International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

An Improve the Onboarding Process in Trade Finance Applications Using Blockchain Technology

Ahmed Mohamed Abd El-Wahab
Information Systems Department
Faculty of Commerce and Business Administration
Helwan University, Cairo, Egypt
ahmed.mohamed.abdelwahab@commerce.***helwan.edu.eg***

Sherif Adel Abd El-Aleem
Business Administration Department
Faculty of Commerce and Business Administration,
Helwan University, Cairo, Egypt
Sherif.abdel@commerce.helwan.edu.eg

Hossam Mohamed Sherif
Information Security Governance, Risk & Compliance
Bank FABMISR, Cairo, Egypt
Hossam.mohamed21@commerce.helwan.edu.eg

Mohamed Ismail Roushdy
Faculty of Computers & Information Technology
Future University in Egypt, Cairo, Egypt
mohamed.roushdy@fue.edu.eg

Abstract— Today, challenges in Know Your Customer (KYC) and Anti-Money Laundering (AML) processes include inefficiencies, data silos, and the risk of fraudulent activities. Integrating blockchain technology offers a transformative solution to these issues. Blockchain's decentralized and tamper-resistant nature ensures a single, verifiable source of truth for customer information, reducing data discrepancies across institutions. Smart contracts can automate AML compliance checks, ensuring real-time monitoring and rapid response to suspicious activities. The immutability of blockchain records enhances auditability, facilitating regulatory compliance. Furthermore, the secure and transparent nature of blockchain instills trust among stakeholders, fostering collaboration in combating financial crimes. By leveraging blockchain in KYC and AML processes, the financial industry can achieve enhanced efficiency, reduced fraud, and strengthened regulatory adherence.

Keywords- Know Your Customer (KYC); Anti-Money Laundering (AML); Blockchain.

I.INTRODUCTION

Know Your Customer (KYC) is a procedural protocol aimed at validating a customer's identity, eligibility, and background as part of establishing a business relationship [23]. This mandatory process, in accordance with prevailing KYC regulations, is essential for all business institutions. It involves a thorough analysis of the suitability and associated risks to maintain an ongoing business relationship. An effective KYC procedure serves as a deterrent to financial fraudulent activities by preventing unauthorized individuals from accessing the banking system [1]

The primary goal of KYC is to shield banks from being unwittingly involved in money laundering and other illicit activities. Consequently, the KYC process aligns seamlessly with the broader framework of any financial institution's Anti-Money Laundering (AML) policy. This verification is carried out by soliciting valid identification documents such as country-specific ID cards, proofs of residence, income documentation, and similar credentials [24] and [2].

With ubiquitous Internet connectivity worldwide, the cost of global information transmission has significantly decreased. A tech-driven initiative has demonstrated the feasibility of leveraging the Internet to establish a globally shared, decentralized value transfer system that is virtually cost-free. This is achieved through consensus mechanisms and voluntary adherence to social contracts, empowered by the default mechanisms in place [3] and [25].

Recent advancements in technologies such as big data, machine learning, and the Internet of Things (IoT) present an effective solution for addressing contemporary challenges related to the storage, management, and accessibility of vast amounts of data, as well as the control of sensing devices. However, the issue of data breaches remains a significant concern in big data and IoT systems. Security, transparency, and privacy are paramount considerations in today's landscape. Blockchain technology emerges as a viable solution, incorporating distributed ledger functionality to enhance security, transparency, and privacy, particularly over insecure communication channels.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Blockchain is an incorruptible, immutable, and decentralized digital public ledger capable of recording not only financial transactions but virtually any valuable information [3].

On the other hand, the conventional KYC (Know Your Customer) approach is centralized and repetitive. There exists a lack of standardization in the required KYC documents across various banks, compelling users to repeat the same KYC procedures when creating accounts with different banks. Moreover, users have limited control over the information they share. Given the sensitivity of KYC data, it is vulnerable to threats from malicious actors. Therefore, it is crucial to ensure that KYC systems are well-secured against unauthorized access and denial-of-service attacks in order to address these challenges.

The structure of this paper unfolds as follows: In Section 2, delves into the background of Blockchain and KYC. While in section 3, conducts an examination of related work. Moving on to section 4, a framework and its implementation is proposed. In addition, section 5, provides a comparison with related work. Finally, conclusion and directions for future work are reported in section 6.

