Centralized KYC-Secure Platform

Shantanu Gonaka
Comp. Engg, VCET
shantanugonaka@gmail.com

Shradha S. Sankhe
Comp. Engg, VCET
shradhasankhe62@gmail.com

Suyash P. Satam
Comp. Engg, VCET
spsatamar102@gmail.com

Abstract- The KYC chain in the financial industry is crucial and necessitates stringent compliance as well as expensive manual labor. According to estimates, the global cost of KYC procedures has increased to $1.5 billion. Evaluating data and keeping tight tabs on them takes very little time and effort takes very little time and effort to evaluate data and keep tight tabs on them. Each financial service provider develops their own set of requirements for KYC documents under the present centralized approach. Users must comply with KYC standards with each institution and service provider they utilize as a result. Even if user information needs to be changed down the road, all financial institutions and service providers must be informed separately. Create a central KYC database that would be available to everyone.

Keywords— CNN (Convolutional Neural Network), SVM (Support Vector Machine), BERT, LSTM (long short-term memory networks), RNN (Recurrent Neural Network), ANN (Artificial Neural Network), DCNN (Deep Convolution Neural Network, MAML (Model-Agnostic Meta-Learning), GRU (Gated Recurrent Unit), BILSTM (Bidirectional Long Short-Term Memory)

I. INTRODUCTION

The KYC process, if done adequately, helps in uncovering any acts of mischief or crime in the past and accordingly disallow such individuals from entering the banking system. intensively. In that case KYC must be privatized with widespread user input. This article discusses how blockchain can be used to remove manual repetitive work, improve transparency, and reduce costs for financial institutions by leveraging technologies such as Artificial Intelligence (AI) and blockchain. It is important to understand the problem areas of the present system, such as peer-to-peer intensively, dynamic user input, and trust between participants. The paper outlines a proposed model for KYC, which involves storing participants' information in the blockchain network and assigning CQs based on the risk factors assessment result. It also compares the result and compares it with other methods of OTP, and presents future work.

Blockchain has many use cases, such as peer-to-peer payments, trade settlements and supply chain tracking, that require trust between participants. KYC can be gained by storing participants' information in the blockchain network, but this is challenging due to constraints like Privacy, Confidentiality, Security. Hyperledger Fabric is the framework used to address these challenges.

Due to the problems with lower customer satisfaction and rising KYC process costs that are existing in the banking industry, We suggest a Blockchain-based system.

II. RELATED WORK

The reviews of recent papers published Centralized KYC-Secure Platform have been put through in this section.

KYC is a mechanism by which banks know about the identity and address of their customers in order to prevent illegal acts. R. Biradar [1] worked Risk management involves onboarding new customers and surveillance of transactions, which can be expensive and expose financial institutions to fines.

Alternatively, Ting-Hsuan Chen [2] developed Thomson Reuters survey found 89% have never had a smooth hassle-free KYC process experience, with 13% changing their association with a particular institution for this reason.

Prince Sinha Ayush Kaul [4] Proposed by Decentralized KYC System IPFS, Blockchain, Ethereum, Smart Contracts, JavaScript are used in Decentralized KYC system, requiring additional Authentication requires additional and authorization to access data.

Somchat Fugkeaw [5] experimented Enabling Trust and Privacy-Preserving e-KYC System Using Blockchain using Scheme delivered security, e-KYC process with the user's consent enforcement feature, Data updated by owner or customer.

P. Mondal R.,Deb M.N.Huda [6] , proposed by Know Your Customer published a paper about Dynamic KYC based MFA authentication provides control equal to existing MFA/2FA, no chance to HASH change & man-in-the-middle (MITM) attack, and CQ Based on Risk Level, Perform and Commit Transaction, Risk Factor Calculated. Section II overviews the related work, Section III introduces the proposed model, Section IV discusses the result, and Section V concludes with fruitful remarks.

Denson George Anand Wani Ashutosh Bhatia [9] worked on Customer Identification Procedures, Customer Identification Procedures, Customer Acceptance Policy, Risk Management, Monitoring of Transactions are used to simulate a scenario where a bank may not trust other banks in the network.

Vincent Schlatt Johannes Sedlmeir Simon Feulner Nils Urbach [10] proposed by Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity.using dataset by DLT also has considerable drawbacks concerning scalability and privacy, owing to the redundant operation of all transactions the SSI experts may translate to many other areas.where the fear of a centralized service provider has so far prevented a more efficient cross organizational identity management.

