KYC using De-centralized Private Blockchain Network

[1]Onkar Naik, [2]Advait Nandeshwar, [3]Pranav Kharat, [4]Dr. Vaibhav Narawade

[1,2,3]UG Student, [4]Professor, Ramrao Adik Institute of Technology, Navi Mumbai, India,

[1]naiksonkar@gmail.com, [2]advait.nandeshwar@gmail.com, [3]pranavkharat7@gmail.com,

[4]vaibhav.narawade@rait.ac.in

Abstract. An ongoing problem in the banking industry is the KYC management system. This is a frustrating process as it involves the same process that has to be done at different customer centers thereby increasing costs. This process is also time-consuming for customers as the same process is done for each bank or bank they are wanting to work with. The personal experience of many customers reveals that this process should be simplified. In this proposed paper, we aim to do this. We are proposing a solution based on Blockchain technology, which would reduce the cost of the standard KYC authentication procedure. An important addition to this is that the entire verification procedure is performed only once per customer, regardless of the number of financial institutions they register, and thus increases visibility by sharing results securely with DLT. This approach involves proof of concept (POC) via Ethereum. This process reduces additional costs, improved customer experience, and increases visibility.

Keywords: Ethereum, KYC, Blockchain, DLT .

I. INTRODUCTION

According to the Reserve Bank of India (2016), KYC is defined as the process through which financial institutions obtain information about the address and identity of the customer.[1] In terms of regulatory procedures, financial institutions (FIs) or Banks need to get into their clients before engaging them or doing any work with them, to avoid illegal activities. Personal Identifiable Information is collected from all sources to detect illegal activities. KYC procedures are the same it is often repetitive, inconsistent, and repetitive, leading to high-level controls as well costs. The process also does include management of risk about the ride of new customers, Transaction monitoring, along with specific banking customer policies. This process is very expensive for banks and might impose heavy fines on them if they do not comply with existing rules. According to a case in the year 2016, the RBI pressed fines upon 13 banks violating the guidelines of the regulatory orders, among other things, in KYC procedures. Each customer must register with the financial institutions each time, which could be done only one time.

KYC using decentralized blockchain will provide better security, better reliability, and trust. The transparency of the whole process will be improved by enhancing the experience and efficiency for customers and FIs alike. Compliance duration would be shorter and cost-effective. There will be an improvement in managing the branches of organizations with localized data availability.[10]

Currently, third-party data providers and external verification agencies provide information and interfaces to extract the required customer information. However, banks are struggling to integrate this data to get an integrated customer perspective. This has led to an increase in the number of cases of failure of banks to comply with legal requirements, leading to large fines and refunds along with damage to their reputation. Banks need to digitize data to store it which requires expensive technology. The state of KYC is always subject to the new regulation. Therefore, KYC resources need to continue to update their guidelines. This increases the need for banks to improve their data collection systems for effective management of risks and compliance. Also, banks do not have a single, integrated KYC system for business, asset management, and trade. Adjusting many of these systems and combining different approaches puts banks under a lot of pressure and adds cost. These observations have strongly encouraged us to take up this issue operating environment.[8]

II. BLOCKCHAIN TECHNOLOGY

Distributed ledger technology, such as blockchain, has achieved notability due to the widespread usage of the cryptocurrency Bitcoin. Bitcoin was the 1st usable cryptocurrency that was not governed by a central jurisdiction. While Distributed ledger technology was at first

 DOI : 10.35291/2454-9150.2022.0126

used to bring forth a state-of-the-art way of generating money and relaying it through the Internet, the technology can also be utilized for running and governing decentralized networks through the use of smart contracts. They are computer protocols for enforcing, facilitating, or verifying predefined provisions whenever a set of circumstances are provided.

Blockchains are digital technologies that integrate cryptographically, data management, networking, and promotional methods to support the testing, execution, and recording of transactions between parties. Blockchain technology ensures the elimination of the double encryption problem, with the assistance of the public-key method of cryptography, in which each proxy is provided with a private key (retained confidential as a password) along with a public key assigned to the remaining proxies. The validity of the information stored in blockchain servers is verified by network nodes which are done using SHA known as the Secure Hash Algorithm.