II.BACKGERAOND

A. BLOCKCHAIN TECHNOLOGY

Blockchain technology stands as a revolutionary innovation with the potential to reshape various industries by introducing unprecedented levels of transparency, security, and efficiency. Initially proposed in Satoshi Nakamoto's seminal 2008 paper, blockchain serves as the foundational technology for cryptocurrencies like Bitcoin, but its applications extend far beyond the realm of digital currencies [4].

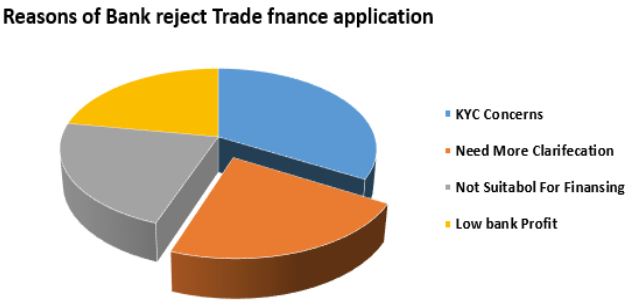
Essentially, blockchain is a decentralized and distributed ledger designed to record transactions across a network of computers. Each transaction, or "block," intricately links to its predecessor, forming an unalterable chain of blocks. This tamper-resistant feature renders recorded information virtually immutable, sparking significant interest across sectors like finance, healthcare, and supply chain management [5].

The decentralized consensus mechanism ensures that all network participants maintain a synchronized, secure, and transparent view of the data. This mechanism not only reduces the risk of fraud but also eliminates the need for intermediaries, streamlining operations. Amid challenges in data security, trust, and operational efficiency, blockchain emerges as a promising solution, offering a new paradigm for information storage and transaction conduct. The technology has the potential to reshape how we interact with data, fostering a future characterized by heightened security, transparency, and decentralization [5].

B. Know Your Customer (KYC)

Know Your Customer (KYC) is a procedure designed to authenticate a customer's identity when seeking to engage with an institution's services. Given the rising concerns such as terrorist financing, corruption, and money laundering, the enforcement of KYC policies has become imperative to thwart illicit transactions. The conventional KYC process is criticized for its deficiencies in privacy and security [6]. According to a recent survey, a significant factor contributing to the rejection of trade finance proposals is associated with KYC (29%), followed by insufficient information and low-profit issues (see Figure 1).

Figure 1. Reasons for the rejection of trade finance applications [7]



- Challenges with the traditional KYC process:
  Conducting KYC is straightforward in countries with electronic identity verification services. However, for financial institutions lacking access to such services, accepting clients poses risks [8]. Consequently, onboarding a new client involves a time-consuming KYC process, with each financial institution independently conducting its own verification. For instance, when a client seeks to open a bank account, the bank forwards their details to registries, where the information is stored for KYC compliance. This repetitive process is undertaken each time a client initiates a new bank account application.
  The term "KYC," or Know Your Customer, emerged in the late 1980s in the banking and financial sector, primarily introduced by the United States. It became imperative for institutions like banks and insurance companies to verify customer information to prevent involvement in illegal activities when enrolling new customers or updating existing ones [9]. Figure 2 illustrates the current KYC process undertaken by institutions for internal customer verification.
- Customers encounter the following challenges in the current KYC filing process[8]:
  1. Trustworthy users may encounter human errors while completing the KYC form. Additionally, for individuals with multiple accounts, the KYC process becomes more time-consuming, making it challenging to validate details for a single account. The primary cause of these issues is the absence of an automated system that captures account holders' details and automatically filters out false positive entries.
  2. There is a shortage of knowledgeable and skilled personnel to provide guidance during the KYC process.
  3. During onboarding, a malicious user may intentionally input incorrect (false positive) KYC data, given that it is stored in a centralized database lacking cross-checking with other organizations. This can increase the screening time for the organization and contribute to reputational risks.
  4. The traditional KYC process, being time-consuming, leads to delays in the overall customer enrollment process with banks or financial institutions.
  5. Despite its time-consuming nature, KYC poses reputational and regulatory risks, potentially

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

tarnishing a brand's name. Enrolling an unscrupulous customer with fraudulent KYC details puts the company's reputation at stake.

6. The absence of common internationally agreed stringent standards makes it difficult for banks in different nations to achieve KYC compliance, especially in transactions involving parties from different nations.

