iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VII **Month of publication:** July 2023

DOI: https://doi.org/10.22214/ijraset.2023.54834

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

E-KYC System Using Blockchain

Soham Chakraborty[1], Akhil Boddul[2], Vivek Patil[3], Ganesh Raje[4], Prof. Ujwala Gaikwad[5]
Department of Computer Engineering, Terna Engineering College, Nerul, Navi Mumbai

Abstract: ***Know your client or simply KYC, is a process utilized by businesses and financial institutions to identify their clients and evaluate any potential risks associated with illegal intentions and unethical behavior. The term KYC often refers to bank regulations and anti-money laundering regulations aimed at governing these activities. Due to concerns over bribery and unethical behavior, companies of all sizes are required to implement KYC to ensure their agents, consultants, and distributors comply with anti-bribery regulations. Despite the use of traditional KYC systems, there are limitations to their effectiveness. To address these limitations, a proposed system has been developed that uses the immutable nature of Distributed Ledger Technology (DLT) to create a tamper-proof system. This system enables customers and financial institutions to verify and record KYC documents on the DLT, providing greater efficiency, cost reduction, improved customer experience, and end-to-end transparency in integrating customer documents into the bank's database. Additionally, this system eliminates the need for repeated KYC checks performed by banks through the creation of a secure and common blockchain database. The blockchain's secure nature ensures that unauthorized changes to the data are immediately invalidated and the use of a proof-of-reputation concept makes the verification process more robust.***

I. INTRODUCTION

To address the issue of money laundering, financial institutions depend significantly on KYC processes. Understanding their customers and preventing money laundering are key components of an institution's anti-money laundering program. The process of verifying the identity of a client, employee, vendor, or stakeholder using validating factors is known as KYC verification. These factors may include photo-based IDs, facial features, answers to randomized questions, and other similar information. [1]

Based on recent estimates, global KYC spending increased to approximately $1.2 billion in 2020. Despite the significant amount of money invested in improving KYC processes, the process is not foolproof and still faces issues. Despite its significance, KYC continues to operate inefficiently. According to estimates, 80% of KYC efforts are focused on information gathering and processing, while only 20% are focused on assessing and monitoring due to time-consuming and labor-intensive tasks, duplication of effort, and the risk of errors. [2] Not only does the current KYC process fail to meet its intended purpose on the financial institution's front, but it also provides customers with a frustrating experience due to its long, repetitive, and tedious nature. The good news is that several financial institutions and service providers are working to address these issues by integrating new technologies such as artificial intelligence and cognitive technologies. The objective is to explore technology that will eliminate inefficiencies and duplications in the KYC process.

The use of blockchain technology presents a viable solution to this problem. To comprehend the potential for blockchain to revolutionize the KYC process, it is necessary to understand the issues currently associated with it. The challenges underscore the need for blockchain technology to be implemented for KYC purposes. Businesses, such as banks, insurance companies, investment firms, and non-banking financial companies (NBFCs), carry out tens of thousands of KYC verification transactions daily. Due to the sheer volume of daily verification transactions, a high degree of confidence in individual verification queries' validation is insufficient. Once the relevant authorities verify identities, KYC verification is deemed complete. However, such a system encounters scaling issues to keep up with business growth. Over-reliance on centralized authorities for authentication, the risk of errors, and a lack of fail-safe mechanisms are among the other challenges. [3]

Using blockchain-based electronic KYC verification provides a highly effective alternative to conventional methods of KYC verification. With distributed ledger technology (DLT), businesses can aggregate data from multiple service providers using decentralized blockchain techniques, creating a single, cryptographically secure and immutable database. This eliminates the need for a third party to verify the accuracy of the information. Employing DLT for customer verification has several advantages, including the ability to verify information independently and efficiently. The use of blockchain technology could streamline and simplify KYC processes. This project involves the implementation, discussion, and analysis of a blockchain-based e-KYC system that collects customer information once, eliminating the need for redundant KYC verification processes.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

