

# Kyc through Blockchain

Prince Mohobia, Dr. P.M. Chaudhari, Harsh Sakhare,  
Najim Sheikh, Ramin Singh, Devanshu Bhajbhuj

Dept. of Computer Science and Engineering, Priyadarshini College of Engineering, Nagpur

**Abstract-** Know Your Customer (KYC) process plays a critical role in helping every bank verify the identity of its customers. Banks must conduct KYC checks to prevent criminals using them to commit crimes such as drug trafficking and terrorism. Current manual KYC processes are insecure, slow, and outdated. E-KYC allows users to quickly complete the recruitment process without leaving their homes. Using blockchain-based KYC verification, these limitations can be eliminated as blockchain provides features such as decentralization, transferability, and security. Governments around the world are using electronic KYC systems to make this task easier and more transparent. Governments around the world are rapidly implementing electronic KYC systems to expedite and improve transparency in this critical activity. This document provides access to unique trust based on a self-governing model that enhances customer privacy, has regulatory authority, and helps banks improve the reliability and accuracy of customer data. Presents a management system. Reduce customer acquisition costs. This article aims to offer a solution to this problem. Our solution uses blockchain to perform one-time KYC verification and eliminate multiple checks to ensure database security. Financial institutions on the blockchain network can access a user's KYC information only with the user's permission.

**Index Terms-** Blockchain, KYC Verification, Ethereum Chain, Banks, Customer

## I. INTRODUCTION

KYC (Know Your Customer) process is a vital component in a bank's arsenal, dedicated to the critical role of certifying the identities of its clients. This procedure is critical in combating criminal activities such as drug trafficking and terrorism, since it ensures that financial institutions remain watchful gatekeepers in the fight against illegal operations. However, traditional manual KYC methods have been plagued by issues of vulnerability, sluggishness, and obsolescence, rendering them inappropriate for modern-day challenges.

The advent of Electronic KYC (E-KYC) represents a promising avenue for addressing these shortcomings, offering customers the convenience of remotely completing the on boarding process without the need to visit a physical branch. A noteworthy advancement in this realm is the integration of blockchain technology into KYC verification. Blockchain's inherent features, including decentralization, transferability, and robust security measures, offer the potential to eliminate these limitations, marking a significant stride toward enhancing the KYC process.

Blockchain platform to implement Blockchain based KYC verification system. Ethereum was developed in 2013 by Vitalik Buterin. Ethereum is a first Blockchain which has introduced concept of smart contract with which distributed

apps can be created on top of the Blockchain. Ethereum could be used to develop different applications on top of it and is not limited as just payment alternative. Our proposed system not only solves the problem of doing KYC but can also provide assistance to verify attested documents as required by other non-banking organizations.

## II. METHODOLOGY

### 1. User Consent Mechanism

The user must provide a username which will be used to create an identity where all information about the user will be stored under the username. A key pair consisting of a private key and a public key will be created to support adding or modifying and identifying users on the blockchain based on their usernames.

### 2. User Training and Support: Currently

We have built this registry over a local test-net that we hosted our personal laptops. So, there are a few limitations regarding scalability, such as the maximum number of banks that can be registered, which is currently capped at 10 and so on. Going ahead, we plan to deploy this registry over the Ethereum network to increase its scalability.

### 3. Integration with Financial Institutions

Running an Ethereum node means running software on a computer while connected to the internet. Performing

tasks on the Ethereum network frequently necessitates the use of Ethereum's embedded computer, known as the Ethereum Virtual Machine. Ethereum's native cryptocurrency called Ethereum (ETH) is used to pay for this computation, which is not free. To use the network, it's necessary to have a small amount of Ether. Ether is entirely digital, making it possible to send it to anyone anywhere in the world instantly. The supply of ether is not subject to any government or company's control; it is decentralized and transparent. Ether is distributed in accordance with the protocol exclusively to stakers who are responsible for network security. The ability to coordinate, make agreements, or transfer digital assets directly with other people is provided by Ethereum. It's not necessary to rely on intermediaries. The control of Ethereum is not held by any government or company. Ethereum's decentralization prevents any government or company from controlling it. It's a difficult task to stop you from receiving payments or using services because of Ethereum's decentralization. In a white paper, Vitalik Buterin introduced Ethereum as a method to create decentralized applications in late 2013.

