e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

SECURING MODERN FINANCIAL BANKING SYSTEMS WITH BLOCKCHAIN: A MULTI-LAYERED ARCHITECTURE FOR TRUST, COMPLIANCE, AND SCALABILITY

Surendra Kumar Pandey*1

*1Computer And Information Technology Tata Consultancy Services Atlanta, USA.

DOI : https://www.doi.org/10.56726/IRJMETS67094

ABSTRACT

Securing efficient and transparent operations are of utmost priority to the Financial Banking sector. The core of applying Blockchain technology to modernize and strengthen up the security in banking industry lies in the decentralization, immutability, cryptography, and consensus. This paper analyzes the use of blockchain for different banking processes such as cross border payments, managing digital asset, and fraud detection. Further, we discuss how the advantages, challenges, and the findings of those that seek to implement blockchain for financial services. While security, trust, and cost optimization are promising advantages of blockchain in the banking domain, the widespread adoption of blockchain in the banking domain is still measured due to the barriers of regulatory, scalability and interoperability. Challenges associated with such secure and seamless transaction are explored in this paper and the possible research pathways identified with its potential application in future.

Keywords: Blockchain, Modern Banking Infrastructure, Consensus Mechanism, Distributed Ledger Technology.

I. INTRODUCTION

Throughout its history the modern financial banking sector has always been on the forefront of the application of innovative technology to ensure security of its customers data and simplify transaction processes. Financial institutions in the past have relied on almost centralized databases and legacy infra structures that were very robust, but it becomes more and more challenges to these entities to take care of the very sophisticated cyber threats. Like traditional approaches, efforts to resolve such issues as slow cross border payments, high cost of intermediaries and lack of transparency in settlement processes have also been made. In turn, the industry has started exploring and adopting the use of blockchain based technology conceived to facilitate the currency represented in a digital form instead of traditional cryptocurrencies.

The unique characteristics of Blockchain, i.e. immutability, decentralization, and cryptographic security make it perfectly position a lot of pains points related to the banking domain [1]. This is a means to keep transparent audit logs, lower the risk of having software-related single points of failure, and create a better cooperative transactional ecosystem in the financial world. Blockchain also helps multiple parties to validate and confirm transactions while minimizing the heavily reliance of an intermediary, causing reduction in operational costs and settlement time [2].

But the space of financial services is complicated, and subject to the asperous mold of regulations and standards (for instance, Know Your Customer (KYC), Anti Money Laundering (AML) or some other compliance schemes) [3]. However, to integrate blockchain solutions into legacy infrastructures, the mandates of the regulation must be addressed, the legacy systems should be interoperable with each other, and the scalability should be achieved for high transaction volumes [4]. In addition, banks must determine data privacy questions when applying distributed ledger approach and manage permissioning models that can fit in different types of users. The major contributions of this work are as follows:

- This work presents a comprehensive blockchain-based architecture that includes five layers for Banking Infrastructures to increase security
- This work highlights the major advancements in the field of Banking sectors related to the use of Blockchain within operations such as information security, and communication risks.
- This work presents a in-depth overview of various components of Blockchain that are utilized for the enhanced security of Banking organizations

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

- This work provides an overall comparison in the areas of improvements compared from traditional banking infrastructure to blockchain-based

The rest of the paper is organized as follows. Section 2 presents a Literature Review that highlights the previous studies and research conducted within the banking sector based on Blockchain. Section 3 presents a comparison between the traditional banking infrastructure to the modern Blockchain based infrastructure. Section 4 presents an in-depth overview of Blockchain and its various use cases along with components. Section 5 presents a five-layer architecture based on Blockchain technology for the Banking industry. Section 6 concludes itself with a conclusion and future research directions.

II. LITERATURE REVIEW

Chorey et al. [5] presented checkpoint model utilizing consensus algorithm based on Blockchain for monitoring several transactions in a banking organization and improved security. Ghosh et al. [6] proposed a framework to be implemented in Corda for banking sector based on Blockchain that resolves issues related to sharing unauthorized information and customer communication. Lu et al. [7] presented various methods based on Blockchain technology that can be implemented in several Taiwan bank organizations.

Al-khawaja et al. [8] highlighted blockchain based methods to improve security of information within banking organizations in America. Quamara et al. [9] provided a in-depth explanation of how blockchain has improved previous banking operations with enhanced security and overcome issues related to compliance. Mishra et al. [10] highlighted the use of blockchain for modeling critical success factors in strong banking processes. Bruno et al. [11] presented a research based on qualatative reasoning regarding the use of blockchain in banking organizations to be seen as an issue and resolution.

