NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Special Issue – 1, 2024
E – ISSN – 2583-7559

A Comprehensive Study of Emerging Blockchain Applications in Cybersecurity

Dr. Charanarur Panem
Department of Cyber Security and Digital Forensics
National Forensic Sciences University Tripura Campus
Agartala , India

Mr. Aditya Mohan Srivastava
Department of Cyber Security and Digital Forensics
National Forensic Sciences University Tripura Campus
Agartala , India

Dr. Gundu Srinivasa Rao
School of Science, Department of Digital Forensics, Malla Reddy University
Hyderabad, India

Dr. H.K. Pratihari
Department of Forensic Science
National Forensic Sciences University Tripura Campus
Agartala , India

Dr. Naveen Kumar Chaudhary
School of Cyber Security and Digital Forensics
National Forensic Sciences University
Gandhi Nagar & Goa, India

Dr. Mampi Devi
Department of Cyber Security and Digital Forensics
National Forensic Sciences University Tripura Campus
Agartala , India

Mr. Laishram Hemanta Singh
Department of Cyber Security and Digital Forensics
National Forensic Sciences University Tripura Campus
Agartala , India

***Abstract*— Present work explores the transformative potential of blockchain technology in cybersecurity. It begins with a fundamental introduction to blockchain's workings, then focuses on its current trends in bolstering cybersecurity, such as identity management and tamper-proof data storage. Real-world examples are used to guide practical implementations in industries like healthcare, finance, and voting. The paper also explores potential developments in the future, such as quantum-resistant cryptography, decentralized autonomous organizations, and artificial intelligence integration. The paper concludes by assessing the lasting impact of blockchain on the broader cybersecurity landscape, highlighting its ability to reshape trust paradigms and empower individuals to control their digital identities.**

Keywords—Blockchain; Cybersecurity; Quantum-resistant; Cryptography; Artificial Intelligence; Cyber threats.

I. INTRODUCTION

A decentralized ledger system known as blockchain is characterized by the fact that blocks of transactions are linked together by means of cryptographic hashes. As a result of each block carrying a one-of-a-kind identifier and pointing to the hash of the block that came before it, an unchangeable chain is formed. Patent and certificate varification are examples of decentralized consensus systems that establish agreement among nodes on the authenticity of transactions without depending on a central authority. Hashes generated by cryptographic algorithms serve as a protection against tampering. The distributed nature of blockchain technology eliminates the need for a single point of control, which in turn improves both security and trust. Certain additional capabilities, like as smart contracts, make it possible for code to execute itself, therefore automating the terms of contracts.

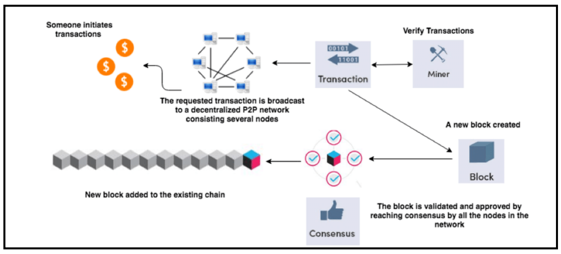


Fig. 1. Fundamental function of blockchain [30]

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Special Issue – 1, 2024
E – ISSN – 2583-7559

Blockchain technology has developed to an extent that it act as key factor in the field of cybersecurity shown in fig.1[1-3]

A number of recent developments have made use of its tamper-proof structure in order to manage digital identities, restrict illegal access, and secure data storage and transfer. Due to this development, blockchain is now positioned as a framework that is transparent, safe, and decentralized, and it has a wide spectrum of applications in the field of cybersecurity shown in fig.2 [4].

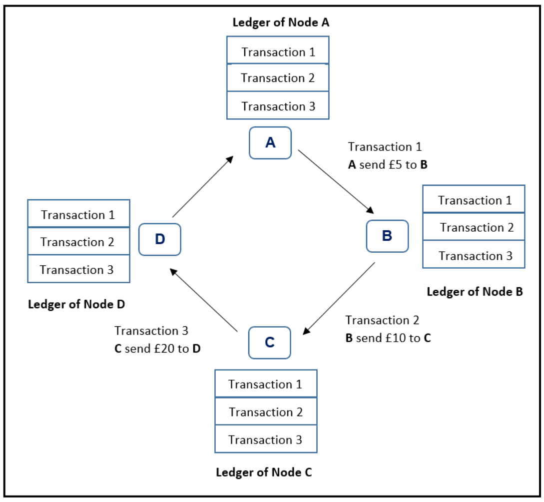
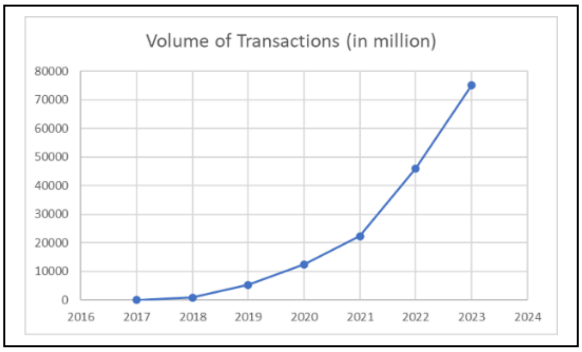