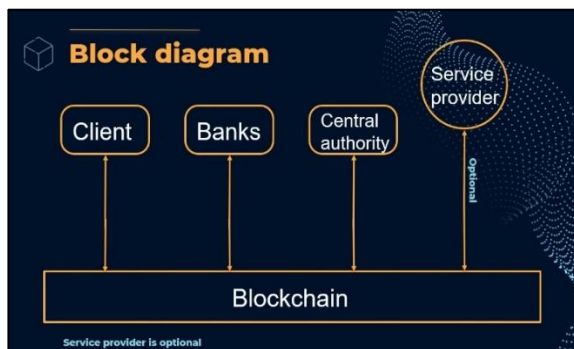


Fig.1 Block Diagram

**4. Security Measures**

Implement robust security measures to protect KYC data from unauthorized access or tampering. Use encryption, multi-factor authentication, and secure key management.

**5. .Audit Trail and Compliance Reporting**

Develop an audit trail that logs all KYC-related activities on the blockchain. This provides transparency and helps in compliance reporting. Generate compliance reports that demonstrate adherence to regulatory requirements.

**6. Testing and Quality Assurance**

Thoroughly test the blockchain-based KYC system for functionality, security, and performance.

**7. User Support**

Provide training and support for both customers and authorized institutions to use the KYC blockchain system effectively.

**8. Evaluation and Feedback**

Evaluate the effectiveness and efficiency of your blockchain-

based KYC system on a regular basis. Collect feedback from users and stakeholders to make improvements.

**9. Project Scope Definition**

Define the specific goals and objectives of your KYC project. Determine what you aim to achieve through the implementation of blockchain technology in the KYC process.

**10. Regulatory Compliance Assessment**

Understand the legal and regulatory requirements related to KYC in your jurisdiction or industry. Ensure that your blockchain-based KYC solution complies with these regulations.

**11. Technology Stack Selection**

Choose the appropriate blockchain platform (e.g., Ethereum, Hyperledger, Corda) and associated technologies for your KYC system. Consider factors like security, scalability, and smart contract capabilities.

**III. RESULT**

The benefits of the proposed system include Better governance of data as Data alterations can be tracked and monitored, direct access to the KYC data saving huge amount of time and lastly storage space is effectively utilized as inspite of saving the complete file on Blockchain, only hash is stored over it.

**Reduced Fraud and Identity Theft**

Using blockchain for KYC verification improves identity verification while decreasing the risk of fraudulent activities like identity theft and document forgery.

**Streamlined Onboarding**

Blockchain automates document verification and reduces the need for repetitive paperwork, simplifying the customer onboarding process. Customers benefit from faster and more efficient account creation.

**Compliance with Regulations**

Blockchain-based KYC systems can be designed to automatically check for AML (Anti-Money Laundering) and CTF (Counter-Terrorism Financing) compliance, lowering the risk of regulatory violations.

**Transparency and auditability**

Because blockchain is decentralized and transparent, it allows for real-time monitoring and auditing of KYC activities. This can help organizations demonstrate compliance to regulators and improve accountability.

**Cost Savings**

Blockchain-based KYC systems can result in cost savings for financial institutions over time. Organizations can reduce

operational costs by reducing manual processes and the need for intermediaries.

**Customer Empowerment**

Customers gain more control over their personal data and can choose who has access to it. This gives them the ability to participate in the KYC process and increases trust in the system.

**Interoperability**

Blockchain-based KYC systems can facilitate data sharing and interoperability between different organizations, such as banks and government agencies, streamlining the verification process. While initial implementations may begin on private or local blockchain networks, the architecture can be designed to allow for an easy transition to public blockchains such as Ethereum, allowing for increased scalability and broader adoption.

**Global Accessibility**

Blockchain-based KYC solutions can be accessed from anywhere in the world via an internet connection, making the process accessible to users across borders. Reduced Paperwork: By reducing paperwork and manual data entry, the KYC process becomes eco-friendlier and more efficient.