Table 1: Recent Developments In The Use Of Blockchain For Banking Infrastructures

Reference	Year	Contribution
Chorey et al. [5]	2024	presented checkpoint model utilizing consensus algorithm based on Blockchain
Ghosh et al. [6]	2023	proposed a framework to be implemented in Corda for banking sector based on Blockchain
Lu et al. [7]	2024	presented various methods based on Blockchain technology that can be implemented in several Taiwan bank organizations
Al-khawaja et al. [8]	2025	highlighted blockchain based methods to improve security of information within banking organizations in America
Quamara et al. [9]	2024	provided a in-depth explanation of how blockchain has improved previous banking operations
Mishra et al. [10]	2023	highlighted the use of blockchain for modeling critical success factors in strong banking processes
Bruno et al. [11]	2024	presented a research based on qualatative reasoning regarding the use of blockchain in banking organizations

III. MODERN FINANCIAL BANKING SYSTEM

New businesses have emerged, filled by banks once established in an industry defined by local, paper-based recordkeeping that now allows banks to deliver real time services to customers globally [12]. While transitioning from mainframe-based operations to internet powered platform, they bring with them convenience as well as novel vulnerabilities, to the latter especially because cyberattacks are becoming more and more sophisticated. In addition, global transactions of all kinds take place with astounding speed across borders — but are held back by clunky, out of date regulations that constitute new compliance hurdles and operational complexity [13]. This requires understanding the change in banking infrastructure over the past few decades, identifying the spots of security issues that persist, and realizing that this maybe the moment

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

when a distributed solution can offer a solution. In the remainder of this subsections, these developments are further explored.

A. Evolution of Banking Infrastructure

In recent decades, there have been multiple technological revolutions of the banking landscape. Early implementations nearly always dealt with centralized mainframe systems to process daily transactions, store account information, evaluate credit and more. As the internet came into existence, banks started to process web-based services for customers to access their accounts, transfer funds, pay bills through the internet [14]. In this transformation, real time payment capabilities were introduced which facilitated the bringing of banking services as fast and wide as possible, beyond geographical boundaries. These innovations brought unprecedented convenience and, at the same time, new forms of the cyber threats which put stress on the traditional security protocols.

The changes in infrastructures have also been accompanied by a change in regulatory requirements that correspond to the former. Due to the clamping down of financial institutions to stringent data protection laws, anti-money laundering norms, and real time risk reporting obligations etc. by central banks and international bodies, financial institutions must now work on data for purposes of compliance as well [15]. As a result, they find themselves caught between the necessity to meet the current demands of the modern digital services and the lack of capacity in both the modern legacy foundation which was never intended to be continuously monitored for such real time oversight nor the volume of global digital transactions present in our current financial environment.

B. Current Security Challenges

While modern banking is prone to setbacks in the form of large-scale breaches and complex cyberattacks, it nevertheless has been made somewhat more secure over the years thanks to steps such as greater encryption, network monitoring, and fraud detection, suggesting that theft rate has probably not risen as justly [16]. That said, centralization is the recent emphasis of cryptocurrency, in that it essentially relies on centralized ledgers—meaning a ledgers compromise is exactly that: a compromise of massive amounts of sensitive customer data. Cross border transactions also involve multiple correspondent banks whereby each intermediary layer introduces additional layers of intermediary and vulnerabilities throughout the payment chain. Usually, these processes lack transparency for end users to know whether their transactions are undisputed, or the cost associated with them at an early stage.

Traditional architectures are rarely up to speed with the vast amount of regulatory bodies requirement such as, onerous record keeping, regular audits and instant reporting of suspicious activities. Legacy systems are in many cases set up in very simple silos, putting parts of the data into a variety of formats and platforms. As a result of this division though, inter department collaboration is also hindered as is external oversight which raises unidentifiable threats to overlooked blind spots. These blind spots and cumbersome manual reconciliation workarounds give opportunity to fraudsters to steal customer and GDPR sensitive information, and inconsistent data trails go against the trust that stakeholders have in the data [17].