Fig. 2. Example of blockchain technology [31]

The adoption of digital transactions following demonetization in India has not only increased government's ability to track money flow but has also opened doors for blockchain and cryptocurrency. Despite a temporary ban crypto transactions in 2018, a Supreme Court decision in March 2020 allowed their resumption, highlighting the evolving role of blockchain technology and cryptocurrencies in shaping the economic. Blockchain's potential to enhance transparency and security in financial transactions is gaining



recognition globally, with implications for economic systems and financial technologies shown in fig.3 [5-6].

Figure 3 . Number of UPI transactions over the years [NPCI]

II. Challenges in Blockchain in Cybersecurity

With its decentralized and tamper-proof characteristics, blockchain technology , offers promising solutions for various cybersecurity challenges. However, its integration with existing systems and emerging trends is not without its hurdles. Here are some key challenges of the evolving applications of blockchain in cybersecurity.

A. Scalability and Performance

Transaction speeds: Due to the consensus processes that they use (for example, Proof-of-Work), public blockchains like Bitcoin encounter bottlenecks that result in sluggish transaction processing when it comes to transactions. This makes it more difficult for them to be used in high-frequency applications such as identity management or Internet of Things security[8].

Consumption of energy: Proof-of-Work consensus, despite its high level of security, necessitates a substantial amount of processing power, which results in a high level of energy consumption. Finding alternatives that are favorable to the environment, such as Proof-of-Stake, is essential for widespread adoption[9].

B. Security and Privacy

Vulnerability to attacks: they are not immune to the actions of malevolent parties. 51% attacks, double spending, and weaknesses included inside smart contracts are all examples of possible dangers. It is essential to implement the use of secure coding principles and robust consensus procedures[10]

Privacy concerns: While public blockchains provide openness, they also have the potential to reveal sensitive data, which raises privacy issues. When it comes to private deployments, permissioned blockchains that include access control are the most suitable option; nevertheless, the complexity of handling identities and access rights is increased[11].

C. Integration and Interoperability

Integration with legacy systems: Adding blockchain to an already-built system can be hard because it needs to be made compatible with new features and data needs to be standardized. [12]

Standardization: The absence of industry-wide standards for blockchain protocols and apps leads to interoperability problems, which in turn impedes the flow of data and communication between various platforms in a smooth manner[13].

D. Legal and Regulatory Considerations

Data ownership and liability: In order for legal frameworks to accept blockchain technology, it is vital to clarify ownership rights and assign accountability for data that has been compromised and stored on blockchains [14].

Regulatory uncertainty: Companies may be hesitant to use blockchain applications if they are concerned about not meeting regulatory requirements. Regulators must work together to solve security and privacy concerns while encouraging innovation[15].

III. THE OBJECTIVES OF THE PRESENT PAPER IS

- To explore blockchain technology and its impact on cybersecurity.
- Challenges and vulnerabilities associated with blockchain will be assessed.
- The paper will analyze how blockchain is currently being used to enhance cybersecurity.
- Specific applications in sectors like identity management, data storage, and communication will be examined.
- The paper will explore potential future advancements in blockchain technology relevant to cybersecurity.
- The goal is to envision a future where robust security is accessible to all

IV. EMERGING TRENDS IN CYBER SECURITY AND THEIR SOLUTION BY USING BLOCKCHAIN

The digital landscape is evolving rapidly, and so are the threats lurking within it. Cybersecurity trends are constantly shifting, requiring innovative solutions to address evolving methods of attack. With its decentralization, transparency, and immutability, blockchain technology is emerging as a powerful tool to tackle these new challenges. The table .1 shown the Emerging trends in cyber security and their solution by using blockchain

