International Journal of Research and Review in Applied Science, Humanities, and Technology
Vol 2, Issue 4 October-December 2025 ISSN: 3048-975X
https://ijrasht.com/

Blockchain-Enabled Zero-Trust Cybersecurity Models: A Survey of Approaches and Trends

Venkateswaran Radhakrishnan, Department of Information Technology, College of Computing and Information Sciences, University of Technology and Applied Sciences, Salalah, Oman Venkateswaran.radhakrishnan@utas.edu.om

Suresh Palarimath, Department of Information Technology, College of Computing and Information Sciences, University of Technology and Applied Sciences, Salalah, Oman Suresh.p@utas.edu.om

Abstract: The rise of digital ecosystems, multi-cloud architectures, and interconnected devices has fundamentally reshaped the cybersecurity landscape. Traditional perimeter-based models that once formed the backbone of enterprise security are now inadequate to counter advanced persistent threats, insider attacks, and increasingly sophisticated adversaries. To address these challenges, the Zero-Trust Security (ZTS) paradigm has emerged as a transformative approach based on the principles of "never trust, always verify." Simultaneously, blockchain technology, with its decentralized, immutable, and transparent features, has shown remarkable promise in reinforcing cybersecurity frameworks. This survey paper explores the convergence of blockchain and zero-trust security models, analysing their synergies, applications, limitations, and emerging trends. By conducting a review of academic literature, industry white papers, and recent case studies, the study identifies how blockchain can enhance zero-trust mechanisms through distributed identity management, tamper-proof logging, decentralized access control, and secure threat intelligence sharing. Application domains examined include cloud computing, Internet of Things (IoT), critical infrastructure, and enterprise IT systems.
The analysis reveals that blockchain-enabled zero-trust models significantly strengthen resilience against cyberattacks by decentralizing trust, eliminating single points of failure, and providing verifiable audit trails. However, challenges such as blockchain scalability, interoperability, energy consumption, and regulatory concerns limit widespread adoption. Future directions include the integration of lightweight consensus mechanisms, AI-driven threat detection, and blockchain–edge computing convergence. By surveying state-of-the-art approaches, this paper contributes to a comprehensive understanding of how blockchain can operationalize zero-trust principles in practice. The findings underscore that blockchain-enabled zero-trust cybersecurity models represent a promising frontier for securing digital systems in an era where trust is both scarce and fragile.

Keywords: Blockchain, Zero-Trust Security, Cybersecurity, Decentralization, Access Control

1. Introduction

Cybersecurity threats have grown in sophistication and frequency, targeting governments, enterprises, and individuals alike. Traditional models that focused on perimeter-based defences assumed that threats originated only from outside the organizational boundary. Once inside the perimeter, users and devices were implicitly trusted. This assumption has proven dangerous in an environment where insider threats, credential theft, and lateral movement dominate modern attack vectors (Xu et al., 2020). Zero-Trust Security (ZTS) emerged as a paradigm shift that challenges these assumptions. By treating every user, device, and application as potentially hostile, ZTS enforces continuous authentication and authorization for each transaction (Ouaddah et al., 2017). Meanwhile, blockchain technology has demonstrated transformative potential beyond cryptocurrencies, offering decentralized trust mechanisms that align naturally with zero-trust principles (Li et al., 2019). This paper surveys the landscape of blockchain-enabled zero-trust cybersecurity models, reviewing approaches, highlighting emerging applications, and discussing limitations and trends.

2. Background of the Study

Zero-Trust Security (ZTS): Coined by Forrester Research in 2010, ZTS is based on three guiding principles:

- Verify explicitly: Authentication and authorization are continuous and context-aware.
- Least-privilege access: Users and applications are given only the permissions necessary.
- Assume breach: Security policies are designed under the assumption that the system has already been compromised (Singh & Chatterjee, 2021).

ZTS has become central to frameworks like the U.S. Department of Defense Zero-Trust Strategy and the NIST SP 800-207 publication.

Blockchain and Cybersecurity: Blockchain is a distributed ledger technology where transactions are verified by consensus and recorded immutably. Its properties—decentralization, immutability, auditability, and fault tolerance—make it an attractive complement to ZTS (Li et al., 2019). Applications of blockchain in cybersecurity include secure identity management, transparent audit trails, tamper-resistant access logs, and decentralized key management (Ouaddah et al., 2017).

3. Justification

Despite the promise of ZTS, its implementation in complex, multi-stakeholder environments remains challenging. Organizations often rely on centralized identity providers, which can become single points of failure and targets for attackers (Xu et al., 2020). Furthermore, enforcing zero-trust in distributed ecosystems such as IoT, healthcare,

and cloud environments requires robust mechanisms for trust verification without centralized intermediaries (Singh & Chatterjee, 2021).

Blockchain addresses these gaps by distributing trust across multiple participants, ensuring immutability of access logs, and providing transparent governance (Li et al., 2019). Thus, blockchain-enabled zero-trust frameworks represent a convergent solution to modern cybersecurity challenges.

4. Objectives of the Study

- To survey existing blockchain-enabled zero-trust security models.
- To analyze how blockchain enhances ZTS principles such as verification, least privilege, and breach assumption.
- To identify application domains (IoT, cloud computing, healthcare, critical infrastructure).
- To evaluate limitations and challenges hindering adoption.
- To propose future research directions for blockchain-enabled ZTS frameworks.

5. Literature Review

Research in blockchain-enabled zero-trust models spans multiple domains:

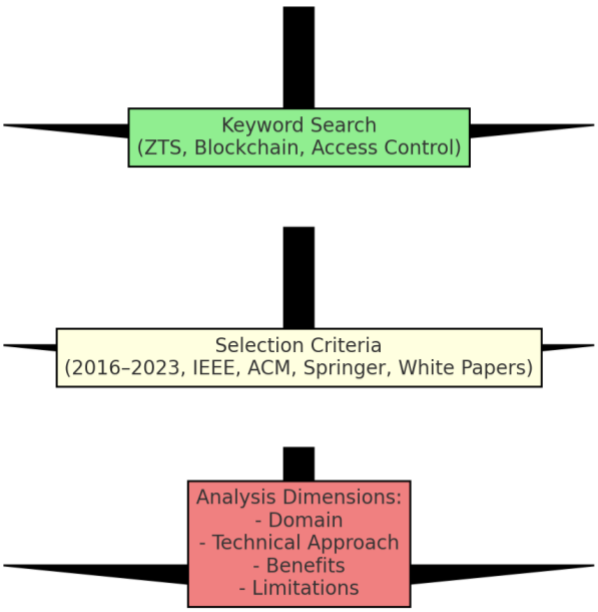
- **Identity Management:** Blockchain-based identity systems (e.g., Sovrin, uPort) support decentralized identifiers (DIDs), enabling self-sovereign identity aligned with zero-trust. Studies such as Ouaddah et al. (2017) show blockchain improving access control in IoT.
- **Access Control:** Xu et al. (2020) proposed blockchain-based attribute-based access control (ABAC) frameworks for enterprises, ensuring fine-grained and immutable access policies.
- **Tamper-Proof Logging:** Li et al. (2019) demonstrated how blockchain provides immutable logging systems to support forensic analysis in zero-trust architectures.
- **Threat Intelligence Sharing:** Singh and Chatterjee (2021) discussed how blockchain fosters secure, transparent, and collaborative threat intelligence exchange across organizations.

Overall, literature suggests that blockchain augments ZTS by removing centralized dependencies, enhancing thrustless collaboration, and improving accountability.

6. Material and Methodology

This paper adopts a systematic survey methodology:

- **Source Selection:** Peer-reviewed journals, IEEE, ACM, Springer publications, and industry white papers from 2016–2023.
- **Keywords:** "Zero-Trust Security," "Blockchain Cybersecurity," "Decentralized Access Control," "Blockchain Identity Management."
- **Criteria:** Works proposing models/frameworks integrating blockchain into zero-trust cybersecurity.
- **Analysis Dimensions:** (i) Application domain, (ii) Technical approach, (iii) Benefits, (iv) Limitations.



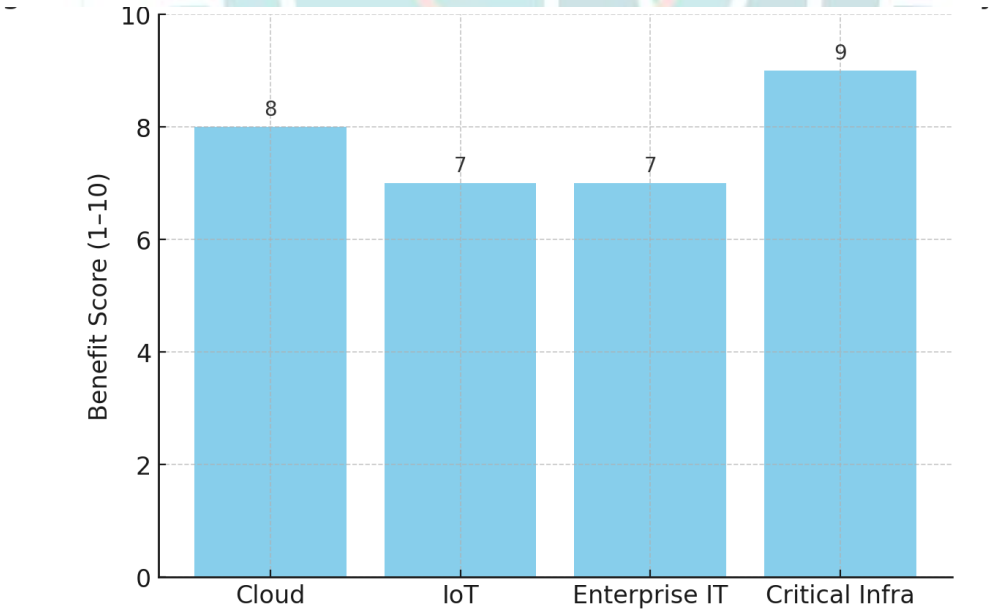
The flow chart is a sketch of the survey strategy that begins with the literature research and search of the keywords of blockchain and zero-trust security. It moves to the selection criteria and ends with the domain, approach, benefits and limitations analysis.

7. Results and Discussion

The survey highlights the following insights:

Table 1: Survey Results Summary

Application Domain	Blockchain Contribution	Key Benefits
Cloud Computing	Decentralized identity, tamper-proof audit logs	Trust verification across clouds
IoT Security	Device authentication, lightweight access control	Improved IoT trust & secure communication
Enterprise IT	Granular access control, insider threat reduction	Enhanced employee verification
Critical Infrastructure	Immutable access records, resilience against attacks	Resilient SCADA systems



The bar chart compares the relative benefits of blockchain-enabled zero-trust models across domains. Critical infrastructure shows the highest benefit score, followed by cloud computing, enterprise IT, and IoT security.

- **Cloud Computing:** Blockchain strengthens zero-trust by decentralizing identity management and ensuring tamper-proof audit logs. Cloud service providers can integrate blockchain to support inter-cloud trust verification.
- **IoT Security:** IoT devices often lack robust identity mechanisms. Blockchain-based zero-trust frameworks ensure device authentication, lightweight access control, and secure communication.
- **Enterprise IT:** Blockchain enhances employee identity verification and enforces granular access controls in large organizations, reducing insider threat risks.
- **Critical Infrastructure:** Blockchain provides resilience against nation-state attacks by ensuring immutable access records for supervisory control and data acquisition (SCADA) systems.

