Volume 02, Issue 09, September 2025 *ISSN: 3049-0952*
www.jsetms.com

DECENTRALIZED KYC FRAMEWORK FOR EFFICIENT CREDIT ALLOCATION IN BANKING

[1] Nisar Fatima
Roll Number: 23L51D0503
College: Shadan Women's College of Engineering and Technology
Email: nisarfatima100000@gmail.com

[2] Samreen Sultana
Designation: Assistant Professor
College: Shadan Women's College of Engineeering and Technology
Email: samreencme@gmail.com

To Cite this Article
Nisar Fatima, Samreen Sultana, "Decentralized KYC Framework For Efficient Credit Allocation In Banking", Journal of Science Engineering Technology and Management Science, Vol. 02, Issue 09, September 2025,pp: 74-82, DOI: http://doi.org/10.64771/jsetms.2025.v02.i09.pp74-82
Submitted: 02-08-2025 *Accepted: 04-09-2025* *Published: 11-09-2025*

ABSTRACT
In the financial industry, banks' adoption of the Know Your Customer strategy improves these businesses' operational effectiveness. The information obtained from the customer throughout the KYC process may be used to prevent potential money laundering, fraud, and other illegal endeavors. Most financial organizations have their own KYC processes in place. A centralized system also makes it possible for several financial institutions to work together and carry out operations. In addition to these two situations, a blockchain-based system can also be used to carry out KYC procedures. The decentralized network of the blockchain will be extremely transparent, allowing all pertinent stakeholders to validate and verify customer data in real-time. Furthermore, the blockchain's privacy and immutability guarantee that customer data is safe and unchangeable, eliminating the possibility of data breaches. By doing away with needless paperwork and data submissions, based on a KYC can further enhance the customer experience. This paper suggests a powered by blockchain KYC method to gather limit, risk, and collateral information from customers after banks approve transactions. Financial institutions can read and write financial data on the blockchain network thanks to the Ethereum-based method. This KYC approach creates an open, flexible, and quick framework between financial institutions. Solutions for the Sybil attack, one of the most serious issues in these networks, are also covered.

1. INTRODUCTION

Distributed record keeping by numerous nodes in a decentralized network is known as blockchain. A copy of the complete blockchain of records is kept on file by each of these nodes. Blockchain seems to have an impact on many conventional business practices because of its unique qualities, which include decentralization, transparency, resilience, auditability, and security. Bitcoin has raised awareness of blockchain, despite the fact that it is an old topic. The paper "Bitcoin: A Peer-to- Peer Electronic Cash System," authored in 2008 by Satoshi Nakamoto or a group of people, is the technical document behind Bitcoin. The article suggests utilizing blockchain technology to transfer digital assets without the need for a financial middleman. The article provides a thorough explanation of how to resolve the double spending issue, which is one of the most significant issues with electronic money transfers. Blockchain technology, which offers a distributed ledger structure, is the foundation of this transfer system's infrastructure. In the blockchain, every network user is

referred to as a node, and node-to-node transactions are connected in blocks. Three generations of blockchains have been implemented since 2008, when Satoshi Nakamoto first released his whitepaper on Bitcoin. Cryptocurrency transactions use Blockchain 1.0, financial applications use Blockchain 2.0, and applications outside of finance, such government, healthcare, and science, use Blockchain 3.0.

There are numerous applications of blockchain in the finance sector. The most important ones include crowdfunding, sukuk, non-fungible tokens (NFTs), payment systems, bitcoin exchanges, and KYC. Usually, banks handle KYC on an individual basis. Banks may also exchange data and carry out the transaction in a central location. In addition, blockchain can be used to do a KYC process. Consumer risk management is improved by the speedier, more transparent, and decentralized KYC procedure made possible by blockchain technology. A bank customer is required to make regular loan payments to the bank after using a loan. Banks should share information about restrictions, risks, and collateral with other banks in order to quantify their risks during the process. If banks have this knowledge, they can assess their customers' risks more rapidly. Central credit bureaus are the foundation of traditional credit evaluation. These organizations obtain client financial data from banks and then sell it back to other financial institutions to make money. However, because credit bureaus have the power to alter the info, this strategy raises questions about confidentiality and protection. Additionally, because data retrieval usually takes place at the end of the day, it is frequently delayed. A blockchain-based model, on the other hand, promotes a decentralized setting in which every participating bank has an identical copy of the client's financial information. Qualified institutions can access data instantly thanks to this shared ledger, which does away with the necessity for a centralized middleman and the fees that come with it. The overall effectiveness of KYC procedures could be greatly increased by decentralized blockchain technology. This can be accomplished in a number of ways, including faster processing, shorter customer onboarding times, lower fraud and money laundering risks, and lower overall expenses for financial institutions. This paper explains how banks use blockchain technology to share bank clients' credit limit, risk, and collateral information. With the aid of a smart contract written in Solidity, a blockchain-based system was created using the Ethereum network. A bank enters the customer's limit, risk, and collateral information into the system after granting them a loan. The bank also has access to the limit, risk, and collateral information that the other bank entered if the customer has previously used a loan from that other bank. Since this study is designed on a private blockchain network, it does not pose a concern with the Sybil attack. The following contributions to the work are confirmed by the authors:

B. Karadag, A.H. Zaim, and A. Akbulut were responsible for the study's idea and design; B. Karadag, A.H. Zaim, and A. Akbulut created the model; B. Karadag, A.H. Zaim, and A. Akbulut analyzed and interpreted the findings; and B. Karadag, A. Akbulut prepared the draft article. After reviewing the findings, each author gave their approval to the manuscript's final draft.

OBJECTIVE

The financial industry has a compelling opportunity to store and exchange credit allocation data in a transparent and safe manner through the use of blockchain technology. All parties participating in the credit allocation process, including banks, borrowers, and other pertinent parties, benefit from the confidence and transparency this distributed ledger technology promotes. Additionally, the efficiency of credit allocation processes can be significantly improved by blockchain technology. Banks can reduce the time and expenses associated with traditional, manual processes by using this technology to expedite the verification and validation of borrower information for credital location data.

PROBLEM STATEMENT

The most important ones include crowdfunding, sukuk, non-fungible tokens (NFTs), payment systems, cryptocurrency exchanges, and KYC. Usually, banks handle KYC on an individual basis. It is also feasible for banks to carry out transactions centrally and exchange information. In addition, blockchain technology can be

used for a KYC process. Consumer risk management is improved by the speedier, more transparent, and decentralized KYC procedure made possible byblockchain technology. A bank customer is required to make regular loan payments to the bank after using a loan. Banks should share information about restrictions, risks, and collateral with other banks in order to quantify their risks during the process. If banks have this information, they can assess their customers' risks more rapidly. Centralized credit bureaus are the foundation of traditional credit evaluation. These organizations collect consumer financial data from banks and then sell it back to other financial institutions to make money. However, because credit bureaus have the power to alter the data, this strategy raises questions about data ownership and security.

Existing System

- Using monetary institutions to launder money was simpler for both individuals and businesses. Financial institutions found it more difficult to identify and stop fraudulent actions, and they were able to transfer illegal funds through the financial system without being adequately detected.
- Due to the inability to adequately screen consumers, financial institutions were exposed to increased financial risks. Fraudsters found it easier to open accounts and conduct fraudulent activities when there was no customer verification. This can result in greater default rates, monetary losses, and higher operating expenses related to risk management.

Disadvantages of Existing System

- Because it inflates asset prices and creates fake economic conditions, it can skew financial markets.
- People may lose faith in the financial system's fairness and openness when money laundering is common.
- As they make investments in procedures and systems to identify and stop money laundering, financial institutions must pay more for compliance.

Proposed System

- In the financial industry, the use of blockchain technology offers an alluring chance for the transparent and safe interchange and preservation of credit allocation data.
- All parties participating in the capital allocation process—banks, borrowers, and other pertinent parties—benefit from this distributed ledger system's increased openness and confidence.
- Additionally, blockchain technology has the potential to significantly improve the effectiveness of credit allocation processes.
- By using this technology for credital location data, banks may expedite the validation and verification of borrower data, which lowers the time and expenses related to manual, traditional operations.

Advantages of Proposed System

- By ensuring that lenders accurately verify their clients' identities, KYC helps avoid fraud and identity theft.
- A safer and more open financial system can be achieved by institutions detecting and preventing the laundering of cash, terrorist funding, and other illicit investments through the use of strong KYC procedures.

2. RELATED WORKS

The 2023 study by Mansoor et al. examines how Blockchain technology can transform the traditional Know Your Customer (KYC) process in banking, which is often costly, slow, and prone to errors. By leveraging Blockchain’s decentralized, secure, and immutable ledger, banks can store and verify customer information more reliably while reducing reliance on intermediaries, minimizing fraud, and enhancing transparency. The article highlights the potential benefits of faster verification, lower operational costs, and increased trustworthiness of data, while also acknowledging challenges such as scalability and privacy concerns. Overall, the study emphasizes that integrating Blockchain into KYC systems could significantly improve

efficiency and security in the banking sector, provided these challenges are effectively addressed.[1]

The 2023 study by Rohitchandran, Santhoshkumar, and Kumar presents a system that integrates blockchain technology, a secure off-chain database, and cryptography to safeguard bank records. In this approach, original bank documents are stored in encrypted form off-chain, while their hash values are recorded on the blockchain to ensure data integrity and enable verification without exposing sensitive information. Smart contracts govern the storage and sharing of data, and cryptographic methods are used for encrypting documents and digitally signing messages. Additionally, a WebApp interface facilitates decentralized communication among transaction parties, enhancing the security, transparency, and reliability of bank record management.[2].