TABLE 1 Trends in cyber security and their solution by using blockchain

Trends	Cyber security aspect	Solution by Application of blockchain
AI-Driven Threat Hunting	It is becoming increasingly common for enterprises to use a proactive strategy for threat hunting by harnessing the capabilities of artificial intelligence. Through the utilization of complex artificial intelligence algorithms, big datasets are analyzed in order to identify possible security threats before they may become more severe. Proactively employing this approach substantially enhances the ability to promptly detect and respond to emerging cyber threats, as it is characterized by its proactive nature.[16]	The integrity of artificial intelligence algorithms and the datasets that are used for threat assessments can be protected by blockchain technology. This allows enterprises to confirm the validity and trustworthiness of the information that is utilized in proactive threat hunting. This is accomplished by keeping AI models and data on a ledger that is both decentralized and resistant to tampering.
Extended Detection and Response (XDR)	To provide a more comprehensive and integrated approach to threat detection and response, XDR systems combine a number of different security techniques and technologies. The purpose of this trend is to increase the effectiveness of incident response and enhance the efficiency of security operations.[17]	XDR systems can have their integrity improved because to the decentralized nature inherent in blockchain technology, which allows for the safe storage and management of logs, alerts, and incident response data. This assures that the information is available throughout the network, that it cannot be altered, and that it is transparent. As a result, the overall efficacy of threat detection and response is improved.
Deepfake Detection and Prevention	There is a serious risk to cybersecurity posed by the proliferation of deepfake technology, particularly when it comes to social engineering and the dissemination of false information. The detection and prevention of the distribution of deepfake material is currently being included into cybersecurity plans through the use of various tools and procedures.[18]	Authenticating and timestamping multimedia material may be accomplished with blockchain technology, which makes it more difficult for hostile actors to produce deep fakes that cannot be detected. Blockchain technology improves the reliability of digital material by creating a record that is both visible and unchangeable, detailing the provenance of content as well as any

		alterations made to it.
Edge Computing Security	As the adoption of edge computing becomes more prevalent, safeguarding the security of the distributed architecture at the network's edge is gaining greater significance. As a means of preserving the integrity and confidentiality of data, cybersecurity solutions are undergoing development in order to handle the one-of-a-kind difficulties that edge computing presents.[19]	The establishment of a decentralized trust model is one way that blockchain technology can improve the safety of edge computing. By utilizing blockchain technology to secure communication and data transmission, enterprises are able to guarantee the integrity and confidentiality of data that is collected at the edge of the network.
Quantum Key Distribution (QKD)	In preparation for the possible danger that quantum computers might pose to conventional encryption methods, The idea of quantum key distribution is emerging as a viable solution. The principles of quantum mechanics are utilized by QKD in order to protect communication channels against assaults that are enabled by quantum physics.[20]	The cryptographic capabilities of blockchain have the potential to supplement QKD by delivering a key management system that is both safe and decentralized. This guarantees that the cryptographic keys that are utilized for secure communication will continue to be resistant to quantum assaults and will not be tampered with.
Cybersecurity for Critical Infrastructure	With the growing digitalization of essential infrastructure, such as power grids and water supply systems, there is a heightened focus on protecting these key components from cyber attacks. This is because of the increased importance of these components. For the purpose of preventing future disruptions, robust cybersecurity measures are absolutely necessary.[21]	Providing a decentralized and resilient network for the management and protection of data connected to infrastructure components is one of the ways that Blockchain technology holds the potential to enhance the security of critical infrastructure. The likelihood of cyber attacks attacking essential systems is decreased as a result of this.

Behavioral Analytics for User Monitoring	The monitoring of user actions and the identification of abnormalities that may signal malicious behavior or illegal access are being accomplished through the utilization of behavioral analytics. Through the utilization of this method, the capability to recognize dangers based on departures from typical patterns of user behavior is improved.[22]	By providing an immutable record of user activity, blockchain technology has the potential to make further contributions to the security of user monitoring systems. By doing so, the integrity of the data collected through behavioral analytics is protected, which makes the data more trustworthy for detecting irregularities and potential security risks.
Continuous Adaptive Risk and Trust Assessment (CARTA)	CARTA is a constantly developing cybersecurity technique that performs real-time assessments of risk and trust variables in a continuous sequence. Through the utilization of this dynamic strategy, companies are able to modify their security measures in accordance with the ever-changing threat landscape.[23]	The openness and decentralized characteristics of blockchain technology have the potential to enhance the reliability of data utilized in risk and trust assessments. For the purpose of making flexible decisions on cybersecurity, this guarantees that organizations have access to a source of information that is both secure and resistant to tampering.
Distributed Cloud Security	Distributed cloud security is a concept that focuses on safeguarding data and applications across numerous cloud environments. This idea is still evolving as cloud computing continues to undergo more development. The issues that are connected with maintaining security in a dispersed cloud system are addressed by this technique.[23]	Through the provision of a decentralized consensus method for the management of access controls and the guaranteeing of the integrity of data across many cloud nodes, blockchain technology has the potential to protect distributed cloud environments. Consequently, this improves the overall security of the architecture of distributed cloud computing.