II. RELATED WORK

It is crucial for financial institutions, and every institution, to verify the identities of their customers. This process usually involves a lengthy practice where specific documents are presented, and various types of background checks or verification are conducted. In the traditional KYC system, each bank performs its own identity check, resulting in a waste of time as each user's identity is verified individually by each organization or government structure. [4]

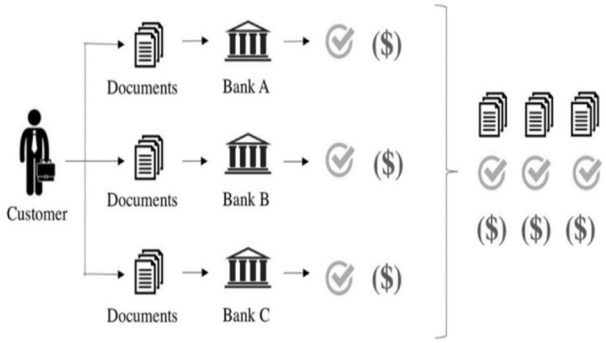


Figure 1 - Manual KYC process[6]

Smart contracts on the Ethereum blockchain have been used by a number of researchers [5, 6, 9–12]. It is advised to keep KYC data off-chain and put only the data hashes on the blockchain to get over Ethereum's limited storage capacity [13,18].

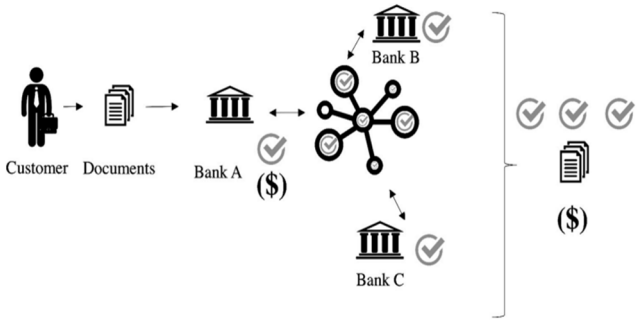


Figure 2 - blockchain based EKYC process[6]

The InterPlanetary File System (IPFS) is used to store certified KYC data, and only the encrypted data hashes are kept on the Ethereum blockchain, according to a method proposed by Patel et al. [12]. They created the KASE service, which generates two different types of smart contracts: one designed specifically for individuals, and another for businesses. The customer smart contract's main goal is to obtain customer data from IPFS storage and add data to the Ethereum blockchain. Obtaining the organization's information from IPFS storage and integrating it into the KASE service are the primary responsibilities of the organisation smart contract. The main duties of the organisation smart contract are obtaining the information of the organisation from IPFS storage and integrating it into the KASE service. Researchers [8] developed a token-based smart contract that addressed the KYC provider, monetary service, KYC-compliant economic service, and confidentiality-focused KYC-compliant banking service in order to facilitate token exchange and movement in banks.

Additionally, permissioned blockchains like Hyperledger allow for the execution of smart contracts. Numerous authors have suggested methods for KYC verification using this method, including Patel et al. [12] (KASE service), M. Steichen et al. [15], and Singhal et al. [16]. These suggested frameworks guarantee the confidentiality and anonymity of participants. According to paper [7], the proposed double-blind data-sharing model ensures confidentiality and anonymity by utilising techniques like public key systems, identity suppliers, consumer approval recorded on the ledger, encrypting data, and protective keys for documents, which enable transferring keys used for encryption among providers on the blockchain. The interfaces of users for processing data and access make up the top tier of the structure, REST-based APIs for contract querying make up the transitional layer, and smart contracts scripts make up the bottom layer. A different Hyperledger-based KYC solution utilising the built-in decentralised public key infrastructure (DPKI) of Hyperledger Indy was also introduced by the authors [9].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