C. Emergence of Distributed Solutions

In response to these challenges, banks as well as fintech firms have come to realize that the established data management, operational security, and reconciliation delays are ripe for change and have begun to observe the promise of distributed ledger technologies (DLTs) including blockchain [18]. However, one of the main reasons for the emergence of DLTs is that this is completely different from the legacy models, where a single centralized repository of truth has always been the norm. What is instead done, is that there is a replicated copy of transaction data at each node in a distributed network such that the data set at every node form a single source of truth determined through a consensus process. Particularly, this structure largely eliminates the need for confirmation of data across different intermediaries.

It is through key attributes such as cryptographic hashing, public key signatures, and consensus mechanisms that ensure the DLT's tamper resistance making unauthorized modification of a block very, very easy until the network sets ample consensus on the validity of the block. While bringing blockchain into the world of existing banking applications entails the compromises in terms of governance, compliance, and performance expectations, an emerging industry concurrence in piloting initiatives and consortia demonstrates that a

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

distributed solution will lend the industry solutions to the problems that have dogged traditional architectures over long [19].

IV. BLOCKCHAIN IN FINANCIAL SERVICES

Under the brutal conditions of centralized data silo and multi layered regulatory framework, blockchain technology has thrown themselves into the place where a more sound and upright financial interaction. Blockchain attempts to avoid large scale breach points (i.e. something that historically have allowed large scale breach) by decentralizing the validation process and cryptographically encrypting each transaction both to a shared ledger [20]. In terms of banks, it could mean reducing intermediary costs as well as settlement times, and a verifiable chain of custody for every financial event. However, this calls for a delicate balance between opening the blockchain's openness for use and maintaining customers' privacy, which then raises importance of the carefully selected consensus mechanisms and advanced cryptographic methods. The next subsections deliver into the market of blockchain and its role in banking.

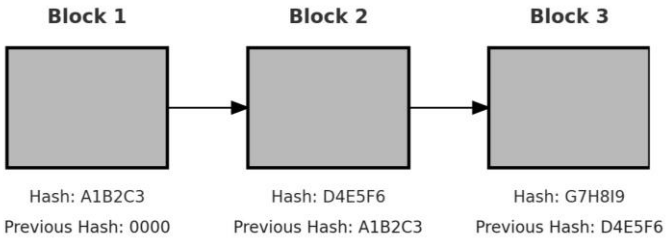

Fig. 1. Blockchain Workflow Diagram

A. Decentralized Trust for Financial Transactions

In the simplest terms, blockchain makes it possible for a trustless model where there is no single central authority or centralized database to put one's trust in. A new transaction of either transferring money, certifying a loan agreement, etc. of any kind is broadcast by each node who is authorized by it to the network [21]. These nodes check transaction details with cryptographic methods so that offenders cannot impersonate other parties. In the context of banking, decentralized trust can reduce the choke point largely induced by the clearinghouses or correspondent banks to have fewer points of systemic failure and faster settlements.

This means that decentralized trust has the advantage that it can reconcile conflicting ledgers. Typical banking workflows experience dispute when the independent databases get out of sync because of technical snag or man error. Blockchain's consensus provides the base mechanism to have one single agreed upon version of truth go through the network without actually the need of doing extensive post transaction audit [22]. It also offers transparency, making it transparent to participants to know the exact log of the financial activities.

B. Consensus Mechanisms

The initial implementation of blockchain, consensus protocols such as Proof of Work (PoW), while necessary, also proved to be too resource-intensive but were very poor to meet the regulated financial environments. Therefore, banks began to shift their interest towards alternatives, like Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT) or Proof of Staking (PoS) [23]. They are permissioned protocols, meaning only a curated set of nodes, i.e. consortium members or by default: approved validators may propose and validate new blocks. Because participants are known and somewhat known, these algorithms do not require too much computation overhead and are also faster than the transaction throughput.

A wrong consensus mechanism is a function of the transaction volume, geographical distribution of nodes and degree of doubt between participants. PBFT variants suited to low latency environments may be chosen by some financial consortia to achieve thousands of transactions per second. For others, PoA makes sense in order to capitalize on a subset of highly reputable entities, such as central banks or large financial institutions, to validate the blocks. These streamlined approaches can provide such a level of performance as these centralised systems, while they retain a degree of decentralisation enough to maintain data integrity [24].

C. Privacy and Compliance Requirements

Keeping the balance between transparency of the ledger and strict confidentiality rules governing customer data is one of the most important hurdles to make blockchain usable in finance. One of the most notable

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

characteristics of public blockchains such as Ethereum is that they store transaction details globally in a nonprivate manner, for example, it is possible to see all transaction data, this is clearly in conflict with bank secrecy and client confidentiality preferences. To address these concerns, permissioned and private blockchains try preventing these troubled patches through control of who joins the network and can see transaction details [25]. Moreover, more sophisticated forms of cryptographic instruments—namely, zero knowledge comes—allow for the legitimization of a transaction news and prevent the identification of its sensitive information.

This also becomes a complication with the Anti Money Laundering (AML) and Know Your Customer (KYC) regulations [26]. Reliable fund origin and destination identification and automated marking of suspicious transactions must be performed by banks. However, these rules are difficult to embed into on chain smart contracts or special software module due to duplication of work, complexity and the question of data retention, version control and auditing rights. Thus, a suitable banking blockchain solution needs to incorporate flexible permissioning and the compliance logic needs to be integrated into it to overcome the stiff demand of various regulators around the globe.

D. Smart Contracts in Banking

Blockchain is only about recording transactions, but the scripts can be programable (commonly called smart contracts) and events automate certain actions occurring based on certain criteria. Therefore, smart contracts are promising the completion of the complex products such as syndicated loans, derivatives or trade finance agreements in the financial area. Much of the time these instruments take the form of more than one party, with its own set of documentation, conditions and timeline. By using a well-designed smart contract, it will be possible to track these variables on chain and to automatically release payments, release collateral or trigger penalties without manual intervention [26]. By automating this, error rates are decreased, and every action is cryptographically traced; thus, building both high transparency and trust.

Nevertheless, banks need to be careful that smart contracts encoded in these banks doesn't have exploits which may endanger funds or expose secret business logic. Along with smart contracts, the ability to combine smart contracts with off chain oracles, trusted data feeds off the blockchain, also enables the solution of other use cases such as a behavior conditioned of real time events (e.g. changes in interest rates or commodity prices).

V. ARCHITECTURE FOR SECURE BANKING WITH BLOCKCHAIN

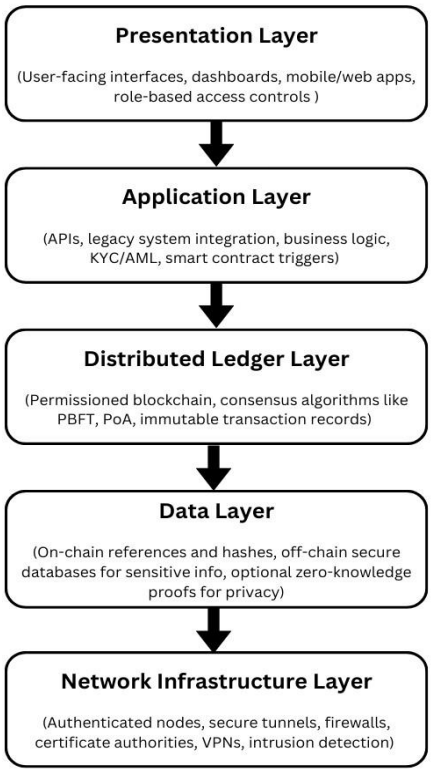

Fig. 2. Five-layer Blockchain-based Architecture for Banking Infrastructure

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

Any compelling strategy for the blockchain in banking must be in a perfect alignment with the financial structural layers that underlie the existing financial operations. This framework is not one that replaces old and established systems by throwing away the old and adopting the new; instead, it integrates blockchain components into different layers of the technology stack to keep legacy systems functioning as usual with their core functions of customer data management, transaction validation and regulatory compliance ticking over. Instituted through partitioning the bank's infrastructure into layers of distinct, but interdependent, working, deploying blockchain capability becomes possible in a structured fashion which secures the bank, enhances the bank process, and supports changing demands. Next, each segment of this multi layer architecture is broken down in the following subsections as each segment of this architecture has been permeated with blockchain technology to form a more complete architecture.

A. Network Infrastructure Layer

The network infrastructure layer is the foundation of a permissioned blockchain in banking. In this case firewalls, encrypted tunnels and access policies conforming to internal security frameworks connect every node (a branch office, a partnering institution, a regulatory body), which allows good transfer of information. Public keys of each node are verified by trusted certificate authorities and issued public key certificates in order to allow only approved entities to join the network. Admittedly, this is not only an environment controlled by us (i.e. we don't allow unauthorized intrusion), but it is an environment in which each node's identity is proven and maintained. With carefully controlled access to the network, banks are assured that no one will tamper or intercept a transaction data or verification message that's been exchanged.

B. Application Layer

The secure network infrastructure is built upon which all operational workflows are orchestrated in the application layer — such as account creation, loan disbursements, compliance checks — and enabled to interact with the blockchain. The ledger is connected to legacy core banking systems as well as to digital channels eg) mobile and web applications using standardised APIs which encapsulate blockchain logic behind familiar service end point. By virtue of having this, staff and customers will be able to enjoy the tamper resistant properties of the ledger without going down low level blockchain stuff. This is where smart contracts live as well, yet their enemy is an automatic response to certain financial events or risk thresholds. Internal modules also have the responsibility of knowing your customer (KYC) and anti-money laundering (AML) screening to ensure that transaction requests comply with legal standards before being sent to the blockchain queue.

C. Distributed Ledger Layer

The blockchain protocol is hosted on the distributed ledger layer at the core of this architecture, which includes the main point of a blockchain. In such banking context permissioned consensus mechanisms (e.g. Practical Byzantine Fault Tolerance, PBFT; or Proof of Authority, PoA) replace mostly energy intensive Proof of Work approach. Incoming transactions are verified by each authorized node on its own and each authorized node contributes to block production to maintain consistency of the network's data. At well, blocks are cryptographically linked to the previous ones to form a data non-changeable record all the financial events. Redundancy and transparency are used here to ensure this risk of changing the ledger is minimal, since the attacker has to have control over a majority of nodes to rewrite it. This in addition to provide configurations in the ledger that enable specialized regulator nodes the ability to conduct real time auditing without impacting transactional throughput and also providing oversight without exposing customer information to the whole network.

D. Data Layer

The data layer of blockchain balances immutability with robust privacy controls needed with banks because banks have to be cautious about retaining large quantities of highly confidential information. Essentially, on chain records tend to include basic digital transaction data as with cryptographic proofs to maintain their light footprint while ensuring that event integrity. At the same time, more sensitive or bulky information, for instance customer identification documents or complex dossier documents that can't be stored on chain, may be externalized off chain to secure databases maintained by the bank itself. Hashes or refers to that can be stored on the blockchain and is used to prove that off chain data is not tampered with. This hybrid model is a fairly balanced one, firstly the blockchain stands for indelible transcriptal records and secondly and most important

the repositories offering safe off chain storage for personal data. There is also space to use additional features to validate transactions while keeping this data as hidden, minimizing data and meeting the privacy principles.

E. Presentation Layer

The topmost presentation layer enables users to click on blockchain-based services by intuitive interfaces and interact with blockchain based services from bank employees, customers or outside regulators. The account holders are able to send payment request, track transaction status, and account information in the personal financial dashboards using web portals and mobile applications. Role based dashboards helps internal staff to see their real time flow of transaction, investigative tools for if it is flagged activity, or a simple analytics of how network is healthier in the end. Special views to aggregate risk indicators and compliance alerts may have been created by regulatory officers to facilitate tasks of oversight. Aside from being tailored to a user's specific permission level (teller gets only what is manageable on a daily basis, executive management and auditors have access to significantly more system wide metrics), this is really critical. The presentation layer clearly delineates roles and privileges, maintaining security in usability without sacrificing functionality on the blockchain, so that the application of blockchain driven functions improves both internal workflow and customer experience alike.

VI. CONCLUSION

This is where blockchain becomes a solution that could furnish financial services with security and transparency on such high demand by modern banking. The banks distribute the validation process over multiple authorised nodes, implement cryptographic defensive measures to minimize dependency on centralized intermediaries and greatly diminish single point of failures. It also provides a base for real-time monitor of transactions, and audit trails and build more confidence with stakeholders. Yet, when blockchain (or some equivalent technology) is embedded into core banking systems, it runs into a number of practical and theoretical challenges that need still further inquiry. Another hurdle which becomes more and more of a barrier to scalability as major financial networks have high transaction throughput characteristics to be overcome is scalability. Similarly, sophisticated cryptographic techniques are necessary to guarantee that sensitive data can indeed not be exposed to unauthorized entities. On the other hand, regulatory compliance in a decentralized environment requires a clear indication of how central banks and financial authorities can incorporate their mandates with two ledger frameworks.

Aiming to look forward, the research that pits blockchain's role as a financial institution will lean on advanced consensus protocols, private technologies, and inter opterable blockchain networks. Such defense would be even more robust if there were, however, enhanced synergy between the conventional bank processes and decentralized design principles. Here we see how financial industry is eager to make use of this growing portfolio of blockchain solutions in order to transform banking services to offer new generation of consumers and businesses speed, transparency and security.

VII. REFERENCES

[1] M. Kour, "Blockchain Technology Changing Landscape of Banking Industry," 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2023, pp. 12121216, doi: 10.1109/ICAAIC56838.2023.10140854.

[2] H. Bhat, G. Bank, Y. Jawale, R. Wairkar and S. Mirchandani, "Decentralized Banking Services using Blockchain Technology," 2023 8th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2023, pp. 515-521, doi: 10.1109/ICCES57224.2023.10192758.

[3] Pandey, S., Bhushan, B. Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks. Wireless Netw 30, 2987–3026 (2024). https://doi.org/10.1007/s11276-024-03714-4

[4] H. Xia and B. Li, "Construction of Credit Bank System Based on Blockchain Technology," 2022 International Conference on Industrial IoT, Big Data and Supply Chain (IIoTBDSC), Beijing, China, 2022, pp. 334-337, doi: 10.1109/IIoTBDSC57192.2022.00068.

[5] Chorey, P.A., Sahu, N. Enhancing Banking Transaction Security with a Hybrid Access Control Consensus Algorithm Through BlockchainEnabled Checkpoint Model. SN COMPUT. SCI. 5, 776 (2024). https: //doi.org/10.1007/s42979-024-03128-1

[6] Ghosh, A., Mukhopadhyay, I. Chakraborty, S. ConsenTrack—Blockchain Based Framework for Open Banking Consent Data Tracking. Hum-Cent Intell Syst 3, 105–122 (2023). https://doi.org/10.1007/s44230-023-00023-5

[7] Lu, YH., Yeh, CC. Kuo, YM. Exploring the critical factors affecting the adoption of blockchain: Taiwan's banking industry. Financ Innov 10, 23 (2024). https://doi.org/10.1186/s40854-023-00523-0

[8] Al-khawaja, H.A., Aburub, F.A. Blockchain for Securing Data Storage in Digital Banking Services. SN COMPUT. SCI. 6, 56 (2025). https: //doi.org/10.1007/s42979-024-03596-5

[9] Quamara, S., Shelke, N.A., Kitukale, G. (2024). Adoption of Blockchain in Banking Industry: Challenges and Perspectives. In: Tanwar, S., Singh, P.K., Ganzha, M., Epiphaniou, G. (eds) Proceedings of Fifth International Conference on Computing, Communications, and CyberSecurity. IC4S 2023. Lecture Notes in Networks and Systems, vol 991. Springer, Singapore. https://doi.org/10.1007/978-981-97-2550-2 64

[10] Mishra, R., Singh, R.K., Kumar, S. et al. Critical success factors of Blockchain technology adoption for sustainable and resilient operations in the banking industry during an uncertain business environment. Electron Commer Res (2023). https://doi.org/10.1007/s10660-023-09707-3

[11] Bruno, E., Iacoviello, G. (2024). Blockchain and Lending Process Efficiency in the Banking Industry. In: Braccini, A.M., Pallud, J., Pennarola, F. (eds) Technologies for Digital Transformation. ItAIS 2022. Lecture Notes in Information Systems and Organisation, vol 64. Springer, Cham. https://doi.org/10.1007/978-3-031-52120-1 6

[12] Pandey, S., Kumar De, A., Choudhary, S., Bhushan, B., Bhatia, S. (2023). Leveraging Blockchain Technology in Industry 4.0 and Industrial Internet of Things (IIoT) Scenarios. In: Sharma, D.K., Sharma, R., Jeon, G., Polkowski, Z. (eds) Low Power Architectures for IoT Applications.

[13] Springer Tracts in Electrical and Electronics Engineering. Springer, Singapore. https://doi.org/10.1007/978-981-99-0639-0 12

[14] S. Sakho, Z. Jianbiao, F. Essaf and K. Badiss, "Improving Banking Transactions Using Blockchain Technology," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1258-1263, doi: 10.1109/ICCC47050.2019.9064344.

