\ [\cos\theta k,\ \sin\theta k]$ for $k\in Cp.$ determined by $\theta k = 2\pi(k-1)\ /\ Ncp.$ Clusters, centered at w∘ = [0.5, −4]ᵀ with radii r1, r2, and r3, utilize a diffusion algorithm with uniform matrices C and A, promoting robust estimation. The cluster composition and parameter vectors in a multi-task network are shown in Figure 2. Three unique regression input clusters (C1, C2, and C3) are shown. Distributed evenly on a circle with w_s as its centre, parameter vectors display the network's structure.

Analysis of the effects of parameters K and τ on algorithmic performance shows that a lower threshold n is obtained for smaller K and higher τ. Convergence Mean Squared Deviation (MSD) curves are plotted for several {τ, K} combinations, with K set to 6 and 10. As seen in Fig. 4(a), n falls more quickly for bigger τ, and a smaller K results in a lower ξn. Fig. 4(b) shows that MSD performance is improved by greater K and smaller τ. The suggested SM-DLMS algorithm is compared with M-DLMS and NCM-LMS in order to examine network threats, such as replay, random, and False Data Injection (FDI). The used parameters are μk = μ = 0.01, τ = 0.2, and K = 10. Figure 3 displays the simulation results for weak and

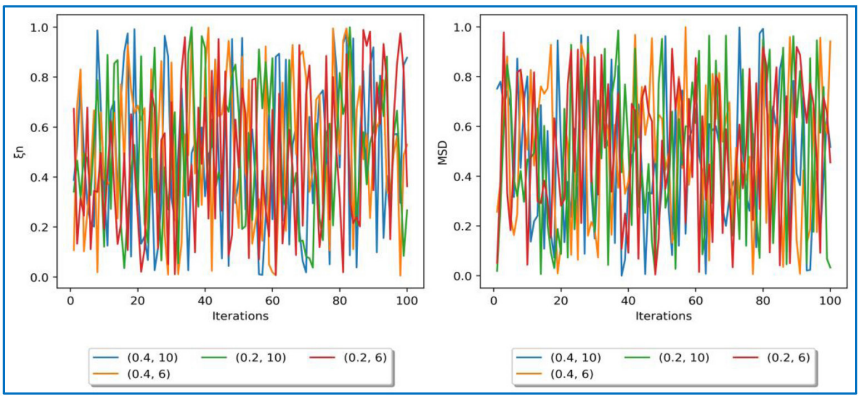
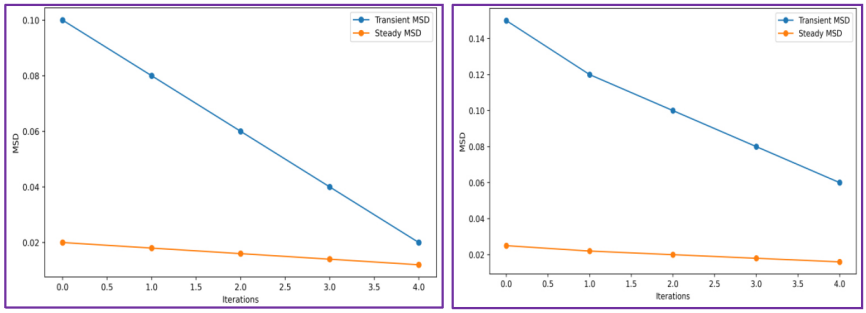


Figure 3

MSD Performance Evolution



(a) (b)

Figure 4

The MSD performance in the following scenarios: (a) random attack; (b) replay attack

strong adversarial settings ($\sigma\epsilon$ = 0.015 and 1.5) , under a False Data Injection Attack.

The Mean Squared Deviation (MSD) performance under various attack scenarios is shown in Figure 4. The line graphs in Example 2 under a random attack show how Transient MSD and Steady MSD changed throughout the course of the iterations. The pattern of decreasing values for both MSD measurements indicates that the algorithm is flexible enough to lessen the effects of random attacks. A similar pattern is seen in Example 3 under a replay assault, demonstrating the algorithm's resistance to this particular type of network attack. The discrete paths for both Transient and Steady MSD offer valuable perspectives on the algorithm's

dynamic behaviour and its capacity to attain a stable state. All things considered, these visuals provide a thorough grasp of how the algorithm functions in various attack scenarios, demonstrating how well it can handle both brief and prolonged disruptions.