Blockchain technology utilizes SHA for interpreting block content into cryptographic fingerprints called 'hash'. SHA can as well be utilized for making digitized documents distinctive 'fingerprints' so that these fingerprints won't be duplicated except if produced on the same document. It guarantees that every single one of the blockchain members can smoothly confirm the genuineness of any pre-accelerated document by speeding up and comparing the hash they are producing with the hash formerly generated using the original document. In addition, the hash will never reveal any particulars about the content of the document, similar to analysing a person's fingerprints can help a person to identify who he or she is but fail to disclose, like in some cases, the facial characteristics of targeted person. Distributed block with many nodes supports the recording of information through the network which is stored sequentially in a list of records separated by blocks and issued to all nodes in the network. The particulars in every block are further used by system protocol for creating a secure hash for identifying specific blocks. Each following block documents the preceding block hash so that each one of the blocks is tied in conjunction in sequence causing it to be difficult to alter the particulars in one block without altering all preceding blocks.

If a single node changes the particulars in its ledger and requests to communicate with the network on basis of that, thus, 'inconsistent' information, the hash would not match the ledger distributed to other nodes in the network, and the functions performed by this node. performance won't be trusted by the remaining nodes. The procedure to verify the transaction and make sure that the blocks are not replaced is done by network nodes.

2.1 KYC using Blockchain Technology

This paper solves the problem in the current KYC process based on three assumptions: Initially, a group of banks, operating in a particular country and hence constrained to follow the same KYC regulations, agree on calibers to provide basic KYC certification to the customer. Secondarily, each of the banks working with the system acknowledges the average cost to implement the core KYC verification process. These costs may depend on each client's problem, based on pre-determined variables like the magnitude of modified documents and client size. Next, the federal regulator conserves the system and authorizes banks for working with the system beneficial for conducting a well-ordered and transparent KYC verification process. [4] This is shown in Figure 1.

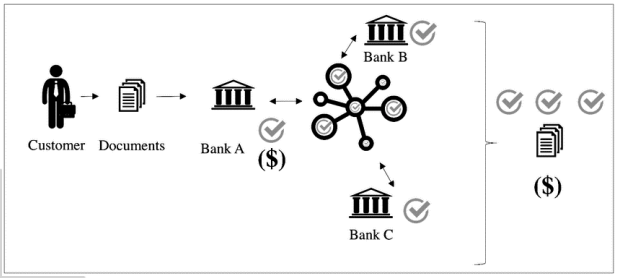

Figure 1: KYC Using Blockchain

These three perspectives are needed to ensure a fair compensation framework for all engaging banks. In addition, a set of 4 constraints are described that must be met by the product. It should make sure equitable distribution of costs of running the core KYC verification process; Must preserve the confidentiality of the KYC process; must ensure that without performing the core process no institution should charge; No institution can access another member center without paying for information. [7]

The Unemployment Status makes sure that the banks that conduct the KYC core verification procedure would not possess the motivation to choose the core behaviour of a different institution KYC validation, and vice versa. Unless a customer discloses information, the system cannot know if the customer is interacting with another financial institution. The artifact consists of two parts. The first part is an official website that guarantees the confidentiality of archived documents. The next part is a distributed book that acts as a consistent history and a cancellation plan in which the KYC process is evenly distributed among the participating institutions. The controller uses and manages the system that empowers the Database and DLT infrastructure.

The regulator plays an important role in the system by developing and maintaining the fabric layer. The smart contract includes a hash code of documents, the public key of the domestic bank, and the certification authority, proving that the customer is guaranteed, to pay a limited amount of

 DOI : 10.35291/2454-9150.2022.0126

compensation to the local financial institution. This system makes sure that the customer must be registered with the desired institution but the results can be used by other financial institutions. Suppose that if a customer wants to engage with X bank, the main KYC verification will be done only once and if the customer wants to work with another financial institution, then KYC details can be downloaded from X-X, thus reducing the time. M costs of running a single customer client KYC process shall not exceed X*M.

Figure 2 shows that the system allows the same customer to engage with 3 similar banks, but now document exchanges and the main KYC verification process occur only one time and costs are lowered to a third. This program satisfies the four constraints described earlier: equality, disrespect, privacy, and inaction. As for privacy as each bank uses only one account per customer, it is hence impossible to identify which bank is behind the public key, customer privacy, and verified banks.

As long as a single customer can engage with all the banks in the system all the institutions can conclude that it was. However, as banks use a single account per customer, their privacy will still be assured in the case of all customers. The constraint of non-completion of work is fulfilled, as it is only by paying the facility only on the list of facilities available to the nearest customer. Because the act of reimbursing other banks for the KYC authentication procedure that has been managed can only be aroused by a real customer requesting to the bank, no bank has the motivation to make fraudulent agreements that claim to have a core KYC verification process, because in that case there will be no real customer behind the institution has requested confirmation.

III. Existing System

3.1. Current KYC System

According to the Reserve Bank of India (2016) [2], KYC is defined as the process through which financial institutions obtain information about the address and identity of the customer. KYC is also known as “Know Your Customer”. It is in general a repetitive process, irregular, and replicated, leading to large administrative overheads and expenses. The process clarifies risk management for users, transactions monitoring, along with certain customer schemes for financial institutions. The process is a huge hole in the pocket of financial institutions and if done under an unregulated format might incur penalties. Figure 1 represents the current KYC process in which each customer has to register the documents multiple times thereby increasing the cost to three times what could have been performed in a single time. With this paper, we have formulated a way to reduce this cost to one-time. [6]

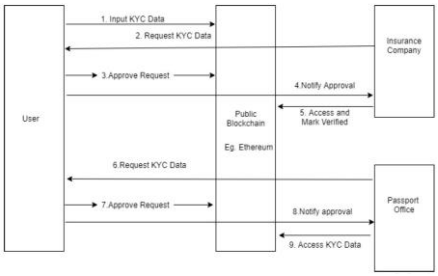

Figure 2: Existing System

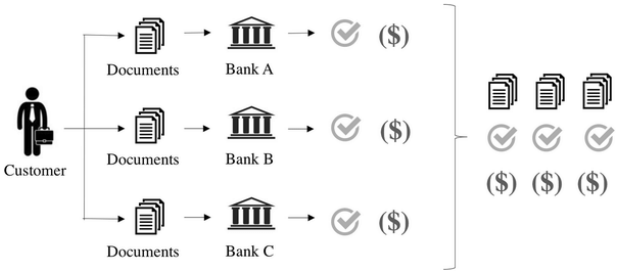

Figure 3: Current KYC System

3.2 Limitations of current KYC process: [3]

Here are some major KYC compliance challenges that banks and financial institutions are facing:

- Authenticity of verifying organization cannot be determined.
- Inter-Organizational Dependency.
- Time consuming process.
- Local database security, so easily comprisable.
- Transmitting KYC Data over network vulnerability.
- Lack of KYC Standards across organizations.
- Compliance duration is longer.

IV. Proposed Methodology

Systems verification issues such as Proportionality, Irrelevance, Privacy, and No minting should be agreed upon by the financial institutions and the national regulator. Context of KYC customer verification is done “at home bank” numerically. Customer public keys and documents are reviewed outside the distributed ledger to protect customer privacy. When the financial institution has decided on the confirmation or rejection of the customer, it retains the document which is digitally signed in the client’s smart contract, which includes the outcome of KYC’s basic verification procedure (rejected/verified) and the document hash. This would cost home bank ‘m’ rupees. Whenever customers come to a non-home financial institution for working with them, they have the authority to share their key which contains the address and public key, and the first smart contract address in which the domestic bank recorded the outcome of the basic KYC verification procedure. After going through a smart contract, the approached bank sees

 DOI : 10.35291/2454-9150.2022.0126

the number of other banks the customer has interacted with till now because it recognizes several social buttons appearing in the record of boarding stations. To add to this record, this bank must pay an average price m/n+1 rupees distributed evenly among other bank participating with the customer to perform the main KYC verification process where n represents number of banks customer currently is working with. [5] This plan makes sure that basic KYC procedure must be done only one time, by the first bank the time the customer wants to work, but the results can be used by numerous financiers' facilities as and when requested by the customer. The entire process can be summed up in Figure 2.