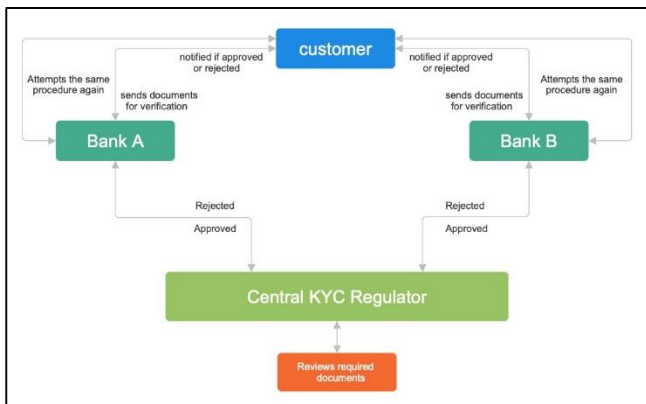


Fig.2 Standard KYC Process

**IV. RELATED WORK**

Bharti Pralhad Rankhambe proposed a method based on distributed ledger technology that can significantly reduce the overall KYC (Know Your Customer) expenses for banks while working with a regulatory authority. This system can eliminate redundant tasks performed by different financial institutions, which enhances effectiveness, transparency and reduces costs. By integrating customer records into the bank database, the proposed system removes the need for middlemen, thereby increasing customer satisfaction. Furthermore, this approach optimizes data storing, updating, sharing, and accessing processes, enhances security, transparency, and privacy, and ensures that all customer records are easily accessible. It does

this by utilizing the DLT, The proposed approach to blockchain technology involves cryptography and a consensus mechanism. This approach enhances customer ownership and improves the customer experience. In a consortium network, each institution acting as a peer can only verify the details and not modify them. Furthermore, although internal operations within each business are dispersed, they appear as one cohesive unit from an external perspective.

The consortium blockchain approach proposed by Ashok Kumar Yadav allows any firm to request data by submitting a service proof of identity. Each organization is assigned an identity to maintain record-keeping. By saving the data online on the blockchain, we can eliminate maintenance costs associated with duplicate information and significantly reduce paperwork.

E. Sai Vikas Reddy proposed an approach based on blockchain technology that lowers the expense of the standard KYC verification process. Irrespective of the number of institutions a customer registers with, the verification procedure is conducted only once for each customer, enhancing transparency by securely communicating the outcomes via DLT. In this scenario, the customer solely registers with one financial institution, thereby reducing the need to register with different financial institutions and eliminating the duplication of effort. With this approach, ethereum is used for proof of concept (POC). This approach improves customer satisfaction, boosts transparency, and lowers overhead costs.

Syed Azhar Hussain and other researchers proposed a self-governed, distributed approach called Know-Your-Consumer (DKYC). This approach enhances customer privacy by requiring prior permission. It also helps regulators oversee the process and allows banks to use reliable and valid customer details. Additionally, it lowers the cost of customer acquisition. The scoring system is constructed via the Proof of Importance consensus algorithm. This enables current conventional identity establishments, such as Civilian Identities, Regulators, National Security Numbers, and other private sector identity stores, to participate and be member of the network to determine the scoring. Prof. A. L. Maind proposed a blockchain-based approach which eliminates middlemen and enables one-time KYC for users. Users have access to the data at any time, from any location, for a variety of purposes. Blockchain technology is secure because it is decentralized, transparent, and doesn't involve third parties. It also processes transactions faster. In the paper "KYC Verification Using Blockchain" by Sunitha N.V., P. Ashwini, Sandhya, Shriraksha Bhat, and Tushara Sasi, a new e-KYC scheme called e-KYC Trust Block is introduced. This scheme uses blockchain technology and the ciphertext policy attribute-based encryption (CP-ABE) method, along with client consent enforcement, to ensure trust, security, and privacy compliance. We also use attribute-based encryption to protect sensitive transactions

stored in the blockchain and allow for fine-grained access. Our experiments show that our system is efficient and scalable in practice.

In this paper, Jose Parra Moyano, Omri Ross, and Ioan Buciu propose a new system to improve the Know Your Customer (KYC) process. The current KYC process is outdated and costs banks up to USD 500 million each year. The authors suggest using Distributed Ledger Technology (DLT) to decrease costs and enhance the customer experience. In the proposed system, the core KYC verification process is only done once, regardless of how many financial institutions the customer plans to work with. Customers can securely share their verification results with any institution through DLT. This system improves efficiency, reduces costs, increases transparency, and enhances the customer experience.

The title of the first paper is "Enabling Trust and Privacy-Preserving e-KYC System using Blockchain" by Somchart Fugkeaw. The paper discusses how banks use electronic know your customer (eKYC) systems on the cloud to verify customer identity data. The security and privacy of e-KYC documents stored in the cloud are important. Existing e-KYC platforms use strong authentication and traditional encryption, but this approach has encryption dependency and communication and key management overheads.