The 2023 study by Platt and McBurney reviews blockchain consensus mechanisms with a focus on their resistance to Sybil attacks, where malicious actors create fake identities to disrupt networks. Analyzing 21,799 research records and narrowing them to 483 relevant studies, the authors categorize mechanisms based on Sybil resistance, leader selection methods, and incentive structures. They find that strong Sybil resistance is typically achieved through Proof-of-Work or Proof-of-Stake, while weaker approaches rely on reputation systems or physical-world links. The study highlights that only a few core paradigms effectively defend against Sybil attacks in permissionless networks, though many innovative mechanisms provide limited protection in smaller-scale or controlled environments. [3]

The 2023 study by Woo and Yoo examines the factors influencing the adoption of blockchain-based electronic lab notebooks for research data management. Using a technology acceptance model and surveying 585 researchers from Korean universities and research institutes, the study finds that perceived usefulness and ease of use reduce perceived risks and increase the intention to adopt the system. Additionally, social norms help lower risk perception and encourage usage. The findings suggest that managers developing blockchain-based research services should focus on minimizing technical risks, providing user-friendly interfaces, and leveraging peer recommendations to promote broader acceptance among researchers.[4]

In the 2023 paper, Nakamoto introduces a peer-to-peer electronic cash system that enables direct online payments without financial intermediaries. The system addresses the double-spending problem by using a decentralized network that timestamps transactions into a continuous chain secured by proof-of-work. The longest chain reflects both the transaction sequence and the majority of computational effort, ensuring security as long as most CPU power is controlled by honest nodes. The network is designed to be minimally structured, allowing nodes to broadcast messages on a best-effort basis and rejoin freely, accepting the longest proof-of-work chain as the definitive record of transactions. [5]

The 2022 study by Karadag, Akbulut, and Zaim reviews blockchain applications within the fintech ecosystem, tracing fintech's evolution from the 1990s through developments in ATMs, cards, mobile transactions, and digital banking. The emergence of Bitcoin in 2008 popularized blockchain, whose decentralized, distributed ledger enables peer-to-peer transactions without intermediaries, while programmable platforms like Ethereum expanded its capabilities beyond simple transfers. The study consolidates various blockchain applications in finance, highlighting their business uses, market volumes, and potential future applications, and also notes that blockchain is increasingly being explored in sectors such as health, supply chain, education, and insurance. [6]

3. METHODOLOGY

The integration of blockchain-based KYC models in banking for credit allocation introduces innovative approaches that enhance data integrity, reduce redundancy, and accelerate decision-making. One key method involves using **permissioned blockchains**, where verified KYC data is stored as hashed references accessible by multiple banks, minimizing duplication and ensuring trust. Another approach leverages **Decentralized Identity (DID)** and **Verifiable Credentials (VCs)**, enabling customers to control their digital identities and

share cryptographically signed KYC proofs with lenders, facilitating privacy-preserving and cross-border credit access.

Additionally, **tokenization of KYC data** into digital assets (such as NFTs) allows secure, portable, and verifiable sharing of identity information, reducing the need for repeated verifications and offering an auditable data usage trail. Lastly, **consortium-based KYC utility platforms** bring banks together on a shared blockchain network to collaboratively validate and reuse KYC records, streamlining credit assessments while distributing compliance responsibilities and costs. These methodologies collectively modernize traditional KYC processes, promoting efficiency, security, and trust in credit allocation systems.

MODULES DESCRIPTION

User Interface Design:

To connect with server user must submit their username and password then only they can able to connect the server. If the user has already left, they can log in directly; if not, they must register their information on the server, including their username, password, email address, city, and country. To maintain the upload and download rate, the database will generate an account for every user. The user ID will be assigned to the name. Logging in is frequently used to enter a certain page. The query will be searched and displayed.

Bank:

Because they offer crucial services that support both personal financial management and economic activity, banks are an integral part of the economic system. They provide a safe haven for people and companies to manage and deposit their money, protecting it from loss or theft.

Admin:

Our project's third module is called Admin. Here, the administrator will log in using the ID and password that

the BC operator created. You will be taken directly to the admin home page after logging in. An administrator's job is to supervise and control the functioning and operations of a system, project, or organization. Administrators are in charge of organizing work, enforcing rules, and making sure that procedures function properly.

Customer:

Customer is the fourth module in our project. As required by the bank, customers must supply accurate, comprehensive, and current personal information, including their address. Additionally, they must promptly submit the proper paperwork and update their information in the event of any changes, such as a name change or new residence. A variety of financial operations carried out by account holders via their banking institution are referred to as customer bank transactions. These include deposits, in which clients put money into their accounts; withdrawals, in which they take money out of their accounts; and transfers, in which they move money between accounts or to other people or organizations. The bank keeps track of every transaction to guarantee correctness and preserve an extensive account history.

Transactions:

Transactions is the fifth module in our project. Customers engage with their accounts through credit and deposit transactions, which are essential banking operations. When money is transferred from another account, deposited into a customer's paycheck, or disbursed from a loan, this is known as a credit. Contrarily, deposits entail clients adding funds to their accounts via a variety of means, such as electronic transfers, checks, or cash deposits. To guarantee that account balances are updated correctly and to give clients a comprehensive and understandable picture of their financial activities, banks carefully document these transactions.

KYC:

A key procedure used by financial organizations to confirm the identification of their customers and evaluate the risks of illicit activity, such fraud or money laundering, is Know Your Customer (KYC). Banks and other financial institutions gather and examine consumer personal data, such as identification documents, proof of address, and financial history, through KYC procedures.

4. ALGORITHM

Know Your Customer (KYC).

The customer identification and due diligence processes used by financial organizations are included in KYC practices. The goal of these processes is to develop a thorough understanding of the client's financial activity, risk profile, and identification. Institutions can successfully reduce possible risks related to money laundering, terrorism funding, and other financial crimes by obtaining and evaluating this data. Additionally, customized service configurations that best meet the demands of the client are made possible by a strong KYC procedure. Blockchain provides a number of benefits for creating a unified platform for safe KYC data storage. The KYC mechanism that banks often employ operates on an individual basis. Blockchain technology offers an alternate method for collaborative KYC that goes beyond individual systems. All participating banks in the network can safely exchange customer information in a decentralized blockchain-based framework.

Block chain

Selecting the appropriate infrastructure is the first stage in developing a blockchain application. There are four primary categories of blockchain networks. Using a private blockchain network or a consortium blockchain network connecting banks is anticipated. Blockchain kinds and their connections.

1. PUBLIC BLOCKCHAIN NETWORK

Since there is no central authority, this kind of network is referred to as decentralized. Every participant (stakeholder) has the same rights and can add new data blocks to the network by validating and generating them. The most well-known example of this type of decentralized network is Bitcoin.

2. BLOCKCHAIN PRIVATE NETWORK

This type of network is permissioned, meaning only one entity controls access and validates transactions. The central authority defines the restricted powers of other parties. When a public authority wants to supervise a single entity, this structure is frequently selected.

3. BLOCKCHAIN NETWORK HYBRID

A hybrid network blends aspects of private and public blockchains. The verification procedure is comparable to a public network, guaranteeing transparency even when access is controlled by a single institution. An excellent illustration of this kind of network is the IBM "Food Trust" initiative, which is utilized in supply chains. Network of Consortium Blockchain. In contrast to private and public chains, consortium networks provide a unique structure within the realm of blockchain technology.

4. SMART CONTRACT

The term "smart contracts," first used by Nick Szabo in 1994, describes computer programs that are self- executing and self-verifying when they are installed on a blockchain network. These programs, which are just collections of pre-established rules, function decentralized and are impenetrable because of the immutability of the blockchain. Smart contracts guarantee the safe and open implementation of agreements through network replication and peer-to-peer supervision.

