Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Cybersecurity Practices in Cryptocurrency and Traditional Banking: An Analysis of Evolving Threats and AI Solutions

Dr. Leelavathi. K[1] , Dr. Ajatashatru Samal[2], Dr. Thirulogasundaram V P[3], Vaishnavi V S[4], Malashree S[5], Dr. B Muthukrishnan[6]

[1]Associate Professor & HOD, Dept of P.G Studies in Commerce, Govt. Arts College (Autonomous) Chitradurga-577501
[2]Associate Professor & HOD, Dept. of MBA, Sri Venkateshwara College of Engineering, Bangalore email-ajatashatru7@gmail.com
[3]Professor in MBA, Donbosco Institute of Management Studies & Computer Applications, Bangalore, Email-drthirulogan2014@gmail.com
[4]Assistant Professor, Dept. of BCA, Donbosco Institute of Management Studies & Computer Applications, Bangalore, Email-Vaishnu.kellur@gmail.com
[5]Assistant Professor, Dept of Commerce & Management, Global Institute of Management and Science, RRNagar, Bangalore
[6]Associate Professor, Dept. of MBA,MLR Institute of Technology, Hyderabad, Email-drbalamuthu@mlrinstitutions.ac.in

New cybersecurity concerns have emerged as a result of the growing interconnection between cryptocurrencies and conventional banking institutions. The report delves deeply into cybersecurity strategies in several industries, examining how threats change over time and how AI might help reduce those risks. We take a look at the specific cybersecurity issues that bitcoin platforms encounter, such as the weaknesses of blockchain technology and the fact that digital assets are decentralised. We next turn our attention to the cybersecurity practices of more conventional banks, drawing attention to the difficulties inherent in dealing with outdated infrastructure and meeting all applicable regulations. This research finds similarities and differences in the cybersecurity procedures of the two industries via a comparison analysis. We also assess how AI-powered tools, such predictive analytics and machine learning algorithms, might improve systems for identifying and responding to threats. The results highlight the need of using AI-powered adaptive cybersecurity techniques to successfully tackle the ever-changing threat environment. Financial institutions, lawmakers, and cybersecurity experts may use the findings of this study to build stronger security standards to protect bitcoin and more conventional banking systems.

Keywords: Cybersecurity, Cryptocurrency, Traditional Banking, Artificial Intelligence, Threat Analysis, AI Solutions, Financial Security.

1. Introduction

With the advent of cryptocurrencies, which pose new challenges to traditional methods of asset management and transaction processing, the financial industry has seen a sea change in the digital era. This change has been happening at the same time as conventional banks have been trying to secure their systems from the myriad of cyberattacks that have been plaguing them. The complexity of cybersecurity has been further increased by the merging of cryptocurrencies and conventional banking, which calls for an in-depth analysis of the techniques and procedures used by each industry.

Cryptocurrency poses distinct cybersecurity risks due to its decentralised and sometimes pseudonymous structure. Although the blockchain technology that supports cryptocurrencies has the potential to increase security and transparency, it also exposes flaws that bad actors may exploit. Problems with smart contracts, stolen wallets, and hacked exchanges have brought attention to the necessity for strong cybersecurity protocols designed specifically for the digital asset market.

Traditional financial systems, on the other hand, have unique cybersecurity challenges due to their long-standing architecture and regulatory frameworks. Despite their pervasiveness in the financial ecosystem, legacy systems aren't always quick to respond to new risks. The significance of modern security measures and compliance with strict regulatory requirements has been highlighted by the growing number of sophisticated cyberattacks that target financial institutions. These assaults include phishing scams, ransomware, and insider threats.

By comparing and contrasting the cybersecurity measures taken by conventional banks and cryptocurrency companies, this study aims to close the knowledge gap between the two fields. Research objectives include cataloguing the ever-changing dangers faced by each industry and assessing the potential of AI to counteract these issues. Machine learning, predictive analytics, and other forms of artificial intelligence have shown potential to improve the capacity to identify and respond to threats. This study seeks to provide a thorough knowledge of how these technologies might strengthen cybersecurity defences by investigating the integration of AI solutions into cryptocurrency platforms and conventional institutions.

With the advent of new technologies and the proliferation of cyber dangers, this paper aims to provide light on the best ways to protect financial systems. Financial institutions, regulators, and cybersecurity experts may use the results to influence their strategy development for protecting sensitive financial data and keeping confidence in the ever-changing financial world.