The title of the second paper is "Putting smart contracts into action for Know Your Customer (KYC) in a decentralized architecture that prioritizes privacy" by Nikolaos Kapsoulis. The paper discusses how enterprise blockchain solutions can protect user privacy in the context of Know Your Customer (KYC). The proposed solution involves using a decentralized schema with two types of smart contracts. Users register and upload their KYC information in a public KYC smart contract using exploited IPFS storage. Actions are recorded as blockchain transactions on the permissioned blockchain of Alastria Network. An admin user can approve or reject the validity and expiration date of the user's KYC documents through the public KYC smart contract.

David Chaum, a cryptographer, suggested a protocol like blockchain in his 1982 dissertation called "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups."

In 2008, Satoshi Nakamoto came up with the idea for the first decentralized blockchain. Nakamoto made improvements to the design by using a method like Hash cash to timestamp blocks. This method didn't need a trusted party to sign the blocks. Nakamoto also added a difficulty parameter to keep the rate of adding blocks stable. The design was then put into action by Nakamoto in the following year. It became a key part of the cryptocurrency bitcoin. The blockchain serves as the public ledger for all transactions on the network.

Satoshi Nakamoto created the first decentralized blockchain in 2008. Nakamoto improved the design by using a Hashcash-like method to timestamp blocks without needing a trusted party's signature. Nakamoto also introduced a difficulty parameter to control how quickly blocks are added to the chain. The following year, Nakamoto implemented the design as a core part of the cryptocurrency bitcoin. The blockchain serves as the public ledger for all transactions on the network. Satoshi Nakamoto used the words "block" and "chain" separately in his original paper. However, by 2016, these words were combined into the single word "blockchain" and became popular.

Ethereum is a blockchain that is decentralized and has smart contract functionality. The platform's native cryptocurrency is called Ether. Ether is the second largest cryptocurrency after bitcoin in terms of market capitalization. The software is open source.

## V. CONCLUSION

This paper suggests using blockchain for KYC verification as a way to cut costs and streamline the process. The system verifies your identity once, and banks can access it through the blockchain network. By maintaining a secure database on the blockchain, information will be more secure and tamper-proof. From the research data, we found that this program is the best compared to other programs because it solves the problem of removing KYC information. The blockchain architecture integrates data from various providers into a protected database, removing the need for third-party authentication. It makes it possible to create a system where users only need to go through the KYC process once to verify themselves. The technology allows financial institutions to use an honest ledger to verify customers' KYC processes, eliminating the need for reverse verification. It makes it possible to create a system where users only need to go through the KYC process once to verify themselves. The technology allows financial institutions to use an honest ledger to verify customers' KYC processes, eliminating the need for reverse verification.

## REFERENCES

1. What is KYC: how to do KYC online: different types of KYC: Paisabazaar. [www.paisabazaar.com/Aadhar-card/what-is-kyc/](http://www.paisabazaar.com/Aadhar-card/what-is-kyc/). retrieved on June 4, 2022
2. Electronic know-your-customer (e-KYC) exposure draft—Bank Negara Malaysia
3. Jarra-Moyano, T Thoroddsen, and O Ross (2018) KYC system that is optimized and dynamic, based on blockchain technology. 3248913 is available at SSRN.
4. Hanbar, H., Shukla, V., Vyjayanthi, C., and Modi, C. (2019) Smart contracts and distributed ledger technology are being used to optimize Kyc.

5. A systematic literature review of blockchain-based e-KYC systems<sup>1</sup>: This article, published in 2023, provides a comprehensive analysis of the existing researches at the intersection of e-KYC and blockchain. It also identifies the limitations and future directions of this domain.
6. How Blockchain Can Automate KYC: Systematic Review<sup>2</sup>: This article, published in 2021, conducts a PRISMA guided systematic review on the blockchain technology for KYC and its application areas from 2014 onwards. It also presents the blockchain platforms such as Ethereum and Hyperledger along with related case studies.
7. What is KYC and How Can KYC on Blockchain Help? This 2022 article explains the concept of KYC and how blockchain can be used to perform KYC with a single click. It also includes a flow diagram that shows how this can be used.
8. Blockchain and KYC: This 2018 article introduces the concept of blockchain and KYC and how they can be combined to improve the efficiency, security, and customer experience of the KYC process. It also discusses the key issues and benefits of using blockchain for KYC.
9. Bangladesh Financial Intelligence Unit: electronic know your customer (e-KYC) guidelines. <https://www.bb.org.bd/mediaroom/circulars/aml/jan082020bfu25.pdf>. Date accessed: October 13, 2021