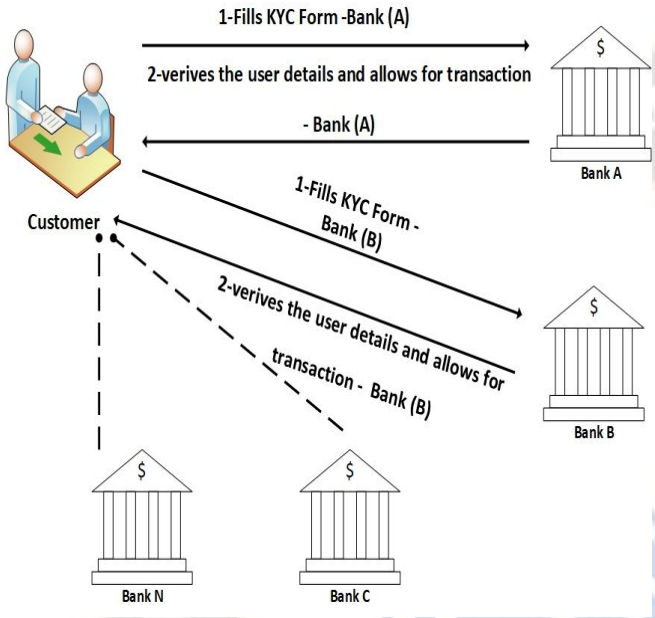


Figure 2. Current State of KYC Filing

TABLE I. OUTLINES THE CHALLENGES ASSOCIATED WITH THE EXISTING KYC SYSTEM ALONG WITH THEIR CORRESPONDING PROPOSED SOLUTIONS

#	Issue [8]	Solution
1	Human error in filling KYC form	Implement video-based KYC to capture live photos of customers
2	KYC process for joint accounts	Apply Machine Learning techniques to automatically remove false positive entries
3	Lack of knowledgeable and skilled personnel	Provide training and utilize automated robotic systems
4	Delays in the overall customer enrollment	Integrate Blockchain technology
5	Reputational and regulatory risks	Utilize Blockchain technology
6	Cross-border compliance	Leverage Blockchain technology for enhanced compliance

From the above-mentioned issues, one possible way to overcome the 4, 5, 6 issues are to use a centralized database, where a single node is designated as an oracle to serve the requests of several client nodes. However, it is highly vulnerable to single point of failure, in case, the oracle fails. Due to such failures, Distributed Ledger Technology (DLT) has emerged as a feasible solution to the same and being distributed in nature, reliability.

Under the current KYC framework, policies such as customer acceptance, customer identification, and transaction monitoring with risk management are critical components [10]. Blockchain technology presents an opportunity for optimization in these areas. First mentioned in Satoshi Nakamoto's 2008 white paper, blockchain is essentially a chain of blocks with immutable records, serving as a public ledger. Originating from the concept of timestamping, blockchain ensures the integrity and authenticity of digital documents across unsecured networks [4].

In essence, blockchain can be described as a platform where individuals lacking mutual trust collaborate to make rational decisions toward a common goal. Nodes in the blockchain network, situated at different locations with varied resources, manage their operations through a message-passing system. As blockchain operates over an insecure network, cryptographic algorithms are employed to uphold data integrity and authenticity, guided by the principle of being visible and verifiable to all within the network [11].

III. RELATED WORK

In the realm of online banking, while its popularity thrives on features like location independence and 24/7 availability, it grapples with security threats such as phishing and malware. Security measures like one-time passwords (OTPs) are employed, but vulnerabilities exist, prompting the consideration of Challenge Questions (CQ) from a dynamic KYC database for transaction authorization. This proposed method ensures secure financial access, mitigates theft risks, and minimizes SMS delays without the need for additional hardware, enhancing dynamic security in online banking [9].In the contemporary landscape, there is a growing emphasis on online transactions and the digitalization of information. This shift towards digitized information has transformed the dynamics of information transfer, enabling faster and more cost-effective processes. The concept of timestamping plays a crucial role, where each digital document receives a timestamp (TS) indicating its creation time before being transacted over a network. This timestamp serves as a verifiable record to prevent subsequent denial by the receiver [12].

When Bitcoin was initially proposed as an application of blockchain, it was primarily designed to facilitate digital currency transactions and eliminate the need for third-party

Intermediaries in currency exchange among countries [13]. As blockchain expanded its reach into various sectors of software development, particularly with the introduction of consortium blockchains, its global recognition grew. In a consortium blockchain, multiple organizations collaborate on a defined goal without trust issues, utilizing the PBFT consensus protocol with state machine replication [14].

Despite the advancement of digital information, challenges persist in the Know Your Customer (KYC) process, which traditionally relies on paperwork and offline methods, emphasizing visual confirmation of the consumer [14].

Perry Mayo proposed a blockchain-based KYC system to enhance efficiency and reduce costs associated with customer onboarding [15]. Rutter advocates decentralizing the KYC process and presents two decentralized scenarios running on Corda: the 'self-sovereign model' and the 'bank sharing model.' Norvill [16] introduced a system allowing automation and permission document sharing to simplify the KYC process.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

The need for adaptation, regulators must innovate and tailor regulations to suit the dynamics of the FinTech landscape. Embracing the concept of RegTech, a fusion of regulation and technology, can provide a viable solution. This involves the digitalization of processes, notably the identification and verification (KYC/CDD), to align with the nature of FinTech. the adoption of E-KYC/CDD involves utilizing electronic signatures for the verification and identification of consumer profiles. This represents a progressive step towards creating regulations that are not only conducive to FinTech but also address the unique challenges posed by the intersection of technology and finance[18].The integration of blockchain with IPFS storage systems minimizes the reliance on paper certificates for approval, resolving issues like staff verification difficulties and redundant clerk submissions [19].

A cloud user identity management protocol based on the Ethereum blockchain, accompanied by the establishment of a straightforward credit management system framework. This novel protocol represents an enhanced iteration of CIDM (Consolidated Identity Management), referred to as the EIDM (Ethereum-based Identity Management) protocol. The improved protocol incorporates JSON Web Token (JWT) from OAuth 2.0 to introduce smart contracts into the EIDM protocol, and a credit management system is integrated to offer a trustworthy identity authentication protocol for both cloud users and service providers. This protocol addresses the issue of over-reliance on third parties in existing identity management system solutions [20]. The paper details the design of a container-based monitoring and auditing architecture aimed at enhancing data privacy in cloud ecosystems. This architecture incorporates a Blockchain network and aligns with GDPR obligations, tracking activities executed by cloud providers on user data 21].

Authentication and authorization (A & A) mechanisms play a pivotal role in ensuring the security of Internet of Things (IoT) applications, particularly in scenarios like smart grid systems where data processing and exchange occur without direct human intervention. These smart grids represent a notable IoT application. In current systems, commonly employed A & A protocols are centralized, introducing security risks such as information leaks, unauthorized access, and identity theft. To address these concerns, this study proposes a new distributed A & A protocol for smart grid networks, leveraging blockchain technology [22].

IV.PROPOSED FRAMEWORK

A. Harnessing Blockchains for Solutions:

Blockchain technology offers a solution to various KYC-related problems, including the onboarding process. The public distributed ledger of blockchain allows for the dissemination of verified client information across multiple banks. Once KYC is completed, other financial institutions can access this information with explicit authorization from the client. This streamlines the KYC process, making it more efficient, simpler, less time-consuming, and cost-effective. Additionally, traditional KYC solutions relying on centralized databases pose security vulnerabilities. In contrast, blockchain replicates KYC data across diverse nodes, ensuring immutability and traceability due to its append-only data structure [23].

B. KYC using Blockchain Technology:

This Proposed Framework show cases how blockchain can be employed to facilitate the KYC process. Figure 3 outlines the KYC (Proposed Framework).

- The process is elucidated as follows:
    1. The client grants a Governmental Institution permission to conduct KYC, providing documents such as an identity card and financial details.
    2. The Governmental Institution reviews and validates the client's
    3. identity and financial information, approving them as 'KYC Compliant.'
    4. The Governmental Institution adds KYC information and status to a blockchain platform, ensuring verification is confirmed.
    5. The Governmental Institution issues the client a token serving as proof of their KYC status.
    6. The client authorizes a third party to verify their KYC status.
    7. The prospective bank verifies the KYC information.