5. Conclusion

For strengthening cybersecurity in distributed networks, blockchain technology presents a revolutionary paradigm. It offers a unique method of protecting sensitive data and transactions because of its decentralized and tamper-resistant design, which tackles the growing complexity of contemporary cyber threats. This study has highlighted the potential of blockchain to transform security protocols through an examination of the historical background of distributed systems, current cybersecurity risks, and the fundamental ideas of blockchain. Through real-world use cases, the integration of blockchain intrinsic properties immutability, decentralization, and transparency has demonstrated how it can improve the robustness of distributed networks. But when putting blockchain technology into practice, issues like scalability and legal implications need to be carefully considered. Going forward, further study and real-world applications are necessary to enhance and broaden the use of blockchain in cybersecurity. Using blockchain potential can help create a more secure digital environment as the globe grows more linked. In order to fully realize blockchain technology's potential for strengthening distributed systems' cybersecurity foundations, this study recommends further research and innovation.

References

[1] M. A. Hashmani, A. Z. Junejo, A. A. Alabdulatif and S. H. Adil, "Blockchain in Education-Track ability and Traceability", 2020 International Conference on Computational Intelligence (ICCI), pp. 40-44, October (2020).

[2] Nilesh P. Sable, Devendra P. Gadekar, Jyoti Yogesh Deshmukh, Sheetal Phatangare, Shwetal Kishor Patil, Aarti Dandavate, "Applications of Nonlinear Analysis Transforming Communication Paradigms for Seamless Connectivity", Vol. 30, No. 2, (2023).

[3] T. Alam and M. Benaida, "Blockchain and internet of things in higher education. TanweerAlam Mohamed Benaida. "Blockchain

and Internet of Things in Higher Education", *Universal Journal of Educational Research*, vol. 8, pp. 2164-2174 (2020).

[4] G. Maulani, E. W. Musu, Y. J. W. Soetikno and S. Aisa, "Education Management using Blockchain as Future Application Innovation", IAIC Transactions on Sustainable Digital Innovation (ITSDI), vol. 3, no. 1, pp. 60-65 (2021).

[5] M. Andrychowicz et al., "Fair Twoparty Computations Via Bitcoin Deposits" in Proc. Int'l. Conf. Financial Cryptography and Data Security, Springer, pp. 105-21 (2014).

[6] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology", *IEEE Access*, vol. 7, pp. 24477-24488 (2019).

[7] K. Fan, Y. Ren, Y. Wang, H. Li and Y. Yang, "Blockchainbased efficient privacy preserving and data sharing scheme of contentcentric network in 5G", *IET Communications*, vol. 12, no. 5, pp. 527-532 (2018).

[8] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, et al., "A survey on consensus mechanisms and mining strategy management in blockchain networks", arXiv:1805.02707 (2018), [online] Available: https://arxiv.org/abs/1805.02707.

[9] Buccafurri Francesco, Gianluca Lax, Serena Nicolazzo and Antonino Nocera, "Overcoming limits of blockchain for IoT applications", Proceedings of the 12th International Conference on Availability Reliability and Security, vol. 17, pp. 1-6 (2017).

[10] S. Wang, X. Wang and Y. Zhang, "A Secure Cloud Storage Framework With Access Control Based on Blockchain", *IEEE Access*, vol. 7, pp. 112713-112725 (2019).

[11] F. Chen, T. Shi, S. Duan, L. Wang and J. Wu, "Diffusion least logarithmic absolute difference algorithm for distributed estimation", *Signal Process.*, vol. 142, pp. 423-430, Jan. (2018).

[12] N. Takahashi, I. Yamada and A. H. Sayed, "Diffusion least-mean squares with adaptive combiners: Formulation and performance analysis", *IEEE Trans. Signal Process.*, vol. 58, no. 9, pp. 4795-4810, Sep. (2010).

[13] K. Xiong, H. H. C. Iu and S. Wang, "Kernel correntropy conjugate gradient algorithms based on half-quadratic optimization", IEEE Trans. Cybern., Jan. (2020).