2. Literature review

Blockchain technology has the potential to significantly impact current monetary systems, according to new study (Chang et al. 2019). This article delves into the intricacies of cryptocurrencies beyond only their use as digital trading tools. However, they have the potential to be significant game-changers, causing a reshaping of the market (Chang et al. 2019). Bitcoin is at the forefront of a new wave of digital currencies that challenge long-held financial norms. Academic studies have shown that investing in Bitcoin may help with diversification (Bauer et al., 2018; Cheah and Fry, 2015). Furthermore, Osmani et al. (2020)

found that these methodologies have changed the risk profiles of investing strategies when they are added to traditional portfolios.

A new way of thinking about diversification has emerged in response to the emergence of cryptocurrencies as an independent asset class. Some have equated their extraordinary volatility to that of speculative bubbles or revolutionary breakthroughs, and their relative youth is a contributing element (Gandal et al., 2018; Sadiq et al., 2023). Cryptocurrency prices are quite sensitive to investor sentiment and market conditions (Gandal et al. 2018). Investors in the US and UK should reevaluate their risk tolerance and investment plans in light of recent market shifts. There could be far-reaching consequences for the global financial system as a result of the increased complexity brought about by the use of cryptocurrencies, which complicates current risk management methods (Chen and Bellavitis 2019). There has been a paradigm change, according to Narayanan et al. (2020), because of the potential for cryptocurrencies to challenge conventional financial institutions. A financial system that has depended on centralised institutions for decades is being shaken to its core by the decentralised character of cryptocurrencies (Narayanan et al. 2020). The use of cryptography affects the potential environments for remittances, international payments, and peer-to-peer transactions (Narayanan et al. 2020).

Since cryptocurrencies provide a significant challenge to the dominance of central banks in the money supply, investigations into the effects on monetary policy and financial stability are necessary (Yermack 2013). Prasad (2014) notes that in response to Bitcoin's success, central bank digital currencies (CBDCs) are seeing a surge in popularity. Thus, CBDCs and cryptocurrencies form a complex web that need thorough examination in light of the evolution of financial markets. Cryptocurrencies have brought about unprecedented change inside financial institutions, expanding well beyond their initial role as digital tokens (Duchenne 2018). The following debate will cover a wide range of subjects, including portfolio diversification, volatility in the US and UK financial markets, and the reevaluation of conventional financial intermediaries (Duchenne 2018). Additional topics brought up by the rise of cryptocurrencies include potential future central banks and the far-reaching consequences this development may have on monetary systems. Financial markets will be forever changed by cryptocurrencies. Long-standing players will have to reevaluate their strategy to keep up with the new opportunities that digital revolution is bringing.

To stay relevant in the current digital economy, conventional banking institutions had to undergo a dramatic transition when cryptocurrencies were introduced, ushering in a new era of financial innovation. What follows is an analysis of the complex process by which conventional banks are responding to the opportunities and challenges presented by the rise of cryptocurrencies. Because of the revolutionary potential of cryptocurrencies, conventional banks have had to reevaluate and revamp their methods of functioning. According to Casu and Girardone (2010), American and British banks have rethought their strategy and put more focus on customer service in response to the unexpected rise of cryptocurrencies. More and more customers want their fiat currency and digital assets handled easily, and conventional banks are having a hard time keeping up. Since cryptocurrencies have spurred a wave of innovation when integrated into traditional banking systems, financial institutions have been pushed to explore potential partnerships with fintech companies. Partnerships between fintech firms and conventional financial institutions have been prompted by blockchain technology,

which is the foundation of cryptocurrencies. Mullen and Finn (2022) found that financial institutions are using blockchain technology to make settlements, local and international money transfers, and regulatory compliance faster and safer.

In response to the rise of cryptocurrencies, central banks have launched their own digital currency research with the introduction of Central Bank Digital Currencies (CBDCs). In order to stay in control of currency problems and monetary policy, central banks have taken a strategic move towards digital innovation by developing CBDCs. Prasad (2014) highlights the delicate equilibrium that CBDCs strive for. Traditional financial institutions will need to make adjustments to their risk management, customer service, and general business strategy as a result of this seismic shift towards CBDCs, as discussed by Thomason et al. (2018). Conventional banks in the US and UK face the formidable challenge of mitigating hazards associated with Bitcoin transactions as they gain popularity. Among these risks, you run the risk of being involved in illicit activities and becoming more susceptible to cyberattacks. Cybersecurity and staying abreast of the constantly evolving AML and KYC regulations are foundational components of good risk management plans, as emphasised by Raskin et al. (2020). In this rapidly digitising financial landscape, it is the responsibility of traditional financial institutions to inform and involve their consumers as they integrate blockchain technology and cryptocurrencies. Implementing clear communication techniques and simple interfaces is vital to assist consumers in making the transition from conventional banking to the new digital financial paradigm.