III. METHODOLOGY

1) *Platform Selection:* The first step in the eKYC methodology is to choose a suitable blockchain platform. Ethereum, Hyperledger, are some of the commonly used platforms for eKYC implementation. The choice of platform should be based on the specific requirements of the eKYC process, such as security, scalability, and cost.
2) *Data Structure Design:* The next step is to define the data structure for storing customer information on the blockchain. This data structure should be designed with privacy and security in mind, and it should allow for easy retrieval of information by authorized parties.
3) *Customer Data Storage:* Customer data is then securely stored on the blockchain using encryption and other security measures to ensure the protection of sensitive information. Access to the customer data is restricted to authorized parties only.
4) *Customer Verification:* The customer's identity is verified using various methods, such as biometrics, government-issued IDs, or other forms of identification. This information is used to confirm that the customer is who they claim to be.
5) *Approval and Rejection:* Based on the results of the customer verification, the customer's request is either approved or rejected. If approved, the customer's information is updated on the blockchain. If rejected, the customer's request is denied and the information is not updated.
6) *Information Update:* Once the customer information is verified and approved, it can be updated on the blockchain. This ensures that authorized parties have access to the most current information.
7) *Information Access:* Authorized parties can securely access the customer information from the blockchain for various purposes, such as for financial transactions, compliance with regulations, or other business requirements.
8) *Compliance:* The eKYC process must adhere to applicable laws and regulations, including anti-money laundering (AML) and know your customer (KYC) regulations. This may entail obtaining customer consent, securely storing their data, and notifying the relevant authorities of any questionable activity.
9) *Monitoring and Maintenance:* Regular monitoring of the eKYC process is necessary to ensure its proper functioning and the security of customer information. This may involve periodic audits and updates to the smart contract and data structure as required.
10) *Security Measures:* Robust security measures, such as firewalls, encryption, multi-factor authentication, and regular backups, must be implemented to protect against data breaches, hacking, and other security threats.

IV. SMART CONTRACTS

Smart contracts are contracts that execute themselves by following the terms of the agreement that are directly written in code. In an eKYC system, smart contracts can automate the process of verifying and storing customer information on a blockchain network. Here's a brief overview of how smart contracts can be used in eKYC:

1) *Data Storage:* Smart contracts can be used to store customer information on a blockchain network in a secure and decentralized manner. This information can be encrypted and only accessible by authorized parties.
2) *Verification Process:* The verification process can be automated using smart contracts. For example, when a customer submits their information for verification, the smart contract can automatically compare the information against a trusted source (such as a government database) to confirm the customer's identity.
3) *Approval and Rejection:* Based on the results of the verification process, the smart contract can automatically approve or reject the customer's request. If approved, the customer's information is updated on the blockchain. If rejected, the customer's request is denied and the information is not updated.
4) *Information Access:* Smart contracts can be used to manage access to the customer information stored on the blockchain. Only authorized parties can access the information, and the access permissions can be managed using the smart contract.
5) *Compliance:* To comply with anti-money laundering (AML) and know your customer (KYC) regulations, it is essential for the eKYC process to adhere to relevant laws and regulations. Smart contracts can be programmed to make sure that the process is in accordance with these regulations. For instance, smart contracts can be used to obtain customer consent, securely store their information, and report any suspicious activity to the appropriate authorities.

By using smart contracts, eKYC processes can be made more efficient, secure, and transparent. The automation of the process reduces the risk of human error and ensures that the process is consistent and transparent.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