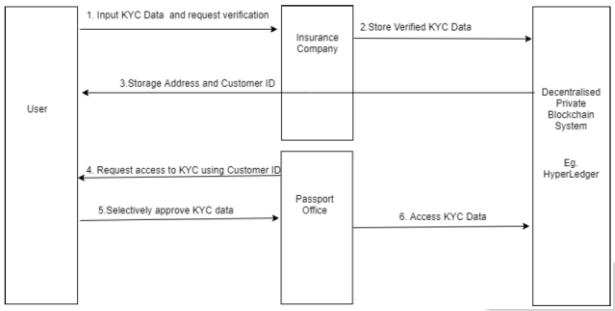

Figure 4: Proposed System

4.1. Tools

Backend is based on the Ethereum blockchain backed by Ganache, which is a personal independent blockchain for Corda distributed application development and Ethereum.[9] Ganache is to be used all over the development cycle; which allows for upgradation, reuse, and testing of the dApp in a safe and secure environment. Ganache comes with 2 options: CLI and UI. The CLI tool also called ganache-cli, which was previously called TestRPC, is there for Ethereum application development. UI is a desktop application that supports Corda technology and Ethereum.

Solidity is a high-level programming language that is contact-oriented and is used for executing smart contracts. Solidity is greatly governed by Python, JavaScript, and C++ and is designed for Ethereum Virtual Machine, also called EVM. Solidity is used to create contracts such as Nedbank, remove bank, and customer, remove customer, getBankRequests.

EVM is an environment in Ethereum for smart contracts for runtime execution. It centers on giving security and executing trustless code by computers across the globe.

4.2. Implementation Details

In the traditional KYC system, each bank will make its identity check e.g., each user is individually tested by an organization or government entity. Therefore, there is a waste of time to look at each identity from the beginning. The development of blockchain and DLT allows us to collect data from different service providers on one single stable and secure domain which doesn't require another 3rd party for the verification of information authenticity. It makes it possible to create a system where the user will only need to perform the KYC process once to verify his or her identity.

In the ledger, each firm represents a bank / financial institution and has registered users for accessing the system. Only financial institutions are capable of performing submit or assessing transactions and also for

recording new unique clients that want to keep their particulars in the system. Once a new client is registered to the system, the financial institutions that registered that client are automatically able to access the client's data and that client is not able to remove access to this institution. Clients can sanction and reject approval from other registered institutions to access their data. Considering that only financial institutions can perform transactions, to approve or remove approval clients must have organization numbers and ledger user information. This information is encrypted and stored in the database. Once the request is made, the backend decrypts that information to perform the transaction.

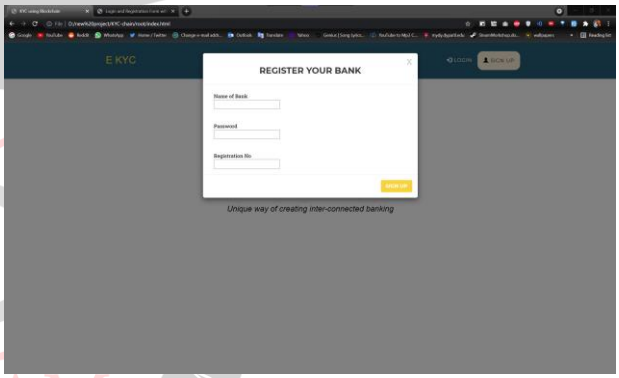

Figure 5: Registering your bank

Figure 5 shows the process of adding a bank to the network. It requires bank name, Ethereum account number and registration number for that bank.

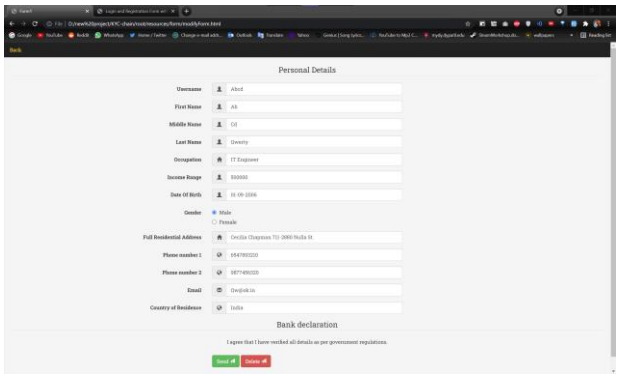

Figure 6: Customer Details Form

Figure 6 shows the process of adding a customer to the network after the user's KYC check has been done. This process would be done by the bank.

 DOI : 10.35291/2454-9150.2022.0126

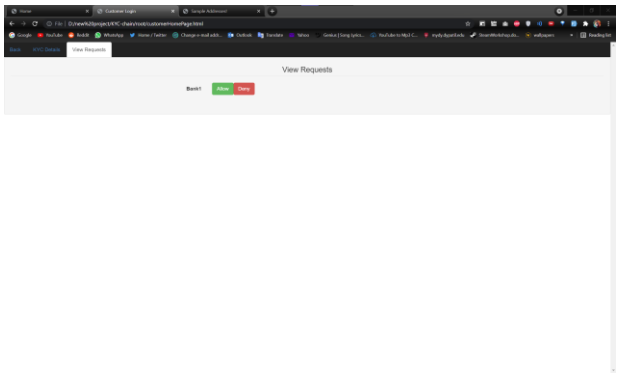

Figure 7: Pending Request

If a bank other than home bank needs KYC details of the customer, then the access to these details have to approved by the customer through customer portal. This process is shown in Figure 7.

V. Conclusion

This paper has shown how DLT (allotted ledger technology) and blockchain have co-opted the KYC system and enabled the use of blockchain clever settlement technology thereby moving towards newer technologies. In contrast to the existing solutions where customers need to perform KYC each time while interacting with a new FI or organization thereby adding the costs, the approach conveyed through this paper is simpler. The implemented system requires registered customers to sanction or reject approval to registered FIs to access their data. Due to simultaneous management of various modules such as web3, smart contract, network management, and messaging passing machine, this approach reduces the cost of integration. It further reduces the client's effort by getting everything in line and in a very secure way through customer-portal. This system provides direct communication between financial institutions and customers with no middleman. The proposed solution is also able to reduce the official regulatory price by dividing the price rather than multiplying it, providing better user enjoyment, and reliability between agencies.

VI. Future Work

– Multiple Banks Connectivity: Current system provides an interface to manually change details upon approval of the user for a single financial institution (FI).

References

[1] Optimised KYC blockchain system, https://ieeexplore.ieee.org/abstract/ document/9071533

[2] Master direction - know your customer (kyc) direction, 2016 (updated as on may 10, 2021) rbi/dbr/2015-16/18 (Feb 2016), https://www.rbi.org.in/CommonPerson/ english/scripts/notification.aspx?id=2607]

[3] How blockchain can help upgrade KYC processes (May 2021), https://www.nasdaq.com/articles/ how-blockchain-can-help-upgrade-KYC-processes-2021-05-05

[4] Kapsoulis, N., Psychas, A., Palaiokrassas, G., Marinakis, A., Litke, A., Varvarigou, T.: Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture (Feb 2020), https://www.mdpi.com/1999-5903/ 12/2/41

[5] Malhotra, D., Saini, P., Singh, A.K.: How blockchain can automate KYC: Systematic review - wireless personal communications (Aug 2021), https://link.springer. com/article/10.1007/s11277-021-08977-0

[6] Parra Moyano, J., Ross, O.: Kyc optimization using distributed ledger technology - business amp; information systems engineering (Dec 2017),

https://link.springer.com/article/10.1007/s12599-017-0504-2

[7] Shabirair, W.M., Steichen, M., Francois, J., State, R.: Blockchain orchestration and experimentation framework: A case study of KYC. NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium (2018). https://doi.org/10.1109/noms.2018.8406327

[8] Yadav, A.K., Bajpai, R.K.: Kyc optimization using blockchain smart contract technology. International Journal of Innovative Research in Applied Sciences and Engineering 4(3), 669–674 (2020). https://doi.org/10.29027/ijirase.v4.i3.2020.669-674

[9] "KYC as a Service (KASE)—A Blockchain Approach."Springerprofessional Nov 2021 https://link.springer.com/chapter/10.1007/978-981-15-5243-4_76#:~:text=The%20proposed%20system%20uses%20blockchain,spent%20on%20verifying%20the%20customers.

[10]. Government of India, National Securities Depository Limited. "Aadhaar Authentication and E-KYC Services." Aadhaar Authentication and E-KYC Services, https://www.egov-nsdl.co.in/e-kyc.html.

 DOI : 10.35291/2454-9150.2022.0126