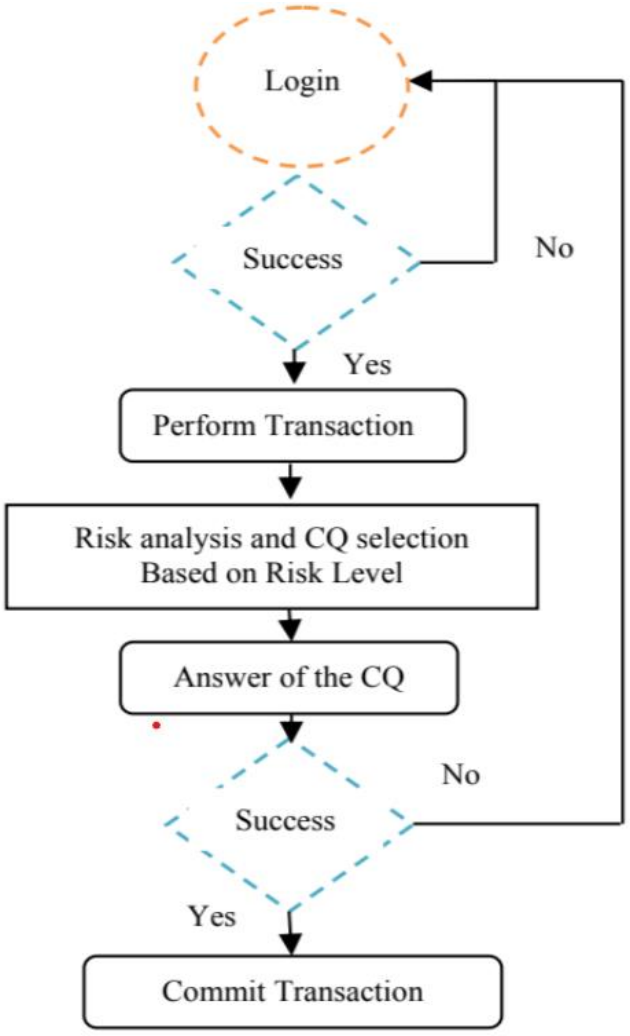
Mohammad Abu Yousuf Abdullah Al Mamun [11] proposed Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology. the IPFS installation has a lot of hassles, it is not at all user friendly. IPFS consumes a lot of bandwidth which is not appreciated by metered internet users.

Pavlo Tertychnyi Mariia Godgildieva Marlon Dumas Madis Ollikainen[12] worked on a Time-aware and interpretable predictive monitoring system for Anti-Money. This ML-based monitoring system for AML needs to provide accurate (calibrated) estimates of the probability that a given customer engages in illicit behaviour,To generate not-redundant and timely alerts.this Contains High Risk.

III. PROBLEM STATEMENT

KYC requirements Consumers must repeat the process and supply identical data to each financial institution in order to comply with KYC regulations. Provide a central KYC database that is accessible to all financial institutions using a safe platform using high encryption and biometric authentication. Customer data sharing should require user consent. This platform ought to make it possible to open new accounts with financial institutions.

IV. EXPERIMENTAL STUDY



The brief idea of the model is depicted in the fig. In the figure the initial step is single factor authentication called login using user ID and password. By Analyzing transaction performers risk level we have selected Blockchain as our solution. In the final state verify the transaction performer based on the blockchain transactions. These transaction is the replacement of OTP or some other existing 2 Factor Authentication models.

Proposed Model

The KYC on blockchain would be a 3 step process: For KYC and AML requirements, customers have to repeat the same process and provide the same information to every financial institution. Develop a central database for KYC/AML that would be accessible by all financial institutions through a secure platform that has high encryption and authentication using biometrics. Sharing of customer data should be subject to user approval. Ideally, this platform should also enable new account creation with financial institutions.

1) Risk Assessment

Risk and threat in online transactions depend on various factors. The prime goal of the FI s is to permit the right user for access to financial networks and restrict all. In this context, we analyse previous activities of the user and calculate similarity between previous and present introducing multiple techniques and algorithms.

2) KYC privacy and security compliance

As the emergence of FinTech innovation and virtual banking has revolutionized the global in the financial service industry, several front-end services have shifted online. e-KYC is one such service that regulators of many countries have implemented policies that allow FIs to implement e-KYC verifications and approve customer applications. Based on the thorough review of a survey of KYC regulations done by Price Waterhouse and Coopers Technical Standard for Digital Identification Systems published by World Bank Group and the report on existing remote on-boarding solutions in the banking sector by EU commissions the security and privacy-related compliance regulated by financial institutions around the globe take customer due diligence as the core consideration and emphasize the following four common requirements for digital identification including KYC compliance. • Verification of customer identification information must be truly authenticated multiple factors and data sources. The proof of identity (POI) must be identifiable and technically and legally valid without tampering. Multiple sources of POI issued by government units and trusted ID providers are required.