V. SYSTEM ARCHITECTURE

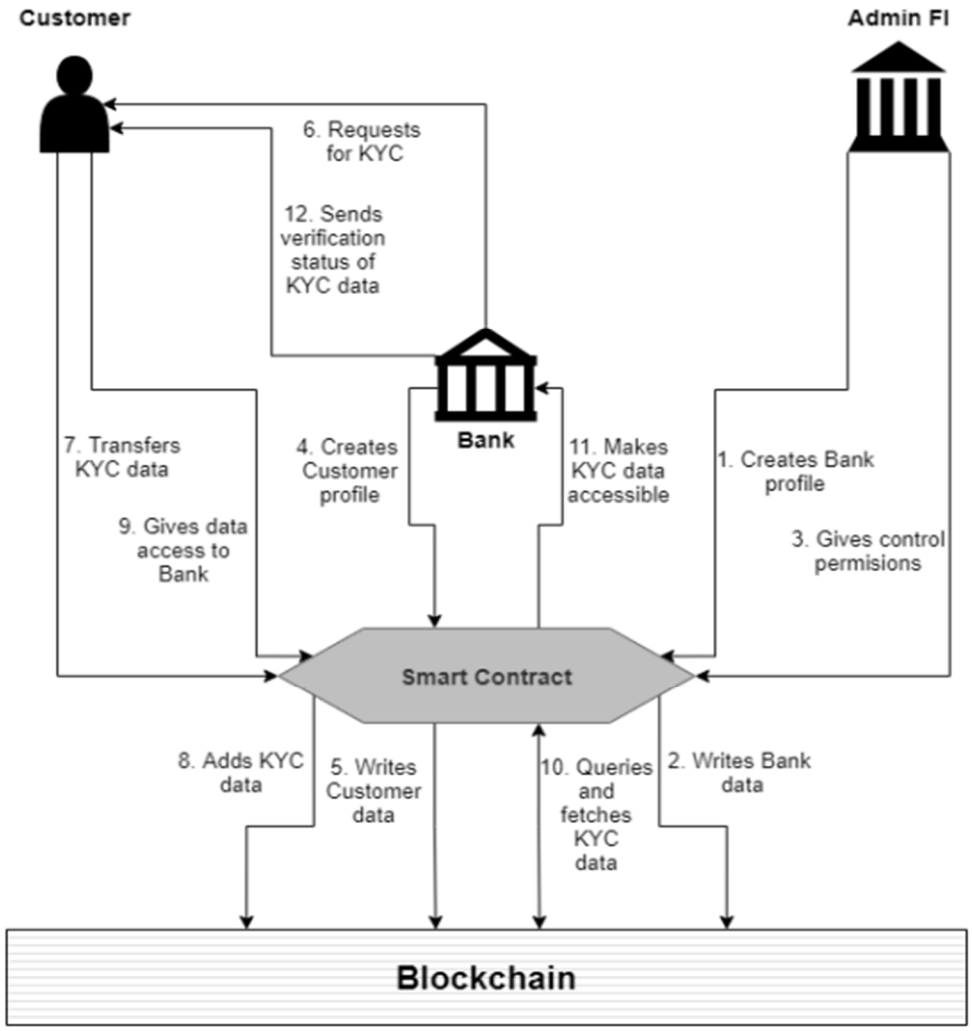


Figure 3 - EKYC system architecture[6]

The architecture of an eKYC system using blockchain typically involves the following components:

1) *User Interface:* This is the front-end component of the system where users can interact with the platform. Users can submit their identity details, documents, and other relevant information through this interface.
2) *Smart Contract:* Smart contracts are self-executing agreements that reside on the blockchain. They can automate the eKYC process, ensuring transparency and security throughout. Additionally, smart contracts can store user identity information and digital signatures in an immutable way, making them tamper-proof.
3) *Blockchain:* The blockchain serves as a decentralized ledger that stores all the information related to the eKYC process. The use of blockchain ensures that the information is immutable and tamper-proof.
4) *Identity Verification:* The system can use a variety of methods to verify the identity of users, such as facial recognition, biometrics, and other methods.
5) *Data Storage:* The system can store user data and other relevant information in a decentralized and secure manner, ensuring that the data is safe from unauthorized access or tampering.

Overall, using blockchain technology for eKYC can provide a secure and efficient platform for verifying user identity, with a reduced risk of fraud and increased transparency.

VI. INTER PLANETARY FILE SYSTEM

IPFS stands for InterPlanetary File System. It is a distributed file system that aims to create a permanent and decentralized method of storing and sharing files. In traditional client-server models, files are stored on a central server, and clients can access them by requesting the data from the server. In contrast, IPFS uses a peer-to-peer network to store and share files, with each node in the network contributing storage and bandwidth resources.