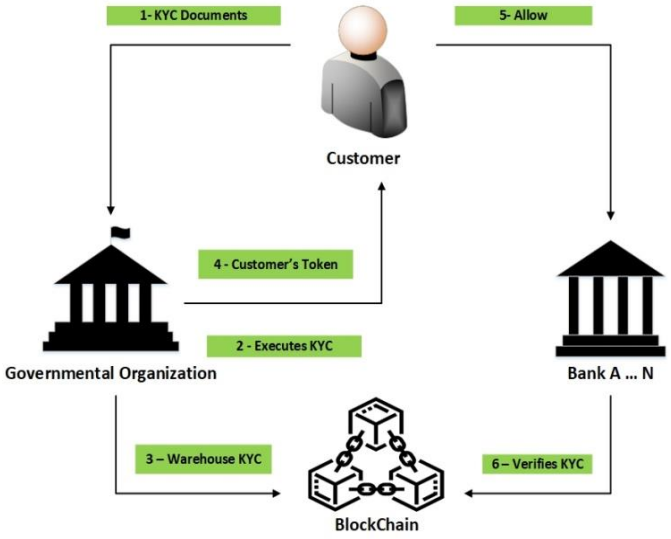


Figure 3. Proposed Framework

C. Blockchain KYC Implementation:

To execute the blockchain KYC, we utilized the Ethereum blockchain platform and employed the Solidity programming language for crafting the smart contract.

The primary operations within the system can be elaborated further below. The implementation of the proposed model encompasses the following steps:

- Prerequisites – The following installed before proceeding mandatory

1. A JavaScript runtime environment.
2. Hardhat: A development environment for Ethereum software.

- Installation.
- Running the Local Blockchain with Hardhat Node shows in Figure 4.
- Hosting KYC Files Locally.
- Deploy the smart contract to the local Ethereum network.
- Creating a Token/Asset shows in Figure 5.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

