IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 May 2024, accepted 31 May 2024, date of publication 6 June 2024, date of current version 13 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3410874

RESEARCH ARTICLE

Blockchain-Based KYC Model for Credit Allocation in Banking

BULUT KARADAG[1], A. HALIM ZAIM[2], AND AKHAN AKBULUT[3], (Member, IEEE)
[1]Computer Engineering Department, Istanbul Commerce University, 34854 İstanbul, Turkey
[2]Computer Engineering Department, Istanbul Technical University, 34485 İstanbul, Turkey
[3]Computer Engineering Department, Istanbul Kültür University, 34156 İstanbul, Turkey

Corresponding author: Bulut Karadag (bulut.karadag@istanbulticaret.edu.tr)

ABSTRACT The implementation of the Know Your Customer (KYC) strategy by banks within the financial sector enhances the operational efficiency of such establishments. The data gathered from the client during the KYC procedure may be applied to deter possible fraudulent activities, money laundering, and other criminal undertakings. The majority of financial institutions implement their own KYC procedures. Furthermore, a centralized system permits collaboration and operation execution by multiple financial institutions. Aside from these two scenarios, KYC processes can also be executed via a blockchain-based system. The blockchain's decentralized network would be highly transparent, facilitating the validation and verification of customer data in real-time for all relevant stakeholders. In addition, the immutability and cryptography of the blockchain ensure that client information is secure and immutable, thereby eradicating the risk of data breaches. Blockchain-based KYC can further improve the client experience by eliminating the requirement for redundant paperwork and document submissions. After banks grant consumers loans, a blockchain-based KYC system is proposed in this study to collect limit, risk, and collateral information from them. The approach built upon Ethereum grants financial institutions the ability to read and write financial data on the blockchain network. This KYC method establishes a transparent, dynamic, and expeditious framework among financial institutions. In addition, solutions are discussed for the Sybil attack, one of the most severe problems in such networks.

INDEX TERMS Know your customer, blockchain, Ethereum, smart contract, distributed ledger.

I. INTRODUCTION

Blockchain is a type of distributed record keeping in a decentralized network by many nodes. Each of these nodes maintains a copy of the entire blockchain of records [1]. Due to its distinctive features such as decentralization, transparency, robustness, auditability and security, blockchain appears to affect many traditional ways of doing business [2]. Although blockchain is an old topic, its awareness has increased with Bitcoin. Bitcoin's technical document is the article titled ''Bitcoin: A Peer-to-Peer Electronic Cash System'' written in 2008 by a person or group named Satoshi Nakamoto [3]. The article proposes the transfer of digital assets using blockchain technology without using a financial intermediary. The article explains in detail how the double spending problem, one of the most serious problems of electronic money transfers, is solved when making these transfers. The infrastructure of this transfer system is built on blockchain technology, which provides a distributed ledger structure. Each network participant is considered a node in the blockchain, and transactions made by nodes are linked together in blocks. Since Satoshi Nakamoto first published his Bitcoin whitepaper in 2008, three generations of blockchains have been adopted. Blockchain 1.0 is used for cryptocurrency transactions, Blockchain 2.0 for financial applications, and Blockchain 3.0 for applications in areas other than finance, such as government, healthcare, and science [4]. In the financial sector, blockchain is used in a variety of ways. The most essential of them are cryptocurrency exchanges, KYC, payment systems, sukuk, non-fungible

The associate editor coordinating the review of this manuscript and approving it for publication was Abdel-Hamid Soliman.