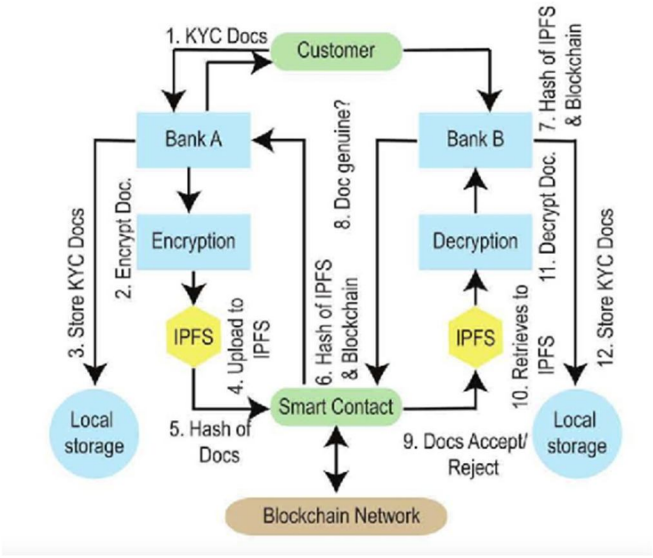


Figure 4 - EKYC system interaction with IPFS[13]

IPFS uses content-addressed storage, which means that files are identified by their content rather than their location. When a file is added to IPFS, it is broken into small pieces and each piece is given a unique hash based on its content. These hashes are used to address the files and ensure that they are distributed and replicated throughout the network.

A. IPFS has Several Benefits, Including

1) *Decentralization:* Files are stored and distributed across the network, making it difficult for any one party to control access to the data.
2) *Permanent Storage:* Files stored on IPFS are designed to be permanent, and can be accessed even if the original uploader goes offline.
3) *Efficient Distribution:* Because files are distributed across the network, they can be downloaded faster and more efficiently than from a single server.
4) *Versioning:* Because files are identified by their content, it is possible to track different versions of the same file, even if they have different names or are stored in different locations.

IPFS is often used as a complementary technology to blockchain, as it provides a decentralized and permanent method of storing data that can be accessed by smart contracts.

IPFS can be used in an eKYC system to securely store and manage user data. In this architecture, user data is encrypted, and its hash is stored on the blockchain. The encrypted user data is then stored on IPFS, and the user is provided with a unique key that is used to access their data.

When a user wants to undergo eKYC, they would submit their data to the system, and a hash of their data would be stored on the blockchain. The system would then encrypt the user's data and store it on IPFS, along with the user's unique key. The user's key would then be provided to the user, who can use it to access their data whenever they need to.

B. This Approach has Several Benefits, Including

1) *Security:* User data is encrypted, and only the user has the key to access it, making it more secure.
2) *Decentralization:* The use of IPFS ensures that user data is stored on a decentralized network, making it more resilient to attacks and ensuring that it is available even if one or more nodes in the network go offline.

3) *Efficiency:* Storing data on IPFS reduces the load on the blockchain, allowing for faster and more efficient processing of eKYC requests.

Overall, using IPFS in an eKYC system can improve security, decentralization, and efficiency, making it a promising approach for implementing secure and scalable eKYC systems.

VII. USER INTERFACE

TypeScript is a superset of JavaScript that adds optional static typing and other features to JavaScript. It is used for developing smart contracts and the front-end of the eKYC system.

For smart contract development, TypeScript is used to write smart contract code using the Solidity compiler, which generates Ethereum Virtual Machine (EVM) bytecode. TypeScript offers a number of benefits over Solidity, such as static type checking and improved error handling, making smart contract development easier and more robust.

For the front-end of an eKYC system, TypeScript is used with web framework like React to build the user interface. TypeScript improves the reliability and maintainability of the front-end code, especially for large codebases. It also helps to reduce the likelihood of bugs and make it easier to refactor code in the future. Additionally, TypeScript helps to integrate front-end code with smart contracts, making it easier to interact with the blockchain and smart contracts in a type-safe and reliable way.