5. DATA FLOW DIAGRAM

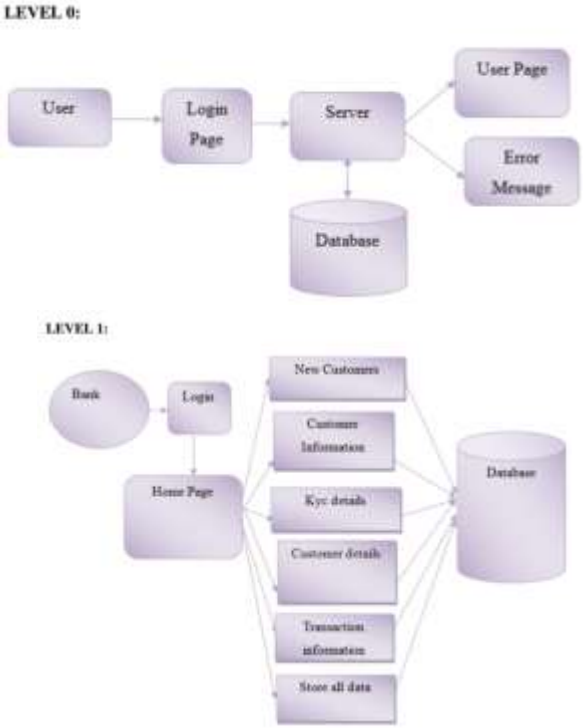

Fig 5: Data Flow Diagram

6. SYSTEM ARCHITECTURE

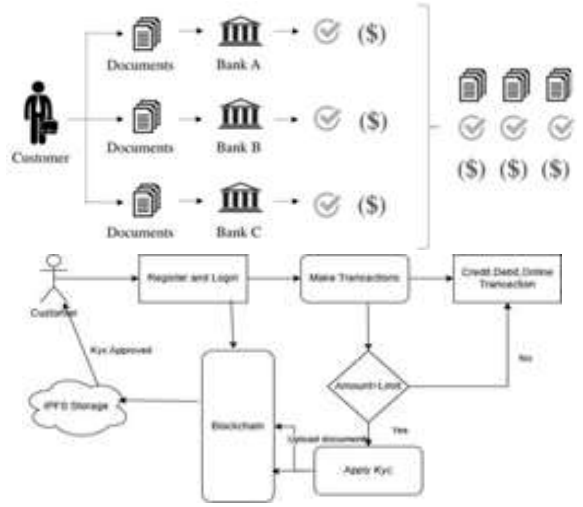

Fig 6: System Architecture of Project

The due diligence and customer identification processes used by financial organizations are included in KYC practices. The goal of these processes is to get a thorough grasp of the client's identity, financial activity, and risk profile. Institutions can successfully reduce possible risks related to money laundering, terrorism funding, and other financial crimes by obtaining and evaluating this data. Additionally, customized service configurations that best meet the demands of the client are made possible by a strong KYC procedure. Blockchain provides a number of benefits for creating a unified platform for safe KYC data storage. The financial industry has a strong chance to store and share credit allocation data in a transparent and safe manner by implementing blockchain technology.

7. RESULTS

The adoption of the proposed system (JBC07_Draft) delivers marked technical enhancements over the legacy VTJBC07 architecture. By leveraging blockchain's immutability and distributed ledger technology, it ensures data integrity, non-repudiation, and auditability across all transactional records. The introduction of decentralized identity management (DID) and reusable KYC frameworks eliminates data redundancy and facilitates interoperable identity verification across consortium members. Real-time data synchronization among participating institutions enhances credit risk assessment accuracy and enables proactive fraud detection through cryptographic validation. The shift from a centralized to a decentralized governance model provides improved system scalability, transparency, and operational resilience. Furthermore, the integration of smart contracts automates compliance enforcement, executes pre-defined business logic, and mitigates the risk of manual errors. Collectively, these technical advancements position the proposed system as a robust, secure, and scalable digital infrastructure optimized for modern, multi-institutional financial ecosystems.

8. FUTURE ENHANCEMENT

Future blockchain-based KYC process improvements are probably going to concentrate on boosting regulatory compliance and broadening its integration across other financial operations. Smart contracts and sophisticated cryptographic techniques will be incorporated into blockchain-based systems as they develop in order to increase security and automate compliance procedures. Letters of Guarantee (LoGs) will be more legitimate and less susceptible to fraud if they are tokenized and managed using non-fungible tokens (NFTs). Furthermore, more cooperation between banks and regulators will aid in resolving current legal and compliance issues, increasing the acceptance and efficiency of blockchain-based KYC solutions. The goal of these developments is to make the financial environment safer, more effective, and more cooperative.

9. CONCLUSION

The private Ethereum network and PoS consensus mechanism were taken into consideration when designing the blockchain-based KYC approach. Blockchain technology thus provides a revolutionary remedy for the drawbacks of conventional KYC in banking. Real-time risk assessment is made possible, data security is strengthened, and onboarding is streamlined with a shared, unchangeable ledger. Although there are still regulatory obstacles to overcome, there is no denying the possibility of improved productivity, teamwork, and risk management in a safe and open environment. Blockchain has the ability to completely transform KYC and usher in a new era of safe and effective consumer identification in banking as it develops and rules change.

10. 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.

[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.

[19] N. Szabo. (2019). Formalizing and Securing Relationships on Public Networks. Accessed: Mar. 11, 2024. [Online].

[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.