V. REAL WORLD APPLICATION

In the realm of cryptocurrency transactions, blockchain serves as the foundational technology for currencies like Bitcoin and Ethereum. This enables secure and transparent digital transactions, revolutionizing the financial landscape by reducing dependence on traditional banking systems. Blockchain's role in creating and verifying ownership of non-fungible tokens (NFTs) brings innovation to the digital asset space. NFTs, representing unique items such as art and collectibles, leverage blockchain's security and decentralization to establish authenticity. Moving into the financial sector, blockchain streamlines transactions, reducing the reliance on intermediaries. Decentralized finance (De-Fi) platforms capitalize on blockchain's capabilities, offering secure and transparent alternatives to conventional financial systems. In healthcare, blockchain ensures the secure transfer of patient records, enhances drug supply chain management and enables real-time monitoring through wearable IoT devices. The tamper-resistant nature of blockchain adds an extra layer of security to sensitive health data. E-Governance experiences a transformation through blockchain, managing digital identities securely, implementing tamper-resistant voting systems, automating government services with smart contracts, and ensuring transparency in budget and expenditure. Blockchain technology 's application in supply chain management ensures transparency, from raw material extraction to the end consumer[25].

VI. THE INFLUENCE OF BLOCKCHAIN TECHNOLOGY IN THE LANDSCAPE OF CYBERSECURITY

The pivotal focus of blockchain technology in the landscape of cybersecurity, particularly in the context of ensuring secure business transactions, notably within the cryptocurrency domain. This study underscores the multifaceted applications of blockchain technology in cybersecurity, with a specific emphasis on distributed ledger, Internet of Things security, DNS, and end-to-end encryption[26].

In the realm of distributed ledgers, blockchain technology emerges as a transformative force, enabling decentralized data storage and mitigating risks associated with centralized systems. . The incorporation of cryptographic checksums adds an additional layer of security, ensuring the integrity of data within this decentralized framework. In the realm of IoT security, blockchain offers a viable solution by providing secure data transfer mechanisms without reliance on centralized control[27].

The integration of blockchain with the Domain Name System (DNS) is particularly noteworthy. Traditional DNS, susceptible to centralized control, gains resilience against potential cyber threats through blockchain's distributed data storage. This approach challenges hackers by obscuring the exact location of stored data, thereby fortifying system security and reducing the susceptibility to data breaches.

Furthermore, the application of blockchain extends to end-to-end encryption systems, a crucial component of messaging services. This integration ensures secure data transfer within messaging systems, leveraging distributed processing and fostering a standardized communication method[28].

Scholarly discourse on the subject, such as the work by Demirkan, Demirkan, and McKee (2020), underscores the potential of blockchain technology to elevate cybersecurity. The technology's contribution lies in its implementation of consent mechanisms, functional resilience, data encryption, transparency, and immutability. Additionally, blockchain diminishes vulnerabilities by automating validation processes, countering DDoS attacks, ensuring data integrity, and supporting distributed storage. Other scholarly works, including Goldstein (2020), delve into the broader implications of how blockchain enhances cybersecurity, ensuring data privacy and veracity. The consensus among researchers is that blockchain serves as a secure platform, effectively minimizing fraudulent activities and fortifying cybersecurity across diverse applications[29].

CONCLUSION

The incorporation of blockchain technology into the field of cybersecurity signifies a transformative and promising initiative. The synergy between blockchain and emerging cybersecurity trends, including AI-driven threat hunting, XDR, deepfake detection, edge computing security, QKD, cybersecurity for critical infrastructure, behavioral analytics, CARTA, and distributed cloud security, holds significant potential in fortifying digital landscapes. Blockchain's inherent attributes, such as decentralization and transparency, prove instrumental in enhancing the integrity of various cybersecurity facets. Nevertheless, challenges like scalability, integration complexities, and regulatory considerations must be navigated. Successfully addressing these challenges creating resilient, efficient, and secure digital environments capable of countering the dynamic threats of the digital age. The collaborative effort to overcome obstacles is crucial for realizing the transformative impact of blockchain on the future of cybersecurity.

REFERENCES

[1]Ganne, E. (2018, January 1). Can Blockchain Revolutionize International Trade

[2]Finck, M. (2018, December 20). Blockchain Regulation and Governance in Europe. Cambridge University Press.

[3]Yokota, R., & Wu, W. (2018, March 20). Supercomputing Frontiers. Springer.