tokens (NFTs), and crowdfunding [5]. KYC is typically a process carried out individually by banks. It is also possible for banks to share information and conduct the transaction centrally. Apart from this, a KYC procedure can be carried out using blockchain. The use of blockchain technology in the KYC process benefits consumer risk management by making it faster, more transparent, and decentralized. Following the use of a loan, a bank customer is obliged to make periodical loan payments to the bank. In the process, banks should measure their risks by sharing information with other banks on limits, risks and collateral. Banks can more quickly determine the risks related to their customers if they have this information. Conventional credit assessment relies on centralized credit bureaus. These entities gather customer financial information from banks and subsequently monetize it by selling it back to financial institutions. However, this approach raises concerns regarding data ownership and security, as credit bureaus possess the ability to manipulate the information. Furthermore, the data retrieval process is often delayed, as it typically occurs on an end-of-day basis. In contrast, a blockchain-based model fosters a decentralized environment where all participating banks hold identical copies of customer financial data. This shared ledger enables immediate data access for authorized institutions, eliminating the need for a centralized intermediary and associated fees. Decentralized blockchain technology has the potential to significantly enhance the overall efficiency of KYC processes. This can be achieved through several mechanisms: improved processing speed, minimized onboarding time for customers, reduced risk of fraud and money laundering, and a decrease in total costs incurred by financial institutions. In this study, the method of sharing the limit, risk and collateral information of bank customers using credit between banks using blockchain is explained. Using the Ethereum [6] network, a blockchain-based system was established with the help of a smart contract in the Solidity language. After a bank provides a loan to its customer, it enters the customer's limit, risk and collateral information into the system. At the same time, if that customer has used a loan from another bank, the bank also accesses the limit, risk and collateral information entered by that bank. Since this study is designed on a private blockchain network, it does not pose a problem with the Sybil attack.

The authors confirm contribution to the paper as follows: study conception and design: B. Karadag, A.H.Zaim, A. Akbulut; model creation: B. Karadag, A. Akbulut; analysis and interpretation of results: B. Karadag, A.H.Zaim, A. Akbulut; draft manuscript preparation: B. Karadag, A. Akbulut. All authors reviewed the results and approved the final version of the manuscript.

II. RELATED WORK

This section includes studies in general finance that are based on blockchain technology. The review by Mansoor et al. [7] focuses into how information storage and monitoring through blockchain technology can change the way that banking is done today, especially with regard to the KYC document verification procedure. The study proposed by George et al. [8] recommends the use of a decentralized platform that eliminates the need for a central authority or intermediary and enables many organizations to securely and transparently communicate and assess KYC information. In order to accomplish this, the paper also outlines the development and deployment of a prototype application that makes use of smart contracts and encryption methods. According to the study, the suggested method can raise regulatory compliance, lower operating expenses, and improve customer experience. The study by Roman [9] mentions problems with the data when calculating the credit score. One of the main problems is limited data sharing due to lack of trust between individuals and third parties. This results in insufficient data and inaccurately calculated results in credit scoring. To solve this problem, they introduced the ''Trusted Data Marketplace'' in their work. This system, which can be integrated with blockchain, contributes to credit scoring. In his study, Karayılan [10] examined the blockchain infrastructure and studied the use of blockchain infrastructure for KYC solutions and the use of blockchain in financial applications. Within the scope of the project, two models were created and compared to create the information sharing network. In the first model, smart contracts are developed and data sharing and storage is provided on the blockchain. In the second model, the data is kept in an external database and keyed in the blockchain. Another study in the financial field is on blockchain, real-time accounting and credit risk modelling. In his work, Byström [11] studied how blockchain will affect the way credit risk modeling is done and how trust and time can be improved with real-time accounting on blockchain. In the study, the feature that records in the blockchain can never be changed is emphasized. Blockchain, a reliable and constantly updated structure, has been applied to store the accounting records of a company using blockchain. Financial data is prepared at regular intervals and added to the company's ledger. An auditor expresses an opinion on the accuracy of the statements. When using this information, investors and credit risk managers must trust that the auditor provides accurate information and accurately records the firm's financial data in the ledger. In this process, the concept of trust is extremely important, from the preparation of financial statements to the approval of the auditor. To ensure this trust, Byström has worked to make blockchain a solution. In his study, the company voluntarily writes its financial data to the blockchain, which will immutably and timestamp the data. In this way, the entire financial data ledger created is visible and will prove the consistency of this data. A blockchain-based credit analysis infrastructure for credit risk management is proposed by Chakraborty [12] By using blockchain technology, the efficiency of financial systems is aimed by ensuring that lenders and debtors make transactions in a safe and transparent manner. The study used machine learning algorithms to determine credit scores