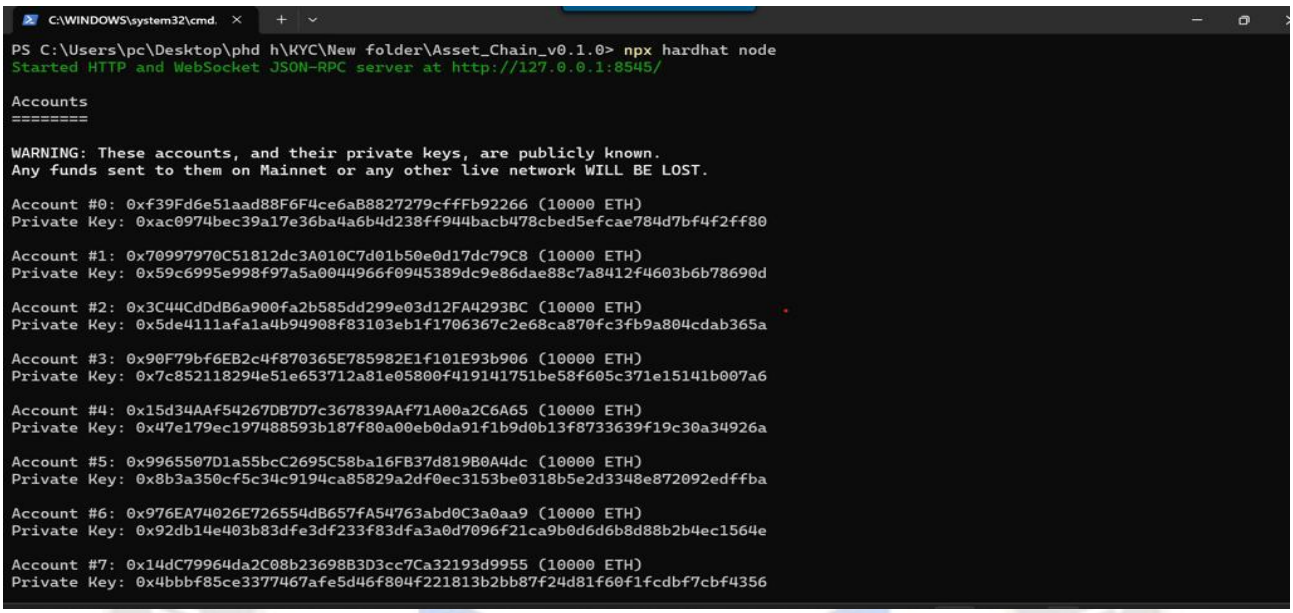


Figure 4. Blockchain Node

Figure 5. Token/Asset

D. Advantages the Proposed System:

1. Streamlined Onboarding Process: The reverification process for customers with existing details in Blockchain is significantly expedited, resulting in a notable reduction in onboarding time.
2. Cost-Efficient Verification: Leveraging shared services can lead to a substantial decrease in the overall cost of client verification.
3. Enhanced Fraud Protection: The immutable nature of Blockchain contributes to a lower risk of fraudulent customer details, bolstering security measures.
4. Transparent Data History: The Blockchain's capability to record all customer data updates facilitates a natural audit trail, enabling the tracking of the origin of any inaccuracies.
5. Heightened Operational Reliability and Security: The anonymity of all operations conducted on Blockchain ensures increased reliability and safety throughout various processes.
6. Strengthened Identity for Refugees: In situations where countries may withhold documents for proof of existence from refugees, Blockchain serves as a valuable tool for citizens to reinforce their identity securely.

V. COMPARISON FOR RELATED WORK

TABLE II. HERE'S A COMPARING KYC IN ONLINE BANKING AND OUR RESEARCH ON TRANSACTION AUTHORIZATION USING KYC INFORMATION ON THE BLOCKCHAIN

Feature	Our Proposal	P. Mondal, et. al [9]	A. Ghozi [18]
Centralization	Decentralized system using blockchain technology.	Centralized system managed by banks or financial institutions.	centralized
Data Storage	KYC information is distributed across the blockchain network, reducing the risk of a single point of failure.	KYC data stored in the databases of individual institutions, leading to data silos.	Stored centrally
Verification Time	Streamlined KYC process on the blockchain allows for quick and	KYC verification process can be time-consuming, involving manual checks	Real-time verification can make the process more time-efficient

	efficient verification.	and communication between institutions.	
Data Immutability	KYC information stored on the blockchain is immutable, ensuring the integrity of the data.	Data can be altered or deleted in centralized databases, potentially leading to inaccuracies.	Immutability may vary, but often includes secure storage and authentication
Security	Blockchain employs cryptographic techniques, providing enhanced security against unauthorized access and tampering.	Centralized databases are susceptible to security breaches.	digital signatures
Efficiency	Blockchain can streamline the KYC process, allowing authorized parties to access and verify information quickly.	KYC processes may involve redundant checks and delays.	Real-time verification enhances overall efficiency
Cost Efficiency	Initial implementation costs may be high; potential long-term cost savings	Cost-effective compared to traditional KYC; varies by platform	Cost-effective, especially in the long run, due to automation and efficiency gains

VI.CONCLUSION

The application of a blockchain experimentation framework emerges as a valuable resource for researchers and developers aiming to gain a deeper understanding of blockchain technology. This underscores the pressing need for a highly adaptable and controllable environment conducive to extensive blockchain experimentation. The paper delves into a discussion of the implementation of a proof-of-concept (POC) for a Know Your Customer (KYC) application on the blockchain, presenting preliminary results that underscore the framework's efficacy in conducting large-scale blockchain evaluation experiments in a real-world setting. Looking ahead, several open questions warrant exploration, particularly in the evaluation of blockchain environments from various perspectives. Emphasis will be placed on addressing security and privacy concerns associated with private blockchain applications.

In summary, the integration of blockchain technology emerges as an innovative solution to challenges encountered in Know Your Customer (KYC) processes. The decentralized and tamper-resistant attributes of blockchain effectively tackle inefficiencies, dismantle data silos, and mitigate the risk of fraudulent activities. By establishing a unified and verifiable source of truth for customer information, blockchain significantly diminishes discrepancies across institutions. Furthermore, the secure and transparent features of blockchain cultivate trust among stakeholders, fostering collaboration within the KYC domain.

Ultimately, the incorporation of blockchain technology into KYC processes offers a transformative solution, promising improved efficiency, minimized fraud, and heightened adherence to regulatory standards.