Objectives of the study

- To analyze and categorize the evolving cybersecurity threats specific to cryptocurrency platforms, including blockchain-related vulnerabilities and digital asset risks.
- To examine the cybersecurity threats faced by traditional banking institutions, including phishing attacks, ransomware, and insider threats.
- To evaluate and compare the cybersecurity measures and practices employed by cryptocurrency platforms and traditional banking institutions.
- To identify common practices and differences in how each sector approaches threat detection, prevention, and response.

3. Research methodology

The cybersecurity procedures of both cryptocurrency platforms and conventional banks are examined in this research using a mixed-methods methodology. In order to comprehend the current cybersecurity procedures and emerging risks in both industries, the research starts with a comprehensive literature study. Next, we'll compare and contrast the cybersecurity tactics and AI applications of conventional banking with cryptocurrencies. The study's overarching goal is to provide practical suggestions based on this data in order to help the banking sector improve its cybersecurity operations.

4. Discussion

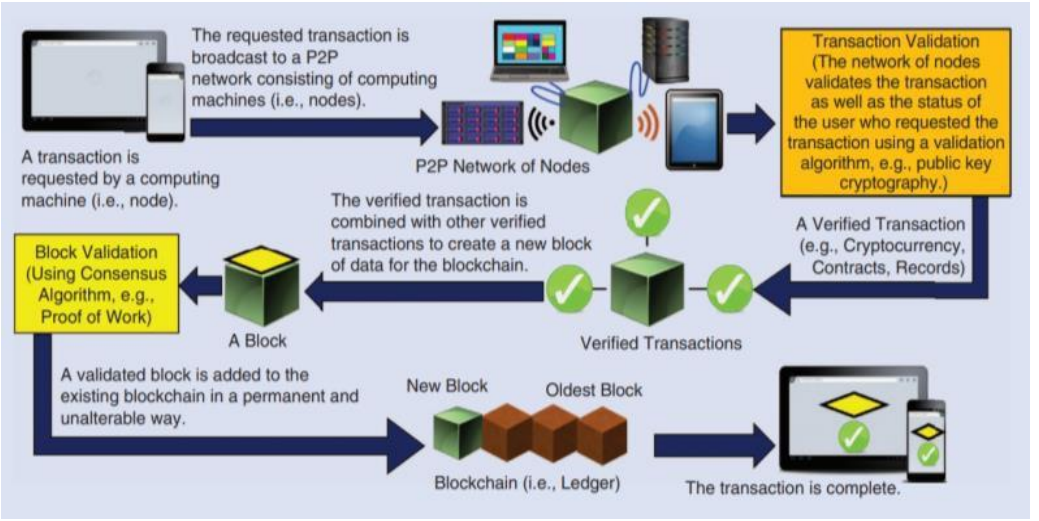

Figure 1 – Overview of blockchain

The whole blockchain transaction procedure is shown in Figure 1. A transaction's lifecycle inside a blockchain network is shown in the diagram. A computational node initiates the procedure by requesting a transaction. A P2P network of computers then receives this request. By using technologies like as public key cryptography, the network verifies both the user's status and the transaction. The transaction is added to the list of confirmed transactions after validation is complete. A fresh data block for the blockchain is generated from these validated transactions. A consensus technique, such Proof of Work, is used to further validate this block. The addition of a new block to the blockchain is an irreversible and permanent process that begins with validation. A series of interconnected blocks makes up the blockchain, which is sometimes called the ledger.

Blockchain processes are both continuous and cyclical, as seen in the figure. The P2P network, the validation of transactions, the production and validation of blocks, and the blockchain are all highlighted as essential components. This procedure guarantees that all transactions in a decentralised system are secure, transparent, and immutable. The graphic depiction illustrates how blockchain technology is decentralised and how consensus procedures are used to protect the network's integrity.