of lenders and borrowers. It has been observed that the proposed infrastructure provides more accurate and faster results than traditional methods. A blockchain-based loan recommendation system for financial institutions, called KiRTi, is presented by Patel [13]. The aim of the study is to facilitate smart credit transactions between potential borrowers and potential creditors without the need for third-party credit rating agencies for credit score generation. KiRTi system stores time series sequential data of potential borrowers in the open blockchain and produces credit scores with the LSTM model. To update the credit score, edge weights are adjusted according to boolean indicators. Smart contracts provide automatic repayment between potential debtors and potential creditors. The system achieved 97.5% accuracy and an F-measure of 0.98304 on the German credit dataset. The system also proved that the computation cost is 20.96 ms and the communication cost is 121 bytes. In this study, BACS [14], a credit scoring classification method based on blockchain and automatic machine learning, was examined. Credit scoring plays an important role in the modern economy, but the process of creating a credit scoring model is laborious and time-consuming. Therefore, blockchain and automated machine learning technologies have been used to automate this process. Blockchain effectively integrates data mining steps such as automatic machine learning, data sampling, feature extraction, feature selection and hyperparameter optimization, while ensuring that credit data is stored in a secure, traceable and immutable manner. The BACS method was tested on a dataset called German Credit Data and achieved an accuracy rate of 75.7%. Additionally, the BACS method showed higher performance than other classification models. These results show that the BACS method is an efficient and accurate method for credit scoring classification. Wang et al. [15] present a systematic and comprehensive overview of self-executing contracts, also known as ''smart contracts,'' deployed on blockchain platforms like Ethereum and Hyperledger, are attracting increasing attention across diverse sectors, particularly within the financial domain. This appeal stems from their inherent ability to automate and enforce contractual stipulations without the need for centralized authorities. However, the widespread adoption of smart contracts is contingent upon addressing significant challenges, including those pertaining to security vulnerabilities and data privacy considerations. In this study, Rohitchandran et al. [16] proposes a system that offers a secure platform for storing and managing bank records. Smart contracts, self-executing code embedded within the blockchain, can govern data storage and access permissions. Additionally, robust cryptographic algorithms employed by blockchain ensure the confidentiality of sensitive financial information. Ali et al. [17] investigates the potential of green cryptocurrencies as a novel asset class for portfolio diversification, particularly within the context of environmental sustainability and adherence to UN SDGs. A four-step selection process is introduced to identify cryptocurrencies with lower environmental footprints. The analysis finds that green cryptocurrencies (ADA, EOS, IOTA, XLM, XTZ) offer comparable or even superior diversification benefits to traditional equity portfolios compared to non-green counterparts (BNB, BTC, ETH, LTC, XRP).

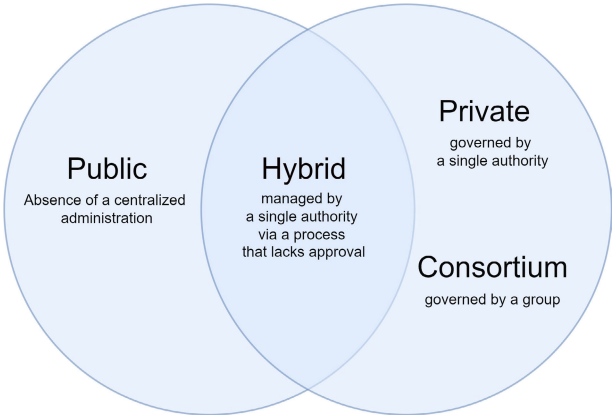

FIGURE 1. Types of blockchain.

III. BACKGROUND

A. BLOCKCHAIN TYPES

The first step in building a blockchain application is choosing the right infrastructure. There are four main types of blockchain networks available [18]. It is expected to use Private Blockchain Network or Consortium Blockchain Network between banks. Figure 1 shows blockchain types and their relationships with each other.

1) PUBLIC BLOCKCHAIN NETWORK

This type of network is called decentralized, meaning there's no central authority. All participants (stakeholders) have equal rights and can contribute to the network by creating and validating new data blocks. Bitcoin is the most well-known example of this kind of decentralized network.

2) PRIVATE BLOCKCHAIN NETWORK

This type of network is permissioned, meaning only one entity controls access and validates transactions. Other participants have limited rights defined by the central authority. This structure is often chosen for public authority applications where a single entity needs oversight.

3) HYBRID BLOCKCHAIN NETWORK

A hybrid network combines elements of public and private blockchains. While a single entity controls access, the verification process is similar to a public network, ensuring transparency. The ''Food Trust'' project by IBM, used in supply chains, is a good example of this type of network.

4) CONSORTIUM BLOCKCHAIN NETWORK

Within the domain of blockchain technology, consortium networks offer a distinct structure compared to private and public chains. Unlike private blockchains controlled by

a single entity, consortium blockchains are governed by a pre-selected group of organizations. This collaborative approach fosters enhanced security through a distributed validation process, while maintaining controlled access to the network. A pertinent example lies in the blockchain network established solely by notaries, where governance and participation are restricted to authorized notary members.