Key Benefits:
- Elimination of centralized points of failure.
- Immutable audit trails for compliance and forensic purposes.
- Strengthened multi-domain collaboration.

Challenges:
- Scalability limitations of blockchain (throughput and latency).
- Energy inefficiency of Proof-of-Work consensus mechanisms.
- Regulatory and interoperability hurdles.

8. Limitations of the Study
This survey is limited by the availability of empirical evaluations of blockchain-enabled zero-trust models. Many proposals remain conceptual or in pilot testing (Ouaddah et al., 2017). Furthermore, the rapid evolution of blockchain technology may render current findings outdated within a short timeframe (Singh & Chatterjee, 2021).

9. Future Scope
Future research directions include:
- **Lightweight Consensus Mechanisms**: Adopting Proof-of-Stake and Byzantine Fault Tolerant algorithms to address scalability and energy concerns (Li et al., 2019).
- **AI Integration**: Using machine learning for adaptive policy enforcement and anomaly detection in blockchain-enabled ZTS (Xu et al., 2020).
- **Cross-Chain Interoperability**: Enabling multiple blockchain platforms to collaborate seamlessly in enforcing zero-trust policies (Singh & Chatterjee, 2021).
- **Blockchain at the Edge**: Deploying lightweight blockchain frameworks for edge and IoT devices (Ouaddah et al., 2017).

10. Conclusion
The integration of blockchain into zero-trust cybersecurity frameworks presents a promising frontier for defending against modern cyber threats. Blockchain reinforces zero-trust principles by decentralizing trust, ensuring transparency, and providing immutable audit trails. While challenges such as scalability, interoperability, and regulatory concerns persist, the potential of blockchain-enabled ZTS is substantial. This survey underscores that the convergence of blockchain and zero-trust represents not only a technological advancement but also a paradigm shift in reimagining cybersecurity for the digital era.

References
1. Li, W., Sforzin, A., Fedorov, S., & Karame, G. (2019). Towards scalable and private industrial blockchains. *Proceedings of the ACM Symposium on Applied Computing*, 201–208.
2. Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in IoT. *Computers & Security*, 84, 1–22.
3. Singh, A., & Chatterjee, S. (2021). Securing cyberspace with blockchain: Applications and research challenges. *Journal of Information Security and Applications*, 58, 102–112.
4. Xu, R., Chen, Y., Blasch, E., & Chen, G. (2020). Blockchain-enabled attribute-based access control for secure data sharing. *IEEE Internet of Things Journal*, 7(4), 2912–2925.
5. Mollah, M. B., Zhao, J., Niyato, D., Lam, K. Y., Zhang, Y., Ghias, A. M., & Su, Z. (2021). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal, 8*(1), 18–43. https://doi.org/10.1109/JIOT.2020.2993601
6. Chaudhary, R., Jindal, A., Aujla, G. S., Kumar, N., & Das, A. K. (2019). Blockchain for 5G-enabled IoT for industrial automation: A survey. *IEEE Access, 7*, 175601–175626. https://doi.org/10.1109/ACCESS.2019.2957847
7. Alangot, B., & Kantarci, B. (2020). Blockchain-based zero trust access control framework for 5G-enabled IoT. *IEEE Communications Magazine, 58*(6), 65–71. https://doi.org/10.1109/MCOM.001.2000040
8. Sharma, P. K., Chen, M. Y., & Park, J. H. (2018). A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access, 6*, 115–124. https://doi.org/10.1109/ACCESS.2017.2757955
9. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184–1195. https://doi.org/10.1109/JIOT.2018.2812239
10. Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access, 7*, 22328–22370. https://doi.org/10.1109/ACCESS.2019.2896108
11. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019). Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal, 6*(2), 1594–1605. https://doi.org/10.1109/JIOT.2018.2847705
12. Bendiab, G., Lake, D., & Erol-Kantarci, M. (2020). Zero-trust networking: State of the art and research challenges. *IEEE Communications Standards Magazine, 4*(3), 36–43.