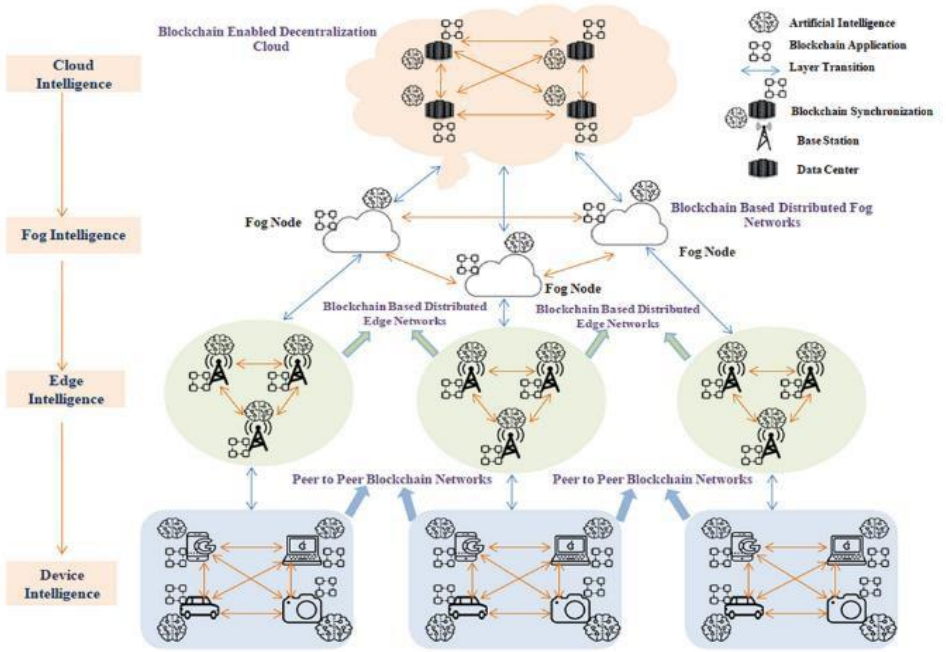

Figure 2 - The design overview of the proposed BlockIoTIntelligence Architecture

The figure presents a comprehensive design overview of a proposed Blockchain IoT Intelligence Architecture. This multi-layered architecture integrates blockchain technology with Internet of Things (IoT) devices and various levels of intelligence processing.

The architecture is structured into four main layers, from top to bottom:

1. Cloud Intelligence: At the top level, representing centralized, high-powered computing resources.

2. Fog Intelligence: The second layer, depicting a distributed network of fog nodes that act as intermediaries between the cloud and edge devices.

3. Edge Intelligence: The third layer, showing local processing units closer to the data sources.

4. Device Intelligence: The bottom layer, representing the IoT devices themselves, such as smartphones, cars, and other smart devices.

Distributed networks based on the blockchain are integrated into the fog and edge layers to improve decentralisation and security. Using decentralised, peer-to-peer blockchain networks to link devices at ground level, the design illustrates the information and intelligence flow across various tiers. Figures show the main parts, which include data centres, base stations, fog nodes, and other Internet of Things devices. Everywhere you look, especially at the fog and edge levels, you can see blockchain in action, which is a testament to its ability to facilitate safe, decentralised data processing and communication. An efficient, scalable, and safe framework for Internet of Things (IoT) applications may be achieved by integrating cloud, fog, edge, and blockchain technologies. The incorporation of blockchain technology ensures

security and decentralisation while intelligence is dispersed across all layers of the network, from centralised cloud resources to individual smart devices.

Examining the cybersecurity procedures of both cryptocurrency platforms and more conventional banks exposes different problems with similar remedies. The research sheds light on the distinct cybersecurity environments of different industries and emphasises the crucial role of AI in strengthening security protocols.

Exchanges for Digital Currency

Because of their decentralised structure and dependence on blockchain technology, cryptocurrency platforms encounter unique cybersecurity threats. While blockchain's immutability and transparency provide many security benefits, they also expose it to risks like smart contract issues and 51% assaults. The research shows that blockchain technology may still be exploited, even if it has built-in security measures to prevent certain threats using cryptography. The need for sophisticated security mechanisms and constant monitoring is brought to light by incidents like exchange breaches and wallet thefts. One potential solution is the use of artificial intelligence (AI) in cryptocurrency platforms. AI-powered machine learning algorithms may help identify suspicious activity and unusual trends in transactions. Problems associated with AI integration, including data privacy and algorithmic transparency, and the efficacy of AI solutions in this setting are ongoing developments.

Establishments of Conventional Banking

On the other hand, the cybersecurity threats associated with traditional financial organisations' centralised architecture are real. It is difficult to manage cybersecurity in an environment where there is dependence on outdated systems and when regulatory constraints are on the rise. The research highlights common dangers including insider threats, phishing, and ransomware, which are made worse by the large attack surface of integrated financial systems. Improved conventional banking cybersecurity, thanks to AI technology, has been seen in areas like real-time fraud detection and risk assessment. Predictive models powered by artificial intelligence and advanced analytics are being used more and more to spot dangers before they might affect operations. However, conventional financial institutions have difficulties in meeting regulatory requirements and integrating AI with current systems.

5. Findings from Comparisons

Several important findings are revealed by the comparison investigation. More and more, AI-driven solutions are being used by both cryptocurrency platforms and conventional banks to improve their cybersecurity measures. But these technologies' uses and effects differ greatly across the two fields. Traditional banks utilise AI for a wider variety of applications, including customer service, risk management, and compliance; cryptocurrency platforms mostly use it for transaction monitoring and fraud detection. Although AI has many useful applications, the research shows that it cannot solve all cybersecurity problems on its own. Security measures in both areas need constant reevaluation in light of new dangers.

6. Conclusion

The results provide a number of suggestions on how to improve cybersecurity in both industries. Improving incident response procedures and bolstering smart contract security should be top priorities for cryptocurrency platforms. To reduce security concerns associated with humans, traditional institutions should educate their employees continuously and focus on integrating AI with their current systems. Innovation in cybersecurity solutions and the exchange of best practices might also result from more cooperation between the cryptocurrency and conventional banking industries. To sum up, cybersecurity tactics need to be adaptable and forward-thinking since the threat environment is changing in both conventional banking and cryptocurrencies. AI technologies are essential for tackling these problems, but their use needs careful management to get the best results. Stakeholders may better safeguard financial systems from a dynamic variety of attacks by comprehending and resolving the distinct and common cybersecurity challenges of the two sectors.

References

1. Aydemir, M., & Aysan, A. (2023). Regulating the unregulated: The advent of Fintech regulations and their impacts on equity-based crowdfunding. BRICS Law Journal, 10(1), 4–18.
2. Baur, D. G., Hong, K., & Lee, A. D. (2018). Bitcoin: Medium of exchange or speculative asset? Journal of International Financial Markets, Institutions and Money, 54, 177–189.
3. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213–238.
4. Campbell-Verduyn, M. A. (2019). Introduction to special section on blockchains and financial globalization. Global Networks, 19(3), 283–290.
5. Casey, M. (2020). Money reimagined: Bitcoin and Ethereum are a DeFi double act. CoinDesk.
6. Casu, B., & Girardone, C. (2010). Integration and efficiency convergence in EU banking markets. Omega, 38(4), 260–267.
7. Chang, S. E., Luo, H. L., & Chen, Y. C. (2019). Blockchain-enabled trade finance innovation: A potential paradigm shift on using letter of credit. Sustainability, 12(1), 188.
8. Cheah, E. T., & Fry, J. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. Economics Letters, 130, 32–36.
9. Chen, Y., & Bellavitis, C. (2019). Decentralized finance: Blockchain technology and the quest for an open financial system. Stevens Institute of Technology School of Business Research Paper. Hoboken.
10. Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5–21.
11. Duchenne, J. (2018). Blockchain and smart contracts: Complementing climate finance, legislative frameworks, and renewable energy projects. In Transforming Climate Finance and Green Investment with Blockchains (pp. 303–317). Cambridge, MA: Academic Press.
12. Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. Journal of Monetary Economics, 95, 86–96.
13. Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: A literature review. Journal of Management Analytics, 7(4), 321–343.
14. Hasan, F., Al-Okaily, M., Choudhury, T., & Kayani, U. (2023a). A comparative analysis between Fintech and traditional stock markets: Using Russia and Ukraine WAR data.

Electronic Commerce Research. In press.
15. Hasan, F., Bellenstedt, M. F. R., & Islam, M. R. (2023b). The impact of demand and supply disruptions during the COVID-19 crisis on firm productivity. Global Journal of Flexible Systems Management, 24(1), 87–105.
16. Hasan, F., Kayani, U., Abdel-Razzaq, A. I., & Choudhury, T. (2022). Interest rate changes and dividend announcements effect on stock returns: Evidence from frontier economy. Pakistan Journal of Commerce and Social Sciences, 16(2), 639–659.
17. Huckle, S., & White, M. (2016). Socialism and the blockchain. Future Internet, 8(3), 49.
18. Kayani, U. (2023). Exploring prospects of blockchain and fintech: Using SLR approach. Journal of Science and Technology Policy Management. In press.
19. Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038.
20. Meiryani, M., Tandyopranoto, C. D., Emanuel, J. E., Lindawati, A. S. L., Fahlevi, M., Aljuaid, M., & Hasan, F. (2022). The effect of global price movements on the energy sector commodity on Bitcoin price movement during the COVID-19 pandemic. Heliyon, 8(6), e10820.
21. Mullen, T., & Finn, P. (2022). Towards an evaluation metric for carbon-emitting energy provenance of Bitcoin transactions. Paper presented at the Fourth ACM International Symposium on Blockchain and Secure Critical Infrastructure, Nagasaki, Japan, May 30–June 3 (pp. 11–21).
22. Nakamoto, S. (2018). Bitcoin: A peer-to-peer electronic cash system. Computer Science.