B. SMART CONTRACT

The concept of smart contracts, originally introduced by Nick Szabo in 1994, refers to self-verifying and self-executing computer programs deployed on a blockchain network. These programs, essentially sets of pre-defined rules, operate in a decentralized manner, resistant to tampering due to the blockchain's inherent immutability. Through replication across the network and peer-to-peer oversight, smart contracts ensure the secure and transparent execution of agreements [19].

With the huge amount of investment in decentralized ledger technologies, especially blockchain, and its rapid evolution as a trend towards being accepted as a new solution to record, share, and synchronize transactions in their respective electronic ledgers, Ethereum smart contracts are becoming the preferred mechanism to implement a wide range of applications in the banking sector, including financial instruments [20]. The use of Ethereum smart contracts in the banking sector has gained significant interest and attention. Banks are increasingly exploring the potential of incorporating Ethereum smart contracts into their operations. A smart contract is a self-executing contract with the terms of the agreement directly written into lines of code. These contracts automatically execute when predetermined conditions are met, without the need for intermediaries or third parties. In the context of the Ethereum Network, a smart contract can be created by writing code that includes the conditions and actions to be executed. This code is then deployed onto the Ethereum Network, where it becomes immutable and transparent. Once deployed, the smart contract on the Ethereum Network can be interacted with by multiple parties.

C. KYC TYPES

KYC practices encompass the customer identification and due diligence procedures employed by financial institutions. These procedures aim to establish a comprehensive understanding of the customer's identity, risk profile, and financial activities. By gathering and analyzing this information, institutions can effectively mitigate potential risks associated with money laundering, terrorist financing, and other financial crimes. Furthermore, a robust KYC process allows for tailored service configurations that best suit the customer's needs. Blockchain offers several advantages for establishing an integrated platform for secure KYC data storage [21]. These advantages are given with their explanations in Table 1.

The KYC model generally used by banks works individually. Beyond individual systems, blockchain technology

TABLE 1. Benefits of creating an integrated platform for safe storage of KYC data.

Scenario	Definition
Streamlined Customer Onboarding	Blockchain technology significantly reduces the need for re-verification of existing customers within the network, leading to faster onboarding times
Enhanced Cost Efficiency	Shared KYC services facilitated by blockchain can lead to a substantial decrease in client verification costs for participating institutions
Mitigated Fraud Risk	The immutable nature of blockchain transactions ensures the integrity of customer data, thereby reducing the risk of fraudulent information
Consent-based Information Sharing	With customer consent, only relevant KYC information is shared with new institutions, facilitating a more streamlined enrollment process
Immutable Audit Trail	All updates to customer data are permanently recorded on the blockchain, enabling easy identification of the source of any inaccuracies
Increased Operational Security	The anonymized nature of transactions on a blockchain network enhances the overall reliability and security of operations
Identity Empowerment	Blockchain technology can empower individuals, particularly refugees facing challenges in obtaining traditional documentation, by providing a secure and verifiable record of their identity

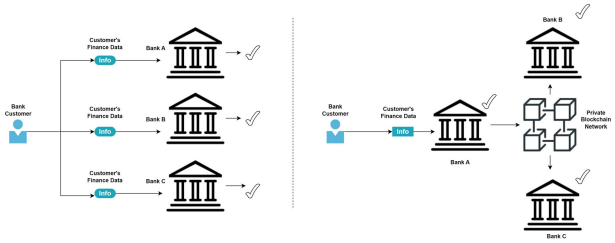

FIGURE 2. Traditional and blockchain based KYC Model.

presents an alternative approach for collaborative KYC. In a decentralized blockchain-based structure, customer information can be shared securely amongst all participating banks within the network. Figure 2 shows the KYC model in both traditional and blockchain based structure.

IV. BLOCKCHAIN BASED KYC MODEL

The application of blockchain technology presents a compelling opportunity for the secure and transparent storage and exchange of credit allocation data within the financial sector. This distributed ledger system fosters trust and transparency amongst all stakeholders involved in the credit allocation process, including banks, borrowers, and other relevant parties. Furthermore, blockchain technology can significantly enhance the efficiency of credit allocation procedures. By leveraging this technology for credit allocation data, banks can streamline the verification and validation of borrower information, resulting in a reduction in both the time and costs associated with traditional, manual processes.

