e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:01/January-2024 Impact Factor- 7.868 www.irjmets.com

A COMPREHENSIVE STUDY ON BENEFITS AND CONCERNS OF BLOCKCHAIN IN SECURITY AND COMPLIANCE IN BANKS

Deepa Ajish[*1]

[*1]IT Security and Compliance Architect, Service Now Automation Leader, Los Angeles, California.

DOI : https://www.doi.org/10.56726/IRJMETS48632

ABSTRACT

This thesis aims to explore the transformative potential of blockchain technology in reshaping the landscape of the banking and financial industry in terms of security, compliance, and risk mitigation. The research will provide a comprehensive review of the literature to assess the potential ramifications of blockchain technology, delve into its merits and demerits, and offer a balanced perspective on its implications for the future of banking and financial services.

Blockchain technology has the capability to enhance security and foster trust by offering a secure and transparent platform for transactions. By significantly reducing human error and making transactions tamper-proof, blockchain can fortify security measures and mitigate risks within the financial sector. Additionally, the digitization and tokenization of financial products can simplify trading, promote inclusivity, increase connectivity, and reduce capital costs.

However, the adoption of blockchain technology in the banking industry poses regulatory challenges and scalability issues. While offering numerous benefits, blockchain requires careful evaluation and planning to mitigate potential pitfalls and maximize its advantages. As the technology continues to evolve and mature, it is crucial for banks to carefully weigh the pros and cons of integrating blockchain into their security and compliance strategies for effective and responsible harnessing of its power.

Keywords: Blockchain technology, Banking industry, Security and compliance, Decentralized digital ledger, Cyberattacks, Cybersecurity

I. INTRODUCTION

In the contemporary era, blockchain technology has emerged as a focal point in the financial realm, especially within banking institutions that are exploring its potential to bolster security and compliance protocols. Blockchain, a decentralized digital ledger, securely and transparently records and authenticates transactions. Its inherent characteristics of immutability and resistance to tampering position it as a prospective tool for tackling the security and compliance hurdles encountered by banks. Nevertheless, like all nascent technologies, it presents both benefits and drawbacks when applied in the banking sector. This paper endeavors to deliver an exhaustive analysis of the pros and cons associated with the utilization of blockchain for security and compliance in banking.

In the modern digital age, the dependence on digital services has seen a significant surge. This increased reliance has inadvertently exposed banks and financial institutions to a heightened risk of cyberattacks. As these organizations transition towards more digital platforms to offer their services, the potential points of vulnerability multiply, making them attractive targets for cybercriminals.

Cyberattacks can lead to substantial financial losses, damage to reputation, and loss of customer trust, which can be devastating for financial organizations. Moreover, the sophistication and frequency of these attacks are also on the rise, further exacerbating the situation.

Therefore, it is of paramount importance for these organizations to invest in robust cybersecurity measures [1]. This includes the implementation of advanced security protocols, regular system updates, employee training, and the establishment of a responsive incident management system. By doing so, banks and financial organizations can better safeguard their digital services and maintain the trust of their customers in the digital age. Research by IBM X-Force reveal that in 2021, a significant 70% of cyberattacks on financial institutions (FI) were directed at banks, with insurance companies being the target of 16% of the attacks, and the remaining 14% affecting other financial institutions [2]. A report by the Boston Consulting Group (BCG) indicates that financial services (FS) are 300 times more likely to fall victim to a cyberattack compared to other sectors [3].

The finance sector exhibits a high level of concern regarding cyber threats. A survey conducted by the Conference of State Bank Supervisors (CSBS) in September 2021 found that over 80% of bankers rated cybersecurity risk as “extremely important”, marking it as the top internal risk. This rating is more than double that of any other operational risk category and shows a significant increase from the 60% reported in the previous year [4].

The advent of internet banking, with its inherent convenience, has positioned it as one of the most efficient and expedient methods of conducting banking transactions. Consequently, digital banking has surfaced as a recent innovation, enabling banking operations to be executed via digital platforms. However, this digital transformation is not devoid of challenges, with cyber threats being a significant concern [5]. Given the high visibility and critical nature of their services, banks are particularly vulnerable to cyberattacks. Consequently, managing cyber risk has become a paramount concern for banking supervisors [1]. To safeguard users during their internet banking activities, it is incumbent upon banks to devise and implement novel strategies to counteract these emerging threats [5].

However, it is also crucial to note that cybersecurity is not a one-time solution but a continuous process of adaptation and improvement, given the ever-evolving nature of cyber threats. Hence, constant vigilance, timely upgrades, and proactive measures are the need of the hour in the fight against cyberattacks in the banking and financial sector.

A research by Statista Research Department published in May 2021 says that, in 2018, the market size for blockchain solutions tailored for the banking system and financial institutions was approximated at 0.28 billion U.S. dollars. The utilization of blockchain technology within the financial sector is anticipated to undergo substantial growth in the forthcoming years, with projections estimating the market size to escalate to approximately 22.5 billion U.S. dollars by 2026. This significant increase underscores the transformative potential of blockchain technology in reshaping the landscape of the financial industry [6].

Blockchain, an emergent technology, has garnered interest across various sectors due to its capacity to enhance security and foster trust. Blockchain harbors the potential to revolutionize the banking and financial industry by offering a secure and transparent platform for conducting transactions. However, the integration of blockchain within the financial sector necessitates a comprehensive overhaul of existing systems and processes. The deployment of blockchain technology can fortify security measures and mitigate risks, thereby benefiting both financial institutions and their clientele. This underscores the transformative potential of blockchain in reshaping the financial landscape while ensuring enhanced security and reduced risk exposure [7].

1. Purpose

The objective of this thesis is to augment the existing body of knowledge and foster a deeper comprehension of the potential application of blockchain technology as a mechanism to bolster security and mitigate risks within the industry. To fulfill this objective, the primary aim of this thesis is to undertake an exhaustive review of the literature to assess the potential ramifications of blockchain technology. This thesis will delve into the merits and demerits of employing blockchain technology in the realm of cybersecurity and compliance within the banking industry. By doing so, it seeks to provide a balanced perspective on the transformative potential of blockchain technology and its implications for the future of banking and financial services.