ReactJS is a popular JavaScript library that is used to build single-page applications (SPAs) with dynamic user interfaces. React components can be used to create reusable UI elements, and the React ecosystem provides numerous libraries and tools to help with state management, routing, and other common tasks in web development.

ReactJS was used to build the front-end components that interact with the blockchain and IPFS network. For example, React components can be used to display the user's personal information and document uploads, and to interact with the smart contract to initiate the KYC process. React can also be used to display the results of the KYC process and any relevant notifications or alerts.

React communicates with the backend of the eKYC system using REST APIs(Application Programming Interface) or websockets. The backend can be built using a variety of technologies such as Node.js, Python, or Ruby on Rails,(Node.js in this case) and can interact with the blockchain and IPFS network using appropriate libraries and protocols.

Node.js is used to develop the back-end of the eKYC system using blockchain. It is used to write smart contracts using Solidity and interact with the blockchain network. Node.js can also be used to develop APIs that allow the front-end (e.g. a React.js application) to communicate with the back-end and access data on the blockchain. Additionally, Node.js is used to integrate the IPFS system into the eKYC system and store customer data on a decentralized network.

Overall, ReactJS along with NodeJS and Typescript provides a flexible and scalable solution for building the user interface of the eKYC system.

VIII. ANALYSIS

Key differences between existing KYC procedures and blockchain-based KYC platforms/procedures:

1) *Centralization vs Decentralization:* Existing KYC procedures are typically centralized, and depend on a singular central institution to guarantee safety of customer data as well as access to it when required. This creates a central point of failure scenario which is solved with the decentralized nature of blockchain thus eliminating the central point of failure and giving safety and immutability of customer data.
2) *Privacy:* Blockchain-based KYC platforms can offer greater privacy by directly giving the control of KYC data to customers, customers can share their data with trusted institutions as per requirement without unilaterally giving data control to one single institution and hoping that the institution follows correct procedures and ethical guidelines while handling customer data.
3) *Efficiency:* Blockchain-based KYC platforms are more efficient than current KYC procedures as the entire procedure is digital and requires no paper work to be carried out manually. Also the redundancy associated with carrying out multiple KYC checks with multiple institutions is eliminated by having a decentralized KYC data store which can then be easily used for supplying customer details as and when and as many times as per requirement.
4) *Transparency:* Blockchain-based KYC platforms are more transparent than a central institution performing KYC checks as unlike an institution which doesn't disclose their activities with customer data, using blockchain a customer is able to exactly track where their KYC details are being submitted as well who are the entities which have requested the aforementioned KYC data.

Overall, blockchain-based KYC platforms offer several advantages over existing KYC procedures, including greater security, privacy, efficiency, and transparency. However, adoption of blockchain-based KYC platforms may be slower due to regulatory concerns and the need for industry-wide collaboration.

IX. POSSIBLE VULNERABILITIES

1) *Centralized Points of Failure:* While blockchain based systems have a decentralized architecture yet they rely on a central authority to verify and initiate institutes like banks into the system, this creates a central point of failure and may put entire system at risk if this central authority fails.
2) *Scalability:* Blockchain based ekyc systems experience issues with scalability due to the large volumes of data being being stored and processed using it, this can lead to increased processing times and costs.
3) *Identify-theft:* Although the overall system is protected by the immutable nature of blockchain, however individual systems on the customer end can still be compromised and their credentials be stolen. This can be lead to a negative impact on the reliability and trust on such ekyc systems.
4) *Regulatory Compliance:* Blockchain-based ekyc systems must comply with existing regulations, such as KYC and AML (Anti-Money Laundering) regulations. Failure to comply with these regulations could result in legal and financial consequences. Such compliance's can slow down adoption of blockchain based ekyc systems by the financial sector.