A Customer's past and present financial information is used when he/she want to use a loan. The loan's limit, risk, and collateral details are crucial after the customer has used it. Banks retain this data about its own clients on a monthly basis. In order to assess limit, risk, and collateral information

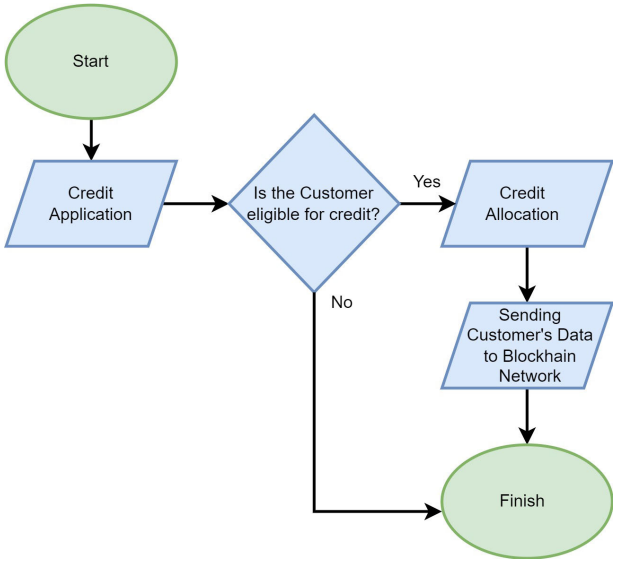

FIGURE 3. Process of customer credit with blockchain based KYC.

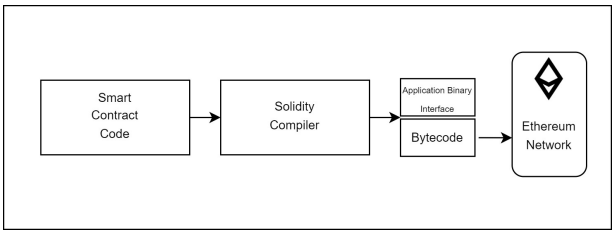

FIGURE 4. Deployment of Smart Contract to Blockchain Network.

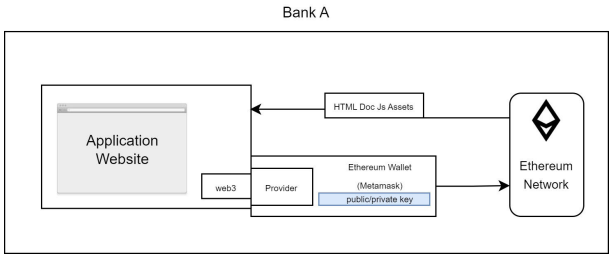

FIGURE 5. Reading/writing of customer's data in blockchain network.

are needed when the same consumer wishes to use a loan from a different bank. If a central system is available, it is used to obtain this data when another bank requests access. The KYC approach based on blockchain is also used for this kind of consumer data transactions. This is how an immediate, transparent, and immutable KYC approach built on blockchain technology is implemented.

As illustrated in Figure 3, the loan application process commences with the customer submitting a request to the bank. The bank then assesses the customer's creditworthiness by analyzing their past and present financial data. Upon loan approval, the customer's credit limit, associated risk profile, and any required collateral information are uploaded to the blockchain-based KYC system. Other financial institutions can subsequently access this data by querying the system using the customer's unique identification number.

In this study, a smart contract was initially developed for the blockchain-based KYC model. The smart contract was developed in Solidity and will run on the Ethereum network. With this smart contract, the customer's risk limit and collateral information are recorded in the network. When the records need to be accessed, the identification number is presented [22]. The smart contract written in Solidity language is first compiled, after which the Application Binary Interface (ABI) and Bytecode are generated. Bytecode is used on the Ethereum network. ABI is a JSON-based code sequence that is used to invoke the smart contract from the interface program. Figure 4 shows the processes for implementing the smart contract on the Ethereum network.