Security and Privacy Requirement	Feature of Our e-KYC TrustBlock
Verification of customer identification information	Our scheme allows any form of POIs to be registered and singed by the customer. We also have a smart contract to support secure verification of the encrypted documents. The authenticity of the customers is firmly verified through their digital signature while the examination of the documents is vetted with FI's officer.
Protection of Customers' credentials or PII	All customers' credentials are protected based on AES and RSA encryption
Auditing Feature	All e-KYC transactions are recorded in the blockchain with the encrypted format
Consent	We develop two algorithms including (1) *create e-consent* and (2) *enforce e-consent* to systematically create digital consent and enable the customer to digitally sign the consent.

• Privacy of customers' credentials or PII should be protected. Encryption and digital signing based on PKI should be employed.

• Auditing features for all transactions and its lineage must be provided.

• Collecting the customers 'credentials must obtain consent from the customers.

V. WORKING

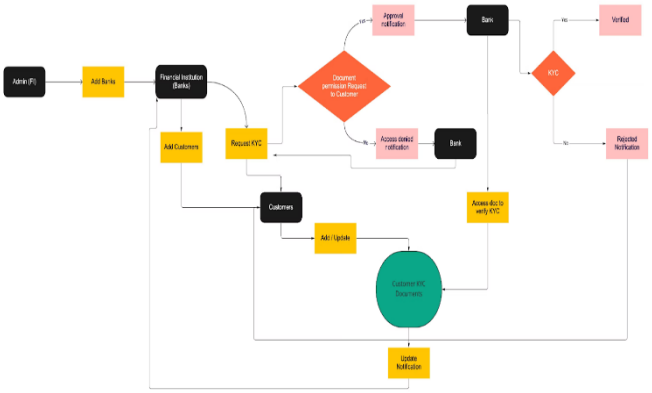
In such cases, smart contracts will be leveraged for automatically updating the system when the user provides new documents. The user submits the new document to FI1 who then broadcasts the change across the blockchain (through the new Hash Function), which then becomes accessible to other FI participants on the network.

- Admins will onboard financial Institutions on the network.
- FIs can be active or inactive based on network protocols.
- FIs can add Customers and request for KYC from customers.
- Customers can approve/reject the KYC request from FIs.
- If can approve/reject the customer's data after verifying.
- If FI rejects Customer's KYC verification, a notification will be sent to the customer with the reason.
- Customers can update the KYC documents again and the update notification gets broadcasted to all the associated FIs.
- all types of user roles must have mandatory metamask addresses on the maintain network.

The evaluation technique for a hate speech detection model can be similar to that of any classification model. Here are some common evaluation metrics and techniques used for hate speech detection models:

1. Design Details:

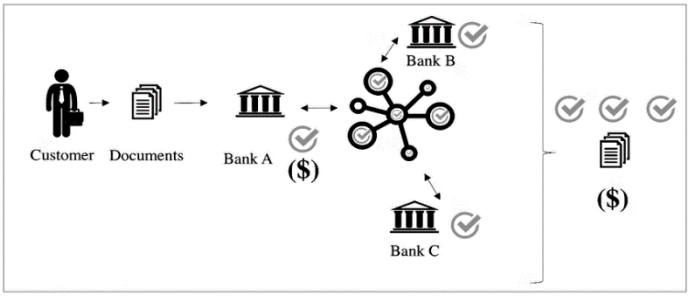
In the proposed KYC chain we have 3 key entities Admins, Financial Institutions and customers.



2. Methodology Proposed System:

KYC is a process by which banks obtain information about the identity and address of the purchasers. It's a regulator governed process of performing due diligence for verifying the identity of clients. This process helps to make sure that banks' services aren't misused. The banks are responsible for completing the KYC procedure while opening accounts. Banks also are required to periodically update their customers' KYC details.

There are various steps for building KYC on blockchain-



1) The users register themselves on the KYC chain-

Users complete profile registration as a one-time setup using their identity verification documents. Once uploaded, the data becomes accessible to, say, Financial Institution number 1 (let's call them as FI1) for verification purposes.

2) User provides access rights of his profile to FI1-

FI1 requests for access to the user profile, the user provides it. FI1 then verifies the KYC data and saves a copy of the hash-value of the uploaded data on the DLT as well as on their private servers. Now, if the KYC data is altered, the Hash Function of the KYC data under user profile will not match the one posted on the platform against FI1's, alerting the other financial institutions on the blockchain of such change.

3)User performs a transaction with FI2 (Financial Institution 2).

Later when FI2 asks the user to perform KYC, the user simply grants access to their user profile to FI2. FI2 then reviews the KYC data (and its Hash Function) with the Hash function uploaded by FI1. If the two match, FI2 would know that the KYC is the same as the one received by FI1.
In case the Hash Functions don't match, FI2 would have to manually validate KYC documents.

A chaincode typically manages business logic agreed to by participants of the network, so it is the same as the "smart contract", in a public blockchain network. State created by a chaincode is made exclusively to that chaincode and can't be accessed directly by another chaincode. However, if given the appropriate permission a chaincode may invoke another chaincode to access its state within the same network.

VI. EXPERIMENTAL SETUP

Details of our sections

- Different Roles: Admin Financial Institution(e.g RBI), Financial Institutions, & Customers Smart Contract consisting of all the rules and protocols required for KYC document flow.
- We have created 2 contacts for Banks and Customers, and inherited those contract KYC contracts. Blockchain Network to deploy the Contract.
- We have used Rinkeby for our contract. Website for user Interface where Users according to their role can access information.

- We have created a web page with React & Native Base.

VII. PERFORMANCE PARAMETERS

The Financial Institution and add their banks after adding customer requests for KYC then access the request for document permission to the customer if the permission is access approval notification to the bank the KYC is verified or rejected. also the bank access doc to verify KYC. Customer add or update their KYC documents. that updated notification will be in a financial institution.

VIII. CONCLUSION, LIMITATIONS AND FUTURE SCOPE

KYC using blockchain is successfully implemented and there are a lot of fine tunings which can be added to this project which can make the user experience much better and can also help us to save more time.

As future scope we can enhance security by using biometric security for the same which will help the customers to have an additional layer of security.

We can also make many changes in UI in order to make it more efficient which in the end will save more time.

Ideally this platform should improve security and make the KYC process more easy than the traditional methods that too by applying all the legal conditions of the government.

REFERENCES

1. FATF, GAFI. "Guidance on the risk-based approach to combating money laundering and terrorist financing," June 2007.
2. J. Moyano, O. Ross, “KYC Optimization Using Distributed Ledger Technology,” Springer Fachmedien Wiesbaden, Business & Information Systems Engineering, vol. 59, Issue 6, pp 411–423 (2017). URL:https://doi.org/10.1007/s12599-017-0512-2.
3. Security Services Using Blockchains: A State of the Art Survey: Tara Salman, Student Member, IEEE, Maede Zolanvari, Student Member, IEEE, Aiman Erbad, Member, IEEE, Raj Jain, Fellow, IEEE, and Mohammed Samaka, Member, IEEE.
4. Vitalik Buterin, “The meaning of decentralization”,February 2017, Retrieved from https://medium.com/@VitalikButerin/the-meaning- of-decentralization-a0c92b76a274
5. Dr. Prerna Mahajan, Abhishek Sachdeva, “A Study of Encryption Algorithm AES, DES and RSA for Security, Global Journals INC. ISSN: 0975-4172, 2013.
6. Ketul Shah, “All you wanted to know about KYC” ,September 2006, Retrieved from http://www.rediff.com/money/2006/sep/12guest.htm
7. Georgios Konstantopoulos, Understanding Blockchain
8. Fundamentals, Part 2: Proof of Work & Proof of Stake, Retrieved from https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb
9. Syeda Farha Shazmeen, Shyam Prasad "A practical approach for secure internet banking based on cryptography," International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012.
10. FFIEC Guidance: Authentication in an internet banking environment, federal financial institutions examination council (FFIEC), Retrieved February 4, 2006
11. W. M. Shabir, M. Steichen, J. Francois. ”Blockchain orchestration and experimentation framework: A case study of KYC”.Network Operations and Management Symposium, IEEE 2018.
12. K. Delmolino, M. Arnett, A. Kosba, A. Miller and E. Shi, ”Step by Step Towards Creating a Safe SmartContract: Lessons and Insights from a Cryptocurrency Lab”, Financial Cryptography and Data Security, pp. 79-94, 2016.