[15] V. Nakonechnyi, S. Toliupa, V. Saiko, V. Lutsenko, G. S. N. Ghno and A. K. Hussain, "Blockchain Implementation in the Protection System of Banking System During Online Banking Operations," 2024 35th Conference of Open Innovations Association (FRUCT), Tampere, Finland, 2024, pp. 492-500, doi: 10.23919/FRUCT61870.2024.10516404.

[16] S. V and N. Suganthi, "Blockchain application in preserving authenticity and enabling transparency in the approval of loans for the clients in banking system," 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2023, pp. 1-5, doi: 10.1109/ICAECA56562.2023.10200205.

[17] Juyal, A., Bhushan, B., Hameed, A.A., Jamil, A., Pandey, S. (2024). Automated and Optimised Machine Learning Algorithms for Healthcare Informatics. In: Garc´ıa Marquez, F.P., Jamil, A., Ramirez, I.S., Eken,´ S., Hameed, A.A. (eds) Computing, Internet of Things and Data Analytics. ICCIDA 2023. Studies in Computational Intelligence, vol 1145. Springer, Cham. https://doi.org/10.1007/978-3-031-53717-2 43

[18] S. Joseph and S. Karunan, "A Blockchain Based Decentralized Transaction Settlement System in Banking Sector," 2021 Fourth International Conference on Microelectronics, Signals Systems (ICMSS), Kollam, India, 2021, pp. 1-6, doi: 10.1109/ICMSS53060.2021.9673610.

[19] K. Singh, P. K P, S. Benakatti and V. Srivatsa, "Revolutionizing Digital Banking: Harnessing Blockchain Smart Contracts for Enhanced Security and Efficiency," 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/SMARTGENCON60755.2023.10442642.

[20] S. Pandey, A. K. De, S. Choudhary and M. Asim, "A Decentralized Blockchain-Based Architecture for Healthcare Industry," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-5,

doi: 10.1109/ICAIIHI57871.2023.10489491.

[21] R. Washimkar, A. D. Vibhute and S. Joshi, "A Short Review of Blockchain Technology in the Banking and Financial Sectors," 2023 International Conference on Integration of Computational Intelligent System (ICICIS), Pune, India, 2023, pp. 1-6, doi: 10.1109/ICICIS56802.2023.10430252.

[22] A. Sharma and M. Damle, "Blockchain Technology: Reinventing the Security and Efficiency posture of the Indian Banking System," 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), Bengaluru, India, 2022, pp. 364-369, doi: 10.1109/IIHC55949.2022.10060224.

[23] N. R. Bagrecha, I. Mustafa Polishwala, P. A. Mehrotra, R. Sharma and B. S. Thakare, "Decentralised Blockchain Technology: Application in Banking Sector," 2020 International Conference for Emerging Technology (INCET), Belgaum, India, 2020, pp. 1-5, doi: 10.1109/INCET49848.2020.9154115.

[24] Pandey, S., Baniya, P., Nand, P., Hameed, A.A., Bhushan, B., Jamil, A. (2024). CryptStego: Powerful Blend of Cryptography and Steganography for Securing Communications. In: Garc´ıa Marquez, F.P., Jamil,´ A., Hameed, A.A., Segovia Ram´ırez, I. (eds) Emerging Trends and Applications in Artificial Intelligence. ICETAI 2023. Lecture Notes in Networks and Systems, vol 960. Springer, Cham. https://doi.org/10. 1007/978-3-031-56728-5 44

[25] M. Attia and A. H. Abed, "A Comprehensive Investigation for Quantifying and Assessing the Advantages of Blockchain Adoption in Banking Industry," 2024 6th International Conference on Computing and Informatics (ICCI), New Cairo - Cairo, Egypt, 2024, pp. 322-331,
doi: 10.1109/ICCI61671.2024.10485028.

[26] B. Jaber, D. Kriwiesh and M. A. AlRagheb, "A Blockchain Framework in the Banking Sector Based in e-KYC System Conceptual Framework," 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2024, pp. 1-4, doi: 10.1109/ICCR61006.2024.10532852.

[27] Pandey, S., Bhushan, B., Hameed, A.A. (2024). Securing Healthcare 5.0: Zero-Knowledge Proof (ZKP) and Post Quantum Cryptography (PQC) Solutions for Medical Data Security. In: Reddy, C.K.K., Sithole, T., Ouaissa, M., OZER,¨ O., Hanafiah, M.M. (eds) Soft Computing in¨ Industry 5.0 for Sustainability. Springer, Cham. https://doi.org/10.1007/ 978-3-031-69336-6 15