As depicted in the Figure 5, accessing a smart contract deployed on the Ethereum network necessitates interaction between a front-end application, an Ethereum wallet, and a provider. Providers like Infura facilitate this interaction. During front-end development, the smart contract address and its corresponding ABI code are crucial elements. Leveraging these components, the front-end application establishes a connection to the user's Ethereum wallet through the chosen provider. Notably, writing data (e.g., recording financial information) to the blockchain incurs a gas fee, whereas reading existing data is typically free. Within the Ethereum blockchain, for instance, the transaction fee is determined by the computational unit cost (gas price) and the maximum allocated computational units (gas limit) specified by the user, as in (1).

$$TransactionCost = GasPrice * GasLimit \tag{1}$$

Within blockchain and distributed systems, Sybil attacks pose a significant threat. These attacks exploit the system's reliance on identities by enabling a malicious actor to create a multitude of illegitimate identities (Sybil identities). This manipulation grants the attacker undue influence over the network, potentially jeopardizing core functionalities such as consensus mechanisms, resource allocation protocols, and security measures.

V. SYBIL ATTACK ON BLOCKCHAIN BASED KYC MODEL

Blockchain technology offers the financial sector a compelling solution for KYC validations. This approach enables selective data sharing while upholding tamper-proof data integrity. However, one vulnerability that arises in blockchain-based KYC modelling is the potential for a Sybil attack [23]. These attacks involve the malicious creation of numerous illegitimate virtual identities to manipulate a digital network. This poses a significant challenge in guaranteeing the authenticity and integrity of KYC data stored on the blockchain. To mitigate the threat of Sybil attacks, various blockchain projects have implemented decentralized and Sybil-resistant consensus mechanisms. These mechanisms rely on subjective inputs such as voting, vouching, and interpretation to establish a distributed source of legitimacy for identity verification.

This approach acknowledges the critical question of ''who verifies the verifier?'' by incorporating subjective inputs and decentralized consensus mechanisms. Consequently, blockchain-based KYC modeling strives to reduce the risk of Sybil attacks and ensure the trustworthiness of identity verification, even in the absence of conventional centralized institutions. In the domain of collaborative cybersecurity, blockchain technology can be instrumental in eliminating single points of failure and bolstering trust management.

Public blockchain networks are inherently susceptible to Sybil attacks due to their open nature. Conversely, private networks, functioning as closed ecosystems with restricted access, offer a significantly lower risk of such attacks. Consensus (data) refers to the collective agreement among nodes on the validity of data. This consensus is achieved through cryptographic consensus algorithms, such as Proof of Work (PoW) or Proof of Stake (PoS), as in (2). PoW and PoS are established consensus mechanisms recognized for their resilience against Sybil attacks within blockchain systems [24]. This research investigates the potential of PoS in a secure private Ethereum network environment. The findings demonstrate that by leveraging a private network and a robust PoS consensus mechanism, a secure architecture can be achieved, effectively mitigating Sybil attack risks.

$$Consensus(data) = f(blockchain\_nodes) \tag{2}$$

VI. RESULT

Within the scope of the study, both traditional and blockchain-based KYC models were examined. While Blockchain-based KYC is superior in terms of features such as technology and security, traditional method is stronger in terms of regulation. A comparison table based on the study results can be seen in Table 2. In addition to the Table 2, the transaction processing time for a single KYC request to be verified and recorded on the blockchain is faster than the traditional KYC process. Because in the traditional KYC process, each transaction is carried out separately by banks, while in the blockchain-based KYC process, it is sufficient to do it only once on the blockchain network. In addition, PoS consensus mechanism discourages Sybil attacks by requiring participants to stake a certain amount of cryptocurrency, making it expensive to create and maintain a large number of fake identities.

VII. DISCUSSION

KYC process is very important in banking. There are potential security vulnerabilities in KYC processes traditionally carried out in banking. Additionally, it is not efficient for each bank to carry out the KYC process separately. The Blockchain-based KYC model both speeds up the processes and offers a decentralized, secure environment. In addition, blockchain-based KYC processes allow banks to quickly make risk assessments. In this way, instant interbank data sharing occurs instead of end-of-day transactions. Thanks to blockchain technology, which has a decentralized structure, the risk of fraud is prevented as the data is immutable and transparent. However, despite their risk-preventing importance, blockchain-based systems are still controversial in terms of regulation and compliance. Some governments do not allow blockchain-based systems. Despite this, blockchain-based systems, including KYC, will continue to be on the agenda in the banking industry as they are reliable, efficient and encourage collaboration.

TABLE 2. Evaluation criteria of traditional and blockchain-based KYC.

Feature	Traditional KYC	Blockchain-based KYC
Centralization	Centralized	Decentralized
Transparency	Enables real-time data sharing	Enables real-time multi data sharing
Security	Data can be manipulated bank personnel	The immutability of blockchain allows for tamper-proof data
Risk Assessment	Risk is calculated only with the bank's own data	Extensive risk assessment is made with data from other banks
Efficiency	Repetitive verification processes among banks	Elimination of duplicate processes
Regulation	Governments allow centralized system	Bank regulation needs improvement

VIII. CONCLUSION

This study, based on the Blockchain-based KYC model, demonstrates the sharing of loan allocation data of bank customers who have been allocated loans. Interbank data sharing is possible with a smart contract written in solidity language on the Ethereum network. The deployment of the prepared smart contract to the Ethereum network and then how to write and read data over this network are mentioned. In addition, it provides a safe environment against Sybil attacks thanks to its construction on a private blockchain network and PoS consensus method. The blockchain-based KYC model was designed considering the private Ethereum network and PoS consensus mechanism. In this way, blockchain technology offers a transformative solution to the shortcomings of traditional KYC in banking. A shared, immutable ledger streamlines onboarding, bolsters data security, and enables real-time risk assessment. Regulatory hurdles persist, but the potential for enhanced efficiency, collaboration, and risk management within a secure and transparent framework is undeniable. As blockchain matures and regulations evolve, it has the potential to revolutionize KYC, ushering in a new era for secure and efficient customer identification in banking.

The exponential growth of global data necessitates secure storage and efficient sharing among stakeholders. Blockchain technology emerges as a frontrunner in this domain, facilitating secure and transparent data exchange. This attribute is likely to drive increased adoption within the financial sector in the coming years. However, regulatory and compliance hurdles persist. Overcoming these challenges will unlock a multitude of use cases for financial institutions. One such scenario involves leveraging non-fungible tokens (NFTs)

to store Letters of Guarantee (LoGs), a prevalent tool in banking. By tokenizing LoGs with NFTs, the technology inherently prevents duplication and counterfeiting, enabling banks to manage associated risks more effectively. The integration of NFTs within the financial ecosystem holds significant promise for fostering enhanced security, efficiency, and collaboration.