[4] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (Bigdata Congress), 557-564.

[5] Deloitte, "Blockchain in Commercial Real Estate," 2021) Chodorow-reich, G., Gopinath, G., Mishra, P., & Narayanan, A. (2020). Cash and the Economy: Evidence from India's Demonetization*. The Quarterly Journal of Economics.

[6]WEF. (January 2021). Digital Currency Governance Consortium.

[7] Number of UPI transactions over the years Image: NPCI

[8] Dorri, A., et al. (2017). Blockchain for cybersecurity and privacy: Architectures, challenges, and applications. IEEE Transactions on Engineering Management, 64(3), 481-498.)

[9] Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media.

[10] Christidis, K., & Devetzis, Y. (2016). Blockchains: Fundamentals and future applications. Morgan Kaufmann.

[11]Andoni, M., et al. (2018). Blockchain technology for the energy sector: Opportunities and challenges. Renewable and Sustainable Energy Reviews, 89, 1964-1976.

[12]Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind Bitcoin is transforming business, money, and our world. Penguin Random House LLC.

[13] Yaga, D., & Mell, P. (2018). Blockchain technology for cybersecurity: NIST cybersecurity and information security program. National Institute of Standards and Technology.

[14]Gatteschi, F., et al. (2018). Blockchain technologies for the supply chain. Journal of Network and Computer Applications, 76, 758-765.

[15]Yermack, D. (2017). Decentralized finance: The promise of open finance. Journal of Financial Intermediation, 27(1), 1-32.

[16] George, V., & Massey, L. (2020). Proactive Strategy to Improve Staff Engagement. Nurse Leader, 18, 532-535.Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (BigData Congress), 557-564.

[17] Al-Jelehawy, A. H. J., Nader, B. G., & Salah, K. T. (2023). Dissemination of Integron Class 1 among XDR isolates of P. aeruginosa in Najaf City. South Asian Journal of Research in Microbiology.

[18] Potthas, C., Berry, P., & Al-Naimi, H. (2023). Social engineering. In Advances in Engineering Innovation

[19] Rahal, B. M., Santos, A., & Nogueira, M. (2020). A Distributed Architecture for DDoS Prediction and Bot Detection. IEEE Access, 8, 159756-159772.

[20] Li, W., Zhang, L., Tan, H., Lu, Y., Liao, S., Huang, J., ... Pan, J.-W. (2023). High-rate quantum key distribution exceeding 110 Mb s^–1. *Nature Photonics*, 17, 416-421.

[21] Nkongolo, M. (2023). Navigating the complex nexus: cybersecurity in political landscapes. ArXiv, abs/2308.08005.

[22] Baskar, N. K. (2021). Combating Insider Threats using 'User Behavioural Analytics'.

[23] Sain, C., Biswas, P., Satpathy, P., Babu, T. S., & Alhelou, H. H. (2021). Self-Controlled PMSM Drive Employed in Light Electric Vehicle-Dynamic Strategy and Performance Optimization. IEEE Access, 9, 57967-57975

[24] Ghallab, A., Saif, M., & Mohsen, A. (2020). Data Integrity and Security in Distributed Cloud Computing—A Review.

[25]IRJET e-ISSN: 2395-0056 Volume: 10 Issue: 09 | Sept 2023 www.irjet.net p-ISSN: 2395-0072 © 2023, IRJET | Impact Factor value: 8.226 | ISO 9001:2008 Certified Journal | Page 370 "Blockchain and Its Applications in the Real World" Rajesh Kumar Kona1, Syed Ishrat2, Sameer Rithwik3, Mahesh Babu Kona4 123 UG student Dept of Cyber security, IOT incl. Blockchain Technology , VVIT, Andhra Pradesh, India 4 UG student Dept of Artificial Intelligence , MITS , Andhra Pradesh, India)

[26]Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (BigData Congress), 557-564.

[27]Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access, 7, 82721-82743.

[28]Bök, P.-B., Noack, A., Muller, M., & Behnke, D. (2020). Domain Name System (DNS). Computernetze und Internet of Things.

[29]Cogliati, B., Ethan, J., & Jha, A. (2023). Subverting Telegram's End-to-End Encryption. IACR Transactions on Symmetric Cryptology, 5-40.

[30] A survey of blockchain from prospectives of applications, Challenges and Opportunities Ahmed Afif Monrat, PhD Student, LTU, Olov Schel´en, Associate Professor, LTU, and Karl Andersson, Associate Professor, LTU

[31] Blockchain with Internet of Things: Benefits, Challenges, and Future Directions Hany F. Atlam Ahmed Alenezi, Madini O. Alassafi, Gary B. Wills