X. CONCLUSION

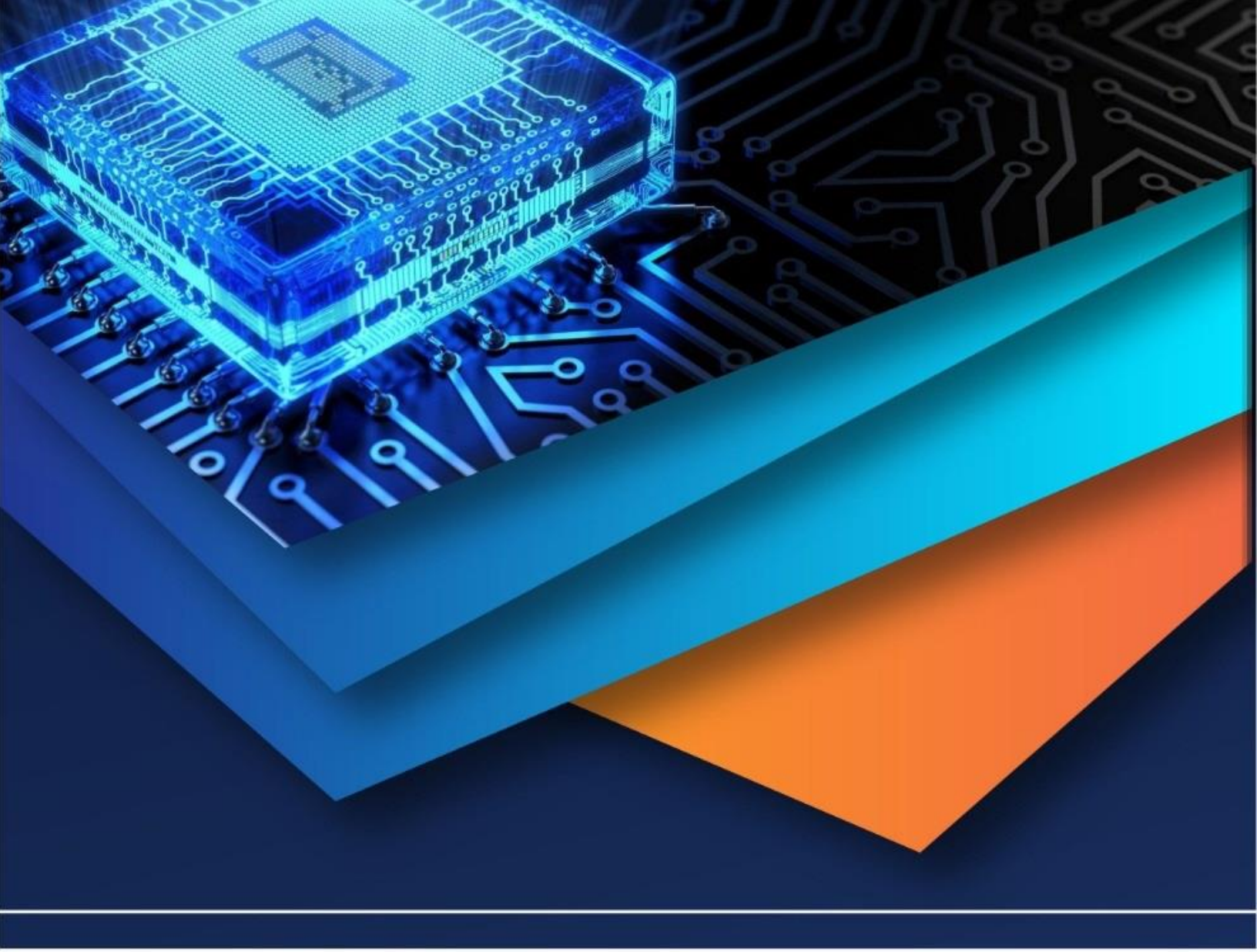
In summary, the e-KYC system leveraging blockchain technology presents multiple advantages over traditional KYC methods. The immutable nature of distributed ledger technology enables the establishment of a tamper-proof system that offers increased efficiency, reduced costs, enhanced customer experience, and end-to-end transparency when integrating customer documents into the bank's database. By maintaining a common secure database within a blockchain, the proposed system eliminates the need for redundant KYC checks by banks.