REFERENCES

[1] AUBOIN, Marc; DICAPRIO and Alisa, Why do trade finance gaps persist: Does it matter for trade and development?, January 2017.
[2] G .Gorton ," Misunderstanding Financial Crises: Why Don't We See Them Coming? Oxford University Press, 2012 ISBN 978-0-19-992290-1." Economic Issues 20.Part 1 (2015).
[3] M. Vukoli,"The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication", 2016
[4] Deloitte,"Blockchain in banking While the interest is huge, challenges remain for large scale adoption Headline Open Sans Bold Subheading Open Sans Light up to two lines of text", 2017, pp.5-32.
[5] S.Haber, and W.S. Stornetta,"How to time-stamp a digital document", Springer, Berlin Heidelberg, 1991.
[6] CHRISTIE, Robert. Setting a standard path forward for KYC. Journal of Financial Transformation, 2018, 47:, pp. 155-164.
[7] M. Mainelli, M. Smith, "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)," The Journal of Financial Perspectives, 2015,vol. 3, no. 3, pp. 38–69.
[8] J. De Geer, "Method and system for identity and know your customer verification through credit card transactions in combination with internet based social data," May 14 2012.
[9] P. Mondal, R. Deb and M. Huda," Transaction Authorization from Know Your Customer (KYC) Information in Online Banking", 9th International Conference on Electrical and Computer Engineering 20-22 December, 2016, pp. 523-526
[10] M.Castro, , "Practical Byzantine fault tolerance and proactive recovery." ACM Transactions on Computer Systems (TOCS) 20, no. 4 (2002), pp. 398-461.
[11] Haber, Stuart, and W. Scott Stornetta. "How to timestamp a digital document." In Conference on the Theory and Application of Cryptography, Springer, Berlin, Heidelberg, 1990, pp. 437-455.
[12] N. Kapsoulis, A. Psychas, G. Palaiokrassas, A. Marinakis, A. Litke, and T. Varvarigou. "Know Your Customer (KYC) Implementation with Smart Contracts on a Privacy Oriented Decentralized Architecture." Future Internet 12, no. 2 (2020): 41.
[13] W.Shbair, M. Steichen, and J.François. "Blockchain orchestration and experimentation framework: A case study of KYC." IEEE/IFIP Man2Block 2018-IEEE/IFIP Network Operations and Management Symposium. 2018
[14] D.Lopez, and B.Farooq. "A multi-layered blockchain framework for smart mobility datamarkets." Transportation Research Part C: Emerging Technologies 111 (2020), pp. 588-615.

[15] M.Parra, José, T. Thoroddsen, and O. Ross. "Optimised and dynamic KYC system based on blockchain technology." International Journal of Blockchains and Cryptocurrencies 1, no. 1 (2019), pp. 85- 106.
[16] J.Moyano, J. Parra, and O.Ross,"KYC optimization using distributed ledger technology." Business & Information Systems Engineering 59, no. 6 (2017), pp. 411- 423.
[17] A.Ghozi, "The Urgency of Electronic Know Your Customer (E-KYC): How Electronic Customer Identification Works to Prevent Money Laundering in the Fintech Industry" diponegoro law review 7.1 (2022), pp. 34-52.
[18] S.Tang, Z.Wang, J.Dong, and Y.Ma, Blockchain-enabled social security services using smart contracts. IEEE Access, 10, (2022), pp.73857-73870.
[19] S.Wang, R. Pei, and Y. Zhang. "EIDM: A ethereum-based cloud user identity management protocol." IEEE Access 7 (2019), pp. 115281-115291.
[20] M.Barati, G.Aujla, S.Member, J.Llanos, K.Duodu, O. Rana, M. Carr, , R.Ranjan, Privacy-aware cloud auditing for GDPR compliance verification in online.
[21] healthcare." IEEE Transactions on Industrial Informatics 18.7 (2021), pp. 4808-4819.
[22] Y.Zhong ,M.Zhou, J.Li, J.Chen, Y. Liu , Y.Zhao, and M. Hu,. Distributed blockchain-based authentication and authorization protocol for smart grid. Wireless Communications and Mobile Computing, (2021), pp. 1-15.
[23] Yadav, A. Kumar, and R.Bajpai, "KYC optimization using blockchain smart contract technology." Int. J. Innov. Res. Appl. Sci. Eng 4.3 (2020). pp. 669-674.
[24] What is KYC?. https://www.swift.com/your-needs/financial-crime-cyber-security/know-yourcustomer-kyc/meaning-kyc. Accessed 07 Oghast 2023
[25] What is KYC: steps to do KYC online: types of KYC: Paisabazaar. https://www.paisabazaar.com/ aadhar-card/what-is-kyc/. Accessed 04 Aghast 2023
[26] K. Kim, M.Latoja, S. Beck and M.Tayag ,"Trade Finance Gaps, Growth, and Jobs Survey", 2021.