REFERENCES

[1] V. L. Lemieux, "Trusting records: Is blockchain technology the answer?" *Records Manage. J.*, vol. 26, no. 2, pp. 110–139, Jul. 2016.
[2] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," *J. Ind. Inf. Integr.*, vol. 13, pp. 32–39, Mar. 2019.
[3] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Apr. 18, 2023. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[4] S. Perera, S. Nanayakkara, M. N. N. Rodrigo, S. Senaratne, and R. Weinand, "Blockchain technology: Is it hype or real in the construction industry," *J. Ind. Inf. Integr.*, vol. 17, pp. 1–20, Jan. 2020.
[5] B. Karadag, A. Akbulut, and A. H. Zaim, "A review on blockchain applications in fintech ecosystem," in *Proc. Int. Conf. Adv. Creative Netw. Intell. Syst. (ICACNIS)*, Nov. 2022, pp. 1–5, doi: 10.1109/ICACNIS57039.2022.10054910.
[6] Ethereum. (2023). *Ethereum Whitepaper*. [Online]. Available: https://ethereum.org/en/whitepaper/
[7] N. Mansoor, K. F. Antora, P. Deb, T. A. Arman, A. A. Manaf, and M. Zareei, "A review of blockchain approaches for KYC," *IEEE Access*, vol. 11, pp. 121013–121042, 2023.
[8] D. George, A. Wani, and A. Bhatia, "A blockchain based solution to know your customer (KYC) dilemma," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Goa, India, Dec. 2019, pp. 1–6.
[9] D. Roman and G. Stefano, "Towards a reference architecture for trusted data marketplaces: The credit scoring perspective," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 95–101.
[10] H. Karaylan, *Blockchain and its applications for financial technology solutions*. İstanbul, Turkey: Yüksek Öğretim Dergisi, 2019.
[11] H. Byström, "Blockchains, real-time accounting, and the future of credit risk modeling," *Ledger*, vol. 4, pp. 40–47, Apr. 2019.
[12] S. Chakraborty, S. Aich, S. J. Seong, and H. C. Kim, "A blockchain based credit analysis framework for efficient financial systems," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, PyeongChang, South Korea, Feb. 2019, pp. 56–60.
[13] S. B. Patel, P. Bhattacharya, S. Tanwar, and N. Kumar, "KiRTi: A blockchain-based credit recommender system for financial institutions," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1044–1054, Apr. 2021.
[14] F. Yang, Y. Qiao, Y. Qi, J. Bo, and X. Wang, "BACS: Blockchain and AutoML-based technology for efficient credit scoring classification," *Ann. Oper. Res.*, pp. 1–21, Jan. 2022, doi: 10.1007/s10479-022-04531-8.
[15] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.
[16] R. Rohitchandran, B. Santhoshkumar, and M. Kumar, "Bank records storage system through blockchain," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, Apr. 2023, pp. 1178–1181, doi: 10.1109/ICICT57646.2023.10134282.
[17] F. Ali, M. U. Khurram, A. Sensoy, and X. V. Vo, "Green cryptocurrencies and portfolio diversification in the era of greener paths," *Renew. Sustain. Energy Rev.*, vol. 191, Mar. 2024, Art. no. 114137, doi: 10.1016/j.rser.2023.114137.
[18] K. E. Wegrzyn and E. Wang. (2021). *Foley*. Accessed: Mar. 9, 2024. [Online]. Available: https://bit.ly/3BbLQTF
[19] N. Szabo. (2019). *Formalizing and Securing Relationships on Public Networks*. Accessed: Mar. 11, 2024. [Online]. Available: https://ojphi.org/ojs/index.php/fm/article/view/548/469
[20] M. Laarabi and A. Maach, "Understanding risk assessment in the context of fractional ownership using Ethereum smart contract," *Adv. Sci., Technol. Eng. Syst. J.*, vol. 5, no. 5, pp. 1028–1035, 2020.
[21] V. D. Kolychev and D. V. Solovov, "Methods and mechanisms of a subsystem formation of financial monitoring of suspicious operations in commercial bank," *KnE Social Sci.*, vol. 3, no. 2, p. 279, Feb. 2018.
[22] B. Karadag. (2023). *Blockchain Based KYC Model. GitHub Repository*. [Online]. Available: https://github.com/BulutKaradag/Blockchain-based-KYC-Model
[23] M. Platt and P. McBurney, "Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance," *Algorithms*, vol. 16, no. 1, p. 34, Jan. 2023, doi: 10.3390/a16010034.
[24] S. Hu, L. Hou, G. Chen, J. Weng, and J. Li, "Reputation-based distributed knowledge sharing system in blockchain," in *Proc. 15th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services*, New York, NY, USA, Nov. 2018, pp. 476–481.

BULUT KARADAG received the B.S. degree in electronics and telecommunication from Marmara University, İstanbul, Turkey, in 2009, and the M.Sc. degree in computer engineering from Ahmet Yesevi University. He is currently pursuing the Ph.D. degree in computer engineering with Istanbul Commerce University. He was a Software Developer with Piworks, from 2010 to 2013, and Kuveyt Turk Participation Bank, from 2013 to 2016. He was the Research and Development Service Manager of the Vakf Participation Research and Development Center, from 2016 to 2022. He has been the Head of the Project Management, Digital Transformation and Innovation, Neova Participation Insurance, since 2022. His current research interests include digital fintech, blockchain, and machine learning.

A. HALIM ZAIM received the M.S. degree in computer engineering from Boi University, in 1996, and the Ph.D. degree in electrical and computer engineering from North Carolina State University (NCSU), in 2001. He was the Vice-Rector of Istanbul Commerce University. He is currently a Faculty Member with the Department of Computer Engineering, Faculty of Engineering, Istanbul Technical University. His research interests include the IoT, big data, network design, cyber security, network security, and communication-network protocols.

AKHAN AKBULUT (Member, IEEE) received the B.S. and M.S. degrees in computer engineering from Istanbul Kültür University (IKU), Turkey, in 2001 and 2008, respectively, and the Ph.D. degree in computer engineering from Istanbul University, Turkey, in 2013. From 2004 to 2013, he was a Research Assistant with the Department of Computer Engineering, IKU, where he was an Assistant Professor, from 2013 to 2017. From 2017 to 2019, he was a Postdoctoral Researcher with the Computer Science Department, North Carolina State University, NC, USA. In 2019, he rejoined the Department of Computer Engineering, IKU, and he was promoted to an Associate Professor. He is currently the Chairperson of the Department of Computer Engineering, IKU. His current research interests include the design and performance optimization of software-intensive systems, machine learning applications, internet architectures, and broadening participation in cloud computing research.