II. BACKGROUND OF BLOCKCHAIN TECHNOLOGY

1. Blockchain technology

Blockchain technology, is a decentralized digital ledger that securely records and verifies transactions across multiple computers. The fundamental principle underpinning blockchain technology is that it allows multiple parties to reach consensus without the need for a central authority. Each transaction recorded on the blockchain is stored in a data structure known as a block [8]. These blocks are linked together in a chronological order, forming a chain, hence the term “blockchain” [9]. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data, ensuring the integrity and authenticity of the information [10]. Figure 1 shows the architecture of blockchain technology and figure 2 illustrates how blockchain works. One of the most notable features of blockchain technology is its immutability. Once a transaction is recorded on the blockchain, it cannot be altered or deleted, providing a transparent and tamper-proof record of transactions [11]. This feature is particularly valuable in scenarios where trust, transparency, and security are paramount.

Furthermore, blockchain technology employs advanced cryptographic techniques to ensure the security and privacy of transactions. This includes the use of public-key cryptography, where each participant has a pair of cryptographic keys - a public key that is openly shared and a private key that is kept as secret. This mechanism ensures that only the owner of the private key can initiate transactions, providing a secure method for authentication and encryption [10].

In conclusion, blockchain technology, with its decentralized nature, immutability, and advanced cryptographic security, presents a transformative potential across various sectors, including finance, supply chain management, healthcare, and more. However, like any technology, it also poses challenges and limitations that need to be addressed for its widespread adoption and effective implementation. These include issues related to scalability, energy consumption, regulatory acceptance, and integration with existing systems. Despite these challenges, the potential benefits of blockchain technology make it a promising solution for many applications [12].

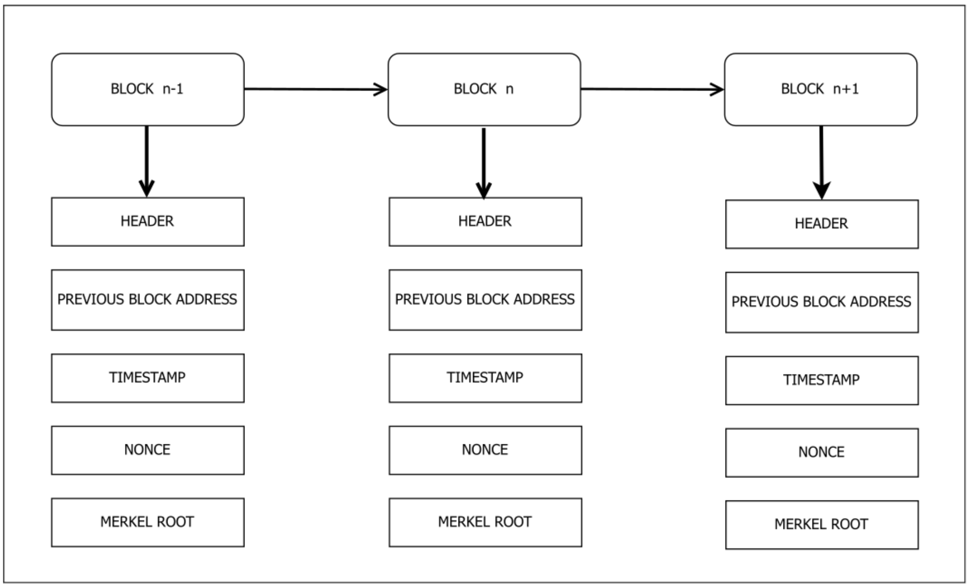

Figure 1: Blockchain architecture

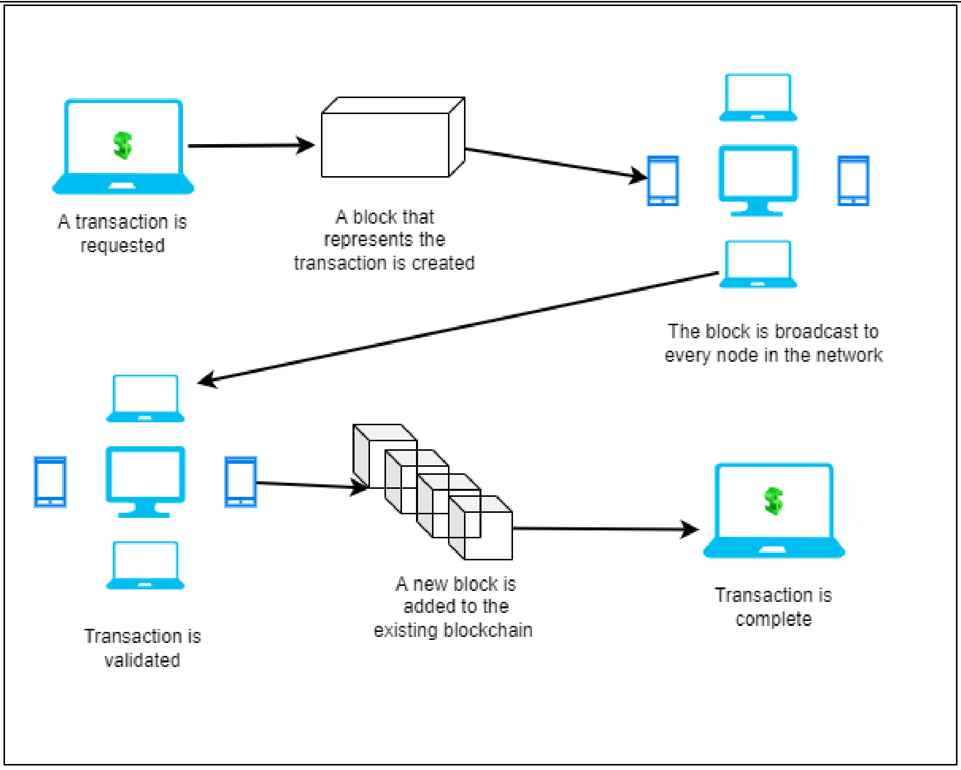
A transaction is requested
A block that represents the transaction is created
The block is broadcast to every node in the network
Transaction is validated
A new block is added to the existing blockchain
Transaction is complete

Figure 2: How blockchain works

2. Evolution of blockchain

The evolution of blockchain technology can be traced back to several key academic papers and concepts. In 1976, a seminal paper titled “New Directions in Cryptography” introduced the concept of a distributed ledger. This was followed by advancements in the field of cryptography, including a paper by Stuart Haber and Scott Stornetta titled “How to Time-Stamp a Digital Document,” which proposed the idea of timestamping data rather than the medium [13].

David Chaum’s model of “Electronic Cash” or “Digital Currency” significantly contributed to the development of blockchain. This was accompanied by protocols such as e-cash schemes that introduced double-spending detection. In 1997, Adam Back introduced “hashcash,” a concept designed to control spam emails. This led to the creation of “b-money” by Wei Dai, a form of money based on a peer-to-peer network [13].

Satoshi Nakamoto is widely recognized as the inventor of blockchain technology following the publication of a paper in 2008 titled “Bitcoin: A Peer-to-Peer Electronic Cash System.” The paper outlined an electronic payment system rooted in cryptography and provided a solution to the double-spending problem, ensuring that a digital currency cannot be duplicated or spent more than once. Nakamoto’s paper introduced the concept of a public ledger, where an electronic coin’s transaction history can be traced and confirmed to prevent double spending [14].

The first open-source program to implement the Bitcoin system was released shortly after the paper’s publication, and the first Bitcoin network began in early 2009 when Nakamoto created the first bitcoins. Despite the anonymity of Bitcoin’s inventor, the cryptocurrency continued to be developed and marketed, supported by a large community addressing various issues with the code. There are hundreds of different cryptocurrencies, but Bitcoin holds the lion’s share of the market and has become the most popular cryptocurrency [13].

3. Types of Blockchain

A. Public or Permissionless blockchain

In the realm of permissionless or public blockchains, there are no prerequisites for system participants to join the network [15]. This form of blockchain epitomizes decentralization, as it permits participants to partake in the consensus process, initiate and read transactions, and uphold the shared ledger [16]. All participants have the ability to publish, access, and validate new blocks, thereby maintaining a comprehensive copy of the entire blockchain [17].

The formation and operation of public blockchains are characterized by their security. While any participant has the liberty to join the network and append transactions as blocks, these blocks undergo verification through resource-intensive consensus processes such as cryptographic puzzle-solving or staking one's cryptocurrency. The integrity of block contents is preserved by cryptographic hashes and a decentralized consensus mechanism. Moreover, a substantial number of nodes can opt for anonymity within the blockchain to safeguard their privacy [15].

Despite the myriad advantages, public blockchains are not devoid of open research challenges. The quest for efficiency is complicated by the extensive participant base and the resource-intensive nature of the consensus mechanisms. These challenges highlight the imperative for continuous research and development in this domain to enhance the performance and applicability of public blockchains [18].

B. Private or Permissioned Blockchain

Permissioned or private blockchains are custom-designed for specific organizations. Access to the network is granted to participants through invitation, and they are assigned distinct roles to maintain the blockchain in a decentralized fashion. The distinguishing feature of private blockchains, as compared to public blockchains, is that only authorized entities are allowed to join the network and manage the blocks [17].

Private blockchains are typically perceived as more secure and efficient than public blockchains, given that the network consists exclusively of recognized participants. The safeguard against tampering is ensured through the application of cryptographic hashes and the consensus of participants, reflecting the protective measures employed in public blockchains. However, in contrast to public blockchains, nodes in private blockchains are not afforded anonymity [16]. While private blockchains offer numerous advantages, they also pose several open research challenges. These predominantly pertain to the potential for block tampering and the threat of the network being breached by internally authorized participants. These issues highlight the necessity for stringent security protocols and continuous research to guarantee the integrity and security of private blockchains [17].

C. Consortium Blockchain

Consortium blockchains, although categorized as private blockchains, are specifically engineered to serve multiple organizations. Access to the network is restricted to invited and trusted participants who bear the responsibility of maintaining the blockchain in a decentralized manner. The consensus process in consortium blockchains is relatively slower compared to that in private blockchains, but it is faster than that in public blockchains [17].

From a security perspective, consortium blockchains provide a more substantial defense against information modification compared to private blockchains. This is due to the implementation of advanced security measures, which is a result of the participation of entities from multiple organizations. As a consequence, the likelihood of hacking is considerably reduced in this type of blockchain [18].

Notwithstanding their benefits, consortium blockchains also pose several unresolved research challenges. These primarily relate to the potential for block tampering and the risk of the network being compromised by authorized internal participants. These challenges underscore the importance of rigorous security measures and ongoing research to ensure the preservation of integrity and security in consortium blockchains [18].

4. Security Analysis

Blockchain technology can be conceptualized as a multi-layered architecture, comprising of (i) a network layer, (ii) a consensus layer, and (iii) an application layer. The network layer signifies the type of network in which the blockchain is deployed. The consensus layer denotes the consensus protocol utilized, and the application layer reflects the technological and architectural choices incorporated into the platform. Each layer is characterized by its unique security flaws and inherits security features from the underlying layers. Typically, the application and consensus layers are built upon the network layer [19].

III. LITERATURE REVIEW

In recent years, the banking sector has observed a marked escalation in cybercrimes. These cybercrimes encompass a range of activities including, but not limited to, data theft, phishing attacks, ransomware attacks, and identity theft. Such criminal activities result in considerable financial losses for both the customers and the banks involved. Furthermore, these crimes have a significant adverse effect on a nation's economy. Financial institutions play a pivotal role in the economy by ensuring liquidity, guaranteeing the money supply, providing loans, savings, and deposits, and facilitating payments and settlements. The potential repercussions of Cyberattacks on these institutions can be significantly damaging [20]. In 2023, data breaches cost an average of USD 4.45 million, marking a record high. This represents a 2.3% increase from the 2022 cost of USD 4.35 million. Over a longer period, the average cost escalated by 15.3% from USD 3.86 million in 2020. Research indicates that the financial sector ranks second in industries with the most expensive data security incidents, with costs reaching USD 5.90 million in 2023. These figures underscore the critical need for robust cybersecurity measures in the financial sector [21].

Internet scams pose a significant threat to both individuals and nations, inflicting harm either directly or indirectly [22]. Financial institutions face a relentless onslaught of cyberattacks on a daily basis, which can lead to the loss of data, funds, and trust [23]. As the prevalence of digital banking increases, these institutions become increasingly susceptible to such threats. With the advancement of technology, the public's demand for immediate online access to all services, coupled with the growing use of cloud storage for large volumes of data, further exacerbates the vulnerability of the banking sector. According to [23], Banks are progressively resorting to outsourcing for the procurement and management of IT assets as a cost-control measure. The onus of ensuring the security of services rendered under outsourced contracts, inclusive of cloud hosting, lies with the bank. However, a significant number of banks lack awareness about the operational procedures of their IT partners, and only a small fraction have instituted mechanisms and protocols for oversight and monitoring. Banks often lack the resources required to monitor external vulnerabilities and networks or to regulate every vendor they collaborate with. It is imperative to consider robust measures to ensure adherence to legal compliances to avert penalties that could be levied due to data breaches. [24] provides a security risk model that offers a security risk framework that employs real-time biometric measures to protect a client's online banking account from unauthorized access. This model assists in identifying any transactions that may have been carried out without the client's awareness. Biometric verification methods, such as facial and fingerprint recognition, are implemented to ensure data security. Despite the model's capacity to facilitate the creation of effective cybersecurity defense strategies at the canonical, logical, and physical representation levels within the financial system, it still necessitates safeguards against a variety of potential cyber threats to enhance its user-friendliness.

The escalating interconnectedness of financial institutions and third-party entities renders these institutions susceptible to both internal and external Information and Communication Technology (ICT) and security threats, which could potentially threaten their existence. To meet their operational, corporate, strategic, and reputational objectives, financial institutions must have robust ICT and security risk management systems in place [25].

The degree of interconnection among financial institutions, financial markets, and market infrastructures, particularly the interdependencies among their information technology systems, creates potential vulnerabilities. For instance, a localized cyber catastrophe could quickly proliferate across markets and countries. This is exemplified by the widespread adoption of digital payment systems and other financial infrastructures for conducting online retail banking, custodial services, and trading [26].

Given the financial industry's substantial dependence on IT systems and other electronic communication tools, as well as the presence of legacy IT systems, the potential adverse effects of a cyberattack are significantly amplified. Moreover, the adoption of cutting-edge technologies such as cloud computing introduces new relationships with businesses that may operate outside the boundaries of regulated financial institutions, thereby adding another layer of complexity to the security landscape [27].

Specifically, concerning the application of blockchain technology to address cybersecurity issues, my understanding is that there is a notable scarcity of Systematic Literature Reviews (SLRs). A recent survey paper in the field of blockchain and cybersecurity was conducted by Salman [28]. In this research, the authors underscore the challenges and issues related to the utilization of security services in the centralized architecture across various application domains. They offer an exhaustive review of the current blockchain-enabled methods for such security service applications in the areas of authentication, confidentiality, privacy, access control, data and resource provenance, and integrity assurance in distributed networks. I believe this study provides a valuable foundation for researchers interested in blockchain-based network and service security. In addition to this, a handful of studies concerning blockchain and its wider impact have been published. I will discuss these studies below to analyze the differences between the topics chosen by the authors and my research.

In late 2016, Conoscenti [29] undertook a systematic literature review (SLR) to examine the application and flexibility of blockchain technology, particularly in the context of the Internet of Things (IoT) and other peer-to-peer devices. Notably, they underscored the potential of blockchain for detecting data misuse without necessitating a centralized reporting system. Nevertheless, their study did not extend to an examination of the wider implications of blockchain technology on cyber security as a whole.

A recent research investigation discovered that malleability attacks, 51% attacks, and wallet security attacks are the predominant forms of assaults on blockchain initiatives [30]. An attacker who acquires control over 51% of the network has the ability to manipulate transactions and endorse a skewed consensus within the network, potentially leading to a double-spending issue. This refers to the act of spending the same bitcoin multiple times. Such a problem is less likely to arise in traditional transaction processes, as these involve the participation of intermediaries who verify the transaction between the sender and receiver, thereby reducing the likelihood of the double-spending issue [31]. Kiviat posits that the elimination of intermediaries in transactions could engender a double-spending issue, as there would be no entity to maintain the centralized ledger. This lack of oversight could potentially enable an electronic unit, such as a dollar, to be expended multiple times. This assertion underscores the critical role of intermediaries in preventing the double-spending problem in traditional transaction systems [32]. In order to mitigate such attacks, a method known as proof-of-stake has been instituted. Proof-of-stake is an algorithm or technique employed to authenticate transactions within the blockchain network, ensuring that a miner's ability to mine blocks is contingent upon the number of blocks they possess. However, the efficacy of the proof-of-stake technique in averting such attacks has been met with considerable criticism [31]. Huoy [33] posits that despite the integration of proof-of-stake as a security measure in the blockchain network, all cryptocurrencies exhibit inherent vulnerabilities. In his scholarly work, he demonstrated that a blockchain network fortified with proof-of-stake remains susceptible to attacks from dishonest nodes. Concurrently, he refuted assertions made by the computer science community that proof-of-stake can guarantee immunity from a 51% attack in a blockchain network. He suggests that another approach to mitigating a 51% attack on the network could be the implementation of a private blockchain [33].

In their comprehensive review, [34] delineate the applications of blockchain technology within the banking industry, underscoring both the anticipated challenges and potential benefits. As per the authors' assertions, blockchain technology harbors the capacity to revolutionize the banking sector. This transformation is envisaged through the enhancement of transaction security, transparency, speed, and cost-effectiveness. The authors posit that these improvements could fundamentally alter the operational dynamics of the banking industry. In their discourse, Tapscott and Tapscott [35] elucidate the reasons why blockchain technology is particularly apt for application in the banking and financial sector.

In his comparative analysis [36], discusses the implications of integrating blockchain technology into the business model of conventional banks for processing international payments. The study posits that the successful implementation of blockchain technology is less probable when pursued in isolation by traditional banks. Conversely, it suggests that a more feasible approach would be for these banks to collaborate with fintech organizations. This integration, the study argues, would enable banks to harness the value of blockchain technology on a more extensive scale, thereby potentially transforming the landscape of international payment processing.

IV. METHODOLOGY

The SLR was conducted to address the questions that emerged following the analysis of the introduction of Blockchain Technology in cybersecurity and compliance within the financial industry. The research was underpinned by a comprehensive search of academic databases such as Google Scholar, IEEE, ScienceDirect, SpringerLink, and ACM Digital Library.

The objective of the SLR was to identify the key areas of focus within the domain and subsequently formulate research questions pertinent to these areas. The SLR process was rigorous and methodical, ensuring that the derived research was both comprehensive and reliable.

The SLR began with the development of a review protocol, which outlined the research objectives and the criteria for inclusion and exclusion of literature. This was followed by the formulation of clear and concise research questions that guided the review process. A systematic search strategy was then employed, encompassing not only electronic literature databases but also manual searches and the identification of yet-to-be-published literature. This ensured a comprehensive overview of the research topic.

The quality of the identified studies was then appraised, and relevant data was extracted. This data was subsequently analyzed and synthesized to answer the research questions about the impact of Blockchain Technology on cybersecurity and compliance within the financial industry.

In conclusion, the SLR provided valuable insights into the domain, answering key research questions and identifying areas for future research. The rigorous and systematic approach of the SLR ensured the reliability and comprehensiveness of the research, making it a valuable resource for further studies in this field.

1. Research Questions

RQ1: What benefits does blockchain technology offer in terms of security and compliance within banking institutions?

RQ2: What potential issues and obstacles might arise from the implementation of blockchain technology in the areas of security and compliance in banking?

2. Data Collection

The data collection process for this research was conducted using a systematic and targeted approach. A comprehensive search of the database was performed using specific keywords to ensure the relevancy and comprehensiveness of the collected data. The keywords used were “Blockchain”, “Banking”, “Bank”, and “Security and compliance”.

These keywords were used in combination with the logical operators ‘AND’ and ‘OR’ to refine the search results. Specifically, the search string was constructed as follows: “Blockchain” AND “Banking” OR “Bank” AND “Security and compliance”. This search string was designed to retrieve articles that discuss the intersection of blockchain technology with banking security and compliance.

The search was not limited to the body of the articles but also included the article titles and keywords. This ensured a wide coverage of relevant literature, capturing articles where the main focus was on the chosen topic.

3. Data Processing

Given the nature of the data extraction process, it was acknowledged that the extracted data might contain impurities, and not all data obtained using the specified keywords would be relevant to the research objectives.

To address this, a manual sorting process was implemented post-extraction. This involved a thorough review of the extracted data to identify and remove any irrelevant or impure data. The sorting process was guided by the research objectives and the predefined inclusion and exclusion criteria, ensuring that only data pertinent to the research questions was retained for further analysis.

V. RESULTS

This section presents a comprehensive analysis of the advantages and disadvantages associated with the application of blockchain technology in enhancing security and compliance within the banking sector.

1. RQ1: Benefits that blockchain technology offer in terms of security and compliance within banking institutions

A. Cost Saving

According to a Santander FinTech study, distributed ledger technology could reduce financial services infrastructure cost between US$15 billion and $20 billion per annum by 2022. This cost reduction is achieved by providing the possibility to decommission legacy systems and infrastructure, significantly reducing IT costs [37].

B. Enhanced data security

Blockchain technology's paramount benefit in banking is its potential to bolster data security. Conventional banking systems are susceptible to cyberattacks and data breaches, leading to substantial financial losses and reputational damage. Blockchain's decentralized data storage makes it exceedingly difficult for hackers to tamper with or corrupt the data.

Each transaction is encrypted and connected to the preceding one, making unauthorized data alteration nearly impossible. Furthermore, blockchain's consensus mechanism necessitates validation and approval of each transaction by all network participants, thereby augmenting the security of data stored on the blockchain [35] [38] [39].

C. Improved transparency and auditability

The distributed ledger technology of blockchain offers a transparent and auditable transaction record. This characteristic is especially beneficial for banking institutions as it facilitates real-time tracking and surveillance of financial transactions. It also empowers auditors to ascertain the precision and comprehensiveness of data, eliminating the need for manual processes. This capability can considerably diminish the time and resources necessitated for audits, thereby enhancing the efficiency of compliance procedures [38] [40] [41].

D. Increased efficiency

Blockchain technology can contribute to heightened efficiency by automating processes and diminishing the necessity for intermediaries.

The implementation of smart contracts, which are autonomous contracts with the agreement's terms directly inscribed into code, can further augment efficiency by automating compliance procedures. This automation can also mitigate the likelihood of human error, thereby enhancing the precision and dependability of compliance processes [35] [42] [43].

E. Enhanced cross-border transactions

Blockchain technology can also expedite cross-border transactions for banking institutions. Conventional cross-border transactions are typically slow and expensive due to the participation of numerous intermediaries, such as correspondent banks. Blockchain allows banks to establish direct connections, obviating the need for intermediaries and decreasing the time and cost linked with cross-border transactions. This can also bolster the security of cross-border transactions as blockchain's transparency and auditability attributes can aid in the prevention of fraud and money laundering.

F. Enhanced information quality

Blockchain technology allows for the storage of any type of information and enables access according to predefined rules and regulations. The feature known as smart contracts autonomously validates and enforces contracts. By transitioning financial data into shared ledgers, the data subsequently reaps the benefits of Blockchain technology [44].

G. Peer-to-peer distributed network

Blockchain technology, a peer-to-peer distributed network, maintains a public record of transactions, ensuring a high level of availability and distribution. Interestingly, blockchain technology does not typically retain the identities of the parties involved or the transaction data. Instead, it focuses on preserving the proof of the transaction's existence. This unique approach to data preservation enhances the security and anonymity of transactions, making blockchain an innovative solution in the realm of digital transactions.

H. Immutability

Immutability refers to the unalterable nature of the data once it has been written onto the blockchain. This characteristic is fundamental to the trustworthiness of blockchain networks, as it ensures that once data is added to the blockchain, it cannot be changed or removed [11]. Immutability is achieved in blockchain through the use of cryptographic hash functions. Each block in the blockchain contains a unique hash value that depends on the data within the block and the hash of the previous block. This creates a chain of blocks, where altering the data within a block would change its hash value and break the chain, making any attempt at data tampering evident.

2. RQ2: Concerns of using blockchain technology in security and compliance in banks

A. Regulatory challenges

Regulatory compliance emerges as a paramount challenge in the application of blockchain technology in banking institutions. Given the novelty of blockchain technology, there exists a void in the clear-cut regulations and guidelines that govern its utilization in the financial sector. This regulatory ambiguity can engender uncertainty for banks, leaving them in a quandary on how to adhere to existing regulations while employing blockchain. Furthermore, the diversity in regulatory requirements across different nations compounds the challenge, making it arduous for banks to operate on a global scale using blockchain technology.

B. Scalability issues

Blockchain technology, despite its potential, is still in its nascent stages and has yet to demonstrate its scalability for extensive use. As the volume of transactions added to the blockchain increases, the performance of the network can deteriorate, posing a challenge in managing a high volume of transactions. This could be a significant drawback for banking institutions, which necessitate the processing of a substantial number of transactions within a limited timeframe. Moreover, as the size of the blockchain expands, it could become problematic, demanding considerable computational resources for network maintenance.

C. Dependence on technology

Banking institutions are profoundly reliant on technology for their routine operations. The incorporation of blockchain technology introduces an elevated level of technological dependency, where any technical anomalies or malfunctions can considerably influence the bank's operations. This scenario can pose a concern for banks, as they are required to guarantee the stability and reliability of their systems to uphold customer trust and confidence.

D. Lack of privacy

While blockchain technology offers improved data security, it concurrently presents privacy challenges. Given that all transactions are documented on the blockchain, any individual with network access can view the data. This transparency can pose a substantial concern for banking institutions, which are obligated to safeguard their customers' sensitive financial information. Although some blockchains provide privacy features, their adoption is not yet widespread, and the efficacy of these features remains under scrutiny.

E. Initial Costs

Blockchain technology presents substantial potential savings in transaction costs and time, offering considerable speculative funds. However, the significant initial capital expenditure required to implement blockchain technology could pose a barrier to its adoption. In addition to the cost-benefit analysis, the adoption of blockchain technology also involves a strategic shift in operations and business models. The transition to a decentralized system can disrupt existing processes and require significant changes in operational procedures.

F. Endpoint Vulnerabilities

Endpoint vulnerabilities, such as those found in unprotected devices (e.g., mobiles or PCs), can provide an entry point for hackers to gain access to the keys needed to infiltrate the blockchain. Once these unauthorized users gain access, they have the potential to inflict significant damage. This is particularly concerning when the compromised endpoints belong to entities with high-level access to the blockchain, such as investment banks. The potential for substantial harm underscores the critical importance of robust endpoint security in safeguarding the integrity of the blockchain.

G. Security and protection

While solutions are available, encompassing private or permissioned blockchains and robust encryption, there still exist advanced security concerns that need to be addressed before the public will entrust their personal data to a blockchain solution. These concerns underline the necessity for rigorous security measures and protocols in the implementation of blockchain technology to ensure the protection of sensitive personal information.

While Blockchain technology provides enhanced security compared to its predecessors, it is not devoid of risks. The integrity of the blockchain network can be compromised in several ways, as detailed below:

1) A 51% attack, where a single entity gains control over 51% of the network nodes, could lead to the manipulation of the ledger and enable double spending [30]. This scenario is plausible on networks with programmable nodes or miners, making public networks more susceptible to 51% attacks than private ones. This is most useful against a proof of work PoW-based system. It is crucial to comprehend the blockchain consensus mechanisms employed and the conditions under which an attacker could potentially subvert them. Constructing a system that necessitates the subversion of more than half of all participating organizations, for instance, may be deemed an acceptable risk. This understanding can contribute significantly to the development of robust and secure blockchain systems.
2) Double spending represents another challenge for blockchain technology. The blockchain network employs mechanisms such as Proof-of-Stake and Proof-of-Work to prevent double spending. However, networks vulnerable to a 51% attack can still experience double-spending [31].
3) The security of Blockchain is also threatened by its encryption algorithm. Quantum techniques or computation can break the cryptography. Nevertheless, Blockchain applications now utilize quantum-resistant cryptographic methods to counter this issue.

H. Distributed Denial-of-Service (DDoS)

A Distributed Denial-of-Service (DDoS) attack has the potential to inundate blockchains with superfluous data and traffic requests. This ensures that the blockchain's server is pushed to its limits, utilizing its processing power to the maximum extent. As a consequence, transactions related to cryptocurrencies may lose their connectivity to the blockchain. Furthermore, a DDoS attack may even provide the attackers with access to online cryptocurrency wallets and exchanges. This highlights the critical need for robust security measures to protect against such attacks and ensure the integrity and functionality of blockchain systems.

I. Third party blockchain vendors

The utilization of third-party blockchain vendors by the banking industry could potentially introduce security vulnerabilities. T

hese vendors may lack standardized security systems, thereby increasing the risk of data breaches. Such breaches could lead to the exposure of sensitive blockchain credentials, potentially falling into unauthorized hands. This highlights the critical need for rigorous security measures when engaging with third-party vendors in the blockchain space.

J. Lack of security vulnerability coverage

Enterprise blockchain software is often underrepresented in security vulnerability databases. Consequently, unless users proactively monitor vendor release notes, they may remain uninformed about security updates. This deficiency in coverage, particularly in databases such as the Common Vulnerabilities and Exposures (CVE) and the U.S. National Vulnerability Database (NVD), presents a significant challenge. If vulnerabilities are not officially acknowledged, they may be overlooked by many large organizations, thereby posing potential security risks. It is imperative to ensure the availability of adequate resources for monitoring security vulnerabilities and updates in your blockchain and smart contract software. Regular monitoring can help in early detection of potential threats and timely implementation of necessary updates, thereby enhancing the overall security of the system. This proactive approach towards security management is crucial in maintaining the integrity and reliability of blockchain and smart contract applications [45].

K. Operational Risks

Assuming the presence of a secure blockchain and well-structured smart contracts devoid of security flaws, it is still necessary to execute the blockchain and smart contract code on a platform that is both well-connected and reliable. If the choice is made to utilize cloud services or third-party hosting, it is imperative to ensure their security.

Transparency and honesty should be sought beyond the standard declarations of SOC 2 compliance. The CSA's Security, Trust, Assurance, and Risk registry serves as a valuable resource for this purpose, allowing for a direct comparison of providers' responses.

The key takeaway is the importance of inquiry. Vendors and service providers who prioritize security will respond to questions without evasion. This proactive approach can significantly contribute to the overall security of the system [45].

VI. FUTURE PERSPECTIVE

The advent of blockchain technology is set to bring about a paradigm shift in the banking sector, especially in the realms of security and compliance [46].

The decentralized and ledger-centric architecture of blockchain makes it a potent tool for bolstering security in banking transactions. By drastically curtailing human error, a leading contributor to data breaches, blockchain renders transactions impervious to tampering and less prone to interception. This technology has the potential to eradicate financial fraud and data duplication while preserving a transparent audit trail [46].

In the compliance domain, blockchain can revolutionize capital markets by mitigating operational risks associated with fraud and human error, thereby diminishing overall counterparty risks.

The digitalization and tokenization of financial products and assets simplify trading, foster global inclusivity, enhance connectivity, and facilitate fractional ownership, all of which contribute to capital cost reduction and liquidity enhancement [46].

Nevertheless, the integration of blockchain technology into the banking sector brings with it substantial regulatory challenges, as the technology could pose numerous hurdles to the existing legal and regulatory frameworks. Consequently, a synergistic approach involving regulatory and private sector support is indispensable for the successful incorporation of blockchain in the banking industry [47].

In summary, blockchain technology harbors immense potential for augmenting security and compliance in the banking sector. However, its successful deployment necessitates meticulous navigation of the regulatory terrain [48].

VII. CONCLUSION

In conclusion, I found that the application of blockchain technology in the realm of security and compliance in banking institutions presents a multifaceted picture. The advantages of employing blockchain are manifold. It can bolster data security by providing a tamper-proof, decentralized record of transactions. This feature enhances transparency and auditability, thereby fostering trust among stakeholders. Furthermore, blockchain can streamline operations, leading to efficiency gains and cost savings. It also has the potential to simplify and expedite cross-border transactions, which are often bogged down by bureaucratic red tape. However, the adoption of blockchain is not without its challenges. Regulatory hurdles pose a significant barrier, as the legal framework for blockchain technology is still evolving. Scalability issues are another concern, given the high volume of transactions handled by banks. The successful implementation of blockchain is heavily reliant on technology, which could be a limiting factor for institutions with limited technological infrastructure. Privacy concerns also arise due to the transparent nature of blockchain transactions. Given these considerations, it is imperative for banks to undertake a thorough evaluation of the risks and benefits associated with blockchain technology. Proper planning and implementation can help mitigate potential pitfalls and maximize the advantages. Blockchain, if leveraged effectively, can serve as a powerful tool for enhancing security and compliance measures in the banking industry. As the technology continues to evolve and mature, and as regulatory frameworks adapt to accommodate this new technology, it is crucial for banks to carefully weigh the pros and cons of integrating blockchain into their security and compliance strategies. This careful evaluation will enable them to harness the power of blockchain technology effectively and responsibly, thereby reaping its numerous benefits.

VIII. REFERENCES

[1] Crisanto, J. C., & Prenio, J. (2017). Regulatory approaches to enhance banks' cyber-security frameworks. Bank for International Settlements, Financial Stability Institute.

[2] IBM Security X-Force, “X-Force Threat Intelligence Index 2022,” IBM Security, 2022. [Online]. Available: “https://www.ibm.com/downloads/cas/ADLMYLAZ”. Accessed December 13 2023.

[3] Boston Consulting Group, “Global Wealth 2019 Reigniting Radical Growth,” Jun. 2019. [Online]. Available: “https://image-src.bcg.com/Images/BCG-Reigniting-Radical-Growth-June-2019_tcm9-222638.pdf”. Accessed December 13 2023.

[4] Conference of State Bank Supervisors, “CSBS National Survey of Community Banks 2021,” Community Banking in the 21st Century 2021. [Online]. Vailabl e: “https: //www.communitybanking.org /~/media/files/publication/cb21publication_2021.pdf”Accessed December 13 2023.

[5] Alghazo, J. M., Kazmi, Z., & Latif, G. (2017, November). Cyber security analysis of internet banking in emerging countries: User and bank perspectives. In 2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS) (pp. 1-6). IEEE.

[6] Statista, “Blockchain use in banking and financial services market size worldwide in 2018 and 2019 with a forecast to 2026” May 2022. [Online]. Available: “https://www.statista.com/statistics/1229290/blockchain-in-banking-and-financial-services-market-size/”. Accessed December 17 2023.

[7] Abou Jaoude, J., & Saade, R. G. (2019). Blockchain applications–usage in different domains. Ieee Access, 7, 45360-45381.

[8] Dashkevich, N., Counsell, S., & Destefanis, G. (2020). Blockchain application for central banks: A systematic mapping study. IEEE Access, 8, 139918-139952.

[9] Treiblmaier, H., Rejeb, A., & Ahmed, W. A. (2022). Blockchain technologies in the digital supply chain. The Digital Supply Chain, 127-144.

[10] Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019, February). Research on the Application of Cryptography on the Blockchain. In Journal of Physics: Conference Series (Vol. 1168, p. 032077). IOP Publishing.

[11] Ali, O., Ally, M., & Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. International Journal of Information Management, 54, 102199.

[12] Thuraisingham, B. (2020, October). Blockchain technologies and their applications in data science and cyber security. In 2020 3rd international conference on smart blockchain (SmartBlock) (pp. 1-4). IEEE.

[13] Sarmah, S. S. (2018). Understanding blockchain technology. Computer Science and Engineering, 8(2), 23-29.

[14] Schollmeier, R. (2001, August). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In Proceedings first international conference on peer-to-peer computing (pp. 101-102). IEEE.

[15] Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. (2018). Decentralized applications: The blockchain-empowered software system. IEEE access, 6, 53019-53033.

[16] Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE communications surveys & tutorials, 21(3), 2794-2830.

[17] Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., ... & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. Ieee Access, 9, 61048-61073.

[18] Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2), 1676-1717.

[19] De Angelis, S., Zanfino, G., Aniello, L., Lombardi, F., & Sassone, V. (2019, October). Blockchain and cybersecurity: a taxonomic approach. In Workshop. EU Blockchain Observatory.

[20] Gulyás, O., & Kiss, G. (2023). Impact of Cyberattacks on the financial institutions. Procedia Computer Science, 219, 84-90.

[21] IBM, “Cost of a Data Breach Report 2023,” 2023. [Online]. Available: “https://www.ibm.com/downloads/cas/E3G5JMBP”. Accessed December 19 2023.

[22] Datta, P., Tanwar, S., Panda, S. N., & Rana, A. (2020, June). Security and issues of M-Banking: A technical report. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 1115-1118). IEEE.

[23] BCG: Banking's cybersecurity blind spot—And how to fix it. [Online]. Available: "https://www.bcg.com/publications/2018/banking-cybersecurity-blind-spot-how-to-fix-it" (2018). Accessed January 02 2024.

[24] Dhoot, A., Nazarov, A. N., & Koupaei, A. N. A. (2020, March). A security risk model for online banking system. In 2020 Systems of Signals Generating and Processing in the Field of on Board Communications (pp. 1-4). IEEE.

[25] E. Banking Authority, "EBA Guidelines on ICT and security risk management," European Banking Authority, November 2019. [Online]. Available: "https://www.eba.europa.eu/guidelines-ict-and-security-risk-management". Accessed December 26, 2023

[26] E. S. R. Board, "ESRB publishes report on systemic cyberattacks," European Systemic Risk Board, February 2020. [Online]. Available: "https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html". Accessed December 27, 2023.

[27] Momoh, I., Adelaja, G., & Ejiwumi, G. (2023). Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution.

[28] Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2018). Security services using blockchains: A state of the art survey. IEEE communications surveys & tutorials, 21(1), 858-880.

[29] Conoscenti, M., Vetro, A., & De Martin, J. C. (2016, November). Blockchain for the Internet of Things: A systematic literature review. In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) (pp. 1-6). IEEE.

[30] Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity challenges in blockchain technology: A scoping review. Human Behavior and Emerging Technologies, 2022, 1-11.

[31] Hui, H., An, X., Wang, H., Ju, W., Yang, H., Gao, H., & Lin, F. (2019). Survey on Blockchain for Internet of Things. J. Internet Serv. Inf. Secur., 9(2), 1-30.

[32] Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain transactions. Duke LJ, 65, 569.

[33] Houy, N. (2014). It will cost you nothing to 'kill' a proof-of-stake crypto-currency. Available at SSRN 2393940.

[34] Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., & Modgil, S. (2021). Measuring the perceived benefits of implementing blockchain technology in the banking sector. Technological forecasting and social change, 163, 120407.

[35] Tapscott, A., & Tapscott, D. (2017). How blockchain is changing finance. Harvard Business Review, 1(9), 2-5.

[36] Sven, M. D. (2018). How blockchain affects business models in international banking. In 11th IBA Bachelor Thesis Conference, July 10th, Enschede, The Netherlands.

[37] PWC, 'Blockchain: A new tool to cut costs" February 2017, [Online]. Available: "https://www.pwc.com/m1/en/media-centre/2017/articles/max-di-gregorio-me-insurance-review-feb2017.pdf". Accessed December 29, 2023.

[38] Sun, J., Yan, J., & Zhang, K. Z. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation, 2(1), 1-9.

[39] Herbert, J., & Litchfield, A. (2015, January). A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology. In Proceedings of the 38th Australasian computer science conference (ACSC 2015) (Vol. 27, p. 30).

[40] Mettler, M. (2016, September). Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom) (pp. 1-3). IEEE.

[41] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

[42] Davidson, S., De Filippi, P., & Potts, J. (2016). Economics of blockchain. Available at SSRN 2744751.

[43] Wan, C., Tang, S., Zhang, Y., Pan, C., Liu, Z., Long, Y., ... & Yu, Y. (2019). Goshawk: a novel efficient, robust and flexible blockchain protocol. In Information Security and Cryptology: 14th International Conference, Inscrypt 2018, Fuzhou, China, December 14-17, 2018, Revised Selected Papers 14 (pp. 49-69). Springer International Publishing.

[44] Chowdhury, M. U., Suchana, K., Alam, S. M. E., & Khan, M. M. (2021). Blockchain application in banking system. Journal of Software Engineering and Applications, 14(7), 298-311.

[45] Techtarget, "8 blockchain security risks to weigh before adoption" November 2023, [Online]. Available: "https://www.techtarget.com/searchcio/tip/8-blockchain-security-risks-to-weigh-before-adoption" Accessed January 03, 2024

[46] EC-Council, "Securing the Future of Banking – Exploring the Synergy of Blockchain and Cybersecurity" September 2023, [Online]. Available: "https://www.eccouncil.org/cybersecurity-exchange/network-security/securing-the-future-of-banking-with-blockchain-based-cybersecuritya/". Accessed January 03, 2024

[47] Portilla, D. L., Kappos, D. J., Ngo, M. V., Rosenthal-Larrea, S., Buretta, J. D., & Fargo, C. K. (2022). Blockchain in the banking sector: A review of the landscape and opportunities. In Harvard Law School Forum on Corporate Governance.

[48] Martino, P. (2021). Blockchain and banking: How technological innovations are shaping the banking industry. Springer Nature.