The proof-of-reputation concept enhances the verification process's robustness, ensuring that the data is reliable and trustworthy. The use of smart contracts in e-KYC systems, whether on Ethereum or Hyperledger, provides privacy, anonymity, and security among peers while preserving the customer's identity. This project's results show that blockchain-based e-KYC systems hold promise as a solution for the current limitations of traditional KYC methods, and financial institutions can adopt them to provide a more secure and efficient customer verification process.

REFERENCES

[1] Thales Group. 2022. Know Your Customer in banking. [online] Available at:https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/issuance/id-verification/know-your-customer [Accessed 11 October 2022].
[2] Appinventiv. 2022. Blockchain: The Solution to Inefficient KYC Process. [online] Available at: https://appinventiv.com/blog/use-blockchain-technology-for-kyc/ [Accessed 11 October 2022].
[3] SignDesk. 2022. Blockchain KYC - The Future of KYC Verification | SignDesk. [online] Available at: https://signdesk.com/in/ekyc/blockchain-kyc-future-of-kyc-verification [Accessed 11 October 2022].
[4] Aydar M, Ayvaz S (2019) Towards a Blockchain based digital identity verification, record attestation and record sharing system. arXiv Prepr arXiv190609791
[5] Biryukov A, Khovratovich D, Tikhomirov S (2018) Privacy-preserving KYC on Ethereum. In: Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies. pp 1–8
[6] Parra Moyano, J., & Ross, O. (2017). KYC Optimization Using Distributed Ledger Technology. Business and Information Systems Engineering, 59, 411–423.
[7] Mainelli, M., & Smith, M. (2015). Sharing ledgers for sharing economies: An exploration of mutual distributed ledgers (aka blockchain technology). Journal of Financial Perspectives, 3, 127–135.
[8] Patel D, Suslade H, Rane J, et al (2021) KYC As a Service (KASE) - A Blockchain Approach. In: Advances in Machine Learning and Computational Intelligence. Springer Dragan CC, Manulis M (2020) KYChain: User-controlled KYC data sharing and certification. In: Proceedings of the ACM Symposium on Applied Computing. pp 301– 307
[9] Sundareswaran N, Sasirekha S, Paul IJL, et al (2020) Optimised KYC Blockchain System. In: 2020 International Conference on Innovative Trends in Information Technology (ICITIIT). IEEE, pp 1-6
[10] Steichen M, Fiz B, Norvill R, et al (2018) Blockchain-Based, Decentralized Access Control for IPFS. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). pp 1499–1506
[11] Singhal N, Sharma MK, Samant S (2020) Smart KYC Using Blockchain and IPFS. In: Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies. Springer Singapore, pp 77—84
[12] Kumar, M., & Nikhil, A. P. (2020). A blockchain based approach for an efficient secure KYC process with data sovereignty. International Journal of Scientific and Technology Research, 9, 3403–3407.

[13] Allemann S (2019) Design and Prototypical Implementation of an Open Source and Smart Contract-based Know Your Customer (KYC) Platform. Dissertation, University of Zurich
[14] Niya SR, Allemann S, Gabay A, Stiller B (2019) TradeMap: A FINMA-compliant Anonymous Management of an End-2-end Trading Market Place. In: 15th International Conference on Network and Service Management, CNSM 2019. pp 1—5
[15] Zhao Z, Liu Y (2019) A Blockchain based Identity Management System Considering Reputation. In: 2019 2nd International Conference on Information Systems and Computer Aided Education, ICISCAE 2019. pp 32–36
[16] Parra-Moyano, J., Thoroddsen, T., & Ross, O. (2019). Optimized and Dynamic KYC System Based on Blockchain Technology. International Journal of Blockchains and Cryptocurrencies, 1, 85–106.
[17] Rajyashree, U. A., Doulani, S., & Pareek, S. (2019). Block Chain Enabled E-Kyc System. International Research Journal of Computer Science (IRJCS), 6, 137–143



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY