International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Know Your Customer (KYC) Process through Blockchain

E. Sai Vikas Reddy[1], Nikhil Suhag[2], Manjunath S[3]

[1]Student, Dept. of Computer Science & Engineering, SJC Institute of Technology, Karnataka, India
[2]Student, Dept. of Computer Science & Engineering, SJC Institute of Technology, Karnataka, India
[3]Asst. Prof. Dept. of Computer Science & Engineering, SJC Institute of Technology, Karnataka, India

---

Abstract - *The sustaining problem in banking industry is KYC management process. This is monotonous process as it involves the same process to be done for different institutions for a customer thereby increasing the cost. The process is also time consuming for customers as the same process takes place for each bank or bank with which they intend to work. The personal experience of many people revealed that this process should be made simple. In this paper we are intended to do this. We propose a solution based on Blockchain technology, which reduce the traditional KYC verification process cost. The Major addition to it is that the whole verification process is conducted only once for each customer, irrespective of the number of institutions they register and thereby increasing the transparency by securely sharing the results through DLT. This approach involves proof of concept (POC) with ethereum. This process reduces cost overhead, improved customer experience and increases transparency.*

Key Words*: *Banking, Blockchain, KYC, Distributed Ledger Technology, Ethereum

1. INTRODUCTION

A bank generally serves to a large client base in both retail and corporate sector. The 'Know Your Customer' process, also known as KYC, which helps the institution to verify identity of client. KYC is a Regulatory and legal requirement that must be fulfilled by the companies or financial institutions for both new and existing clients. The major challenge faced by banking sector is increased regulatory cost of KYC process that has negative impact on business.

The aim of this paper is to propose a new approach to the KYC verification process. We introduce a system, based on DLT, that proposes a solution to the increased costs of the KYC process and the lack of customer satisfaction. The key reason for using DLT is that it allows us to observe the KYC cost structure at an aggregate level for all the financial institutions operating in a jurisdiction and to tackle the inefficiencies that emerge from the duplicated conduct of similar tasks by all participating institutions (i.e., DLT allows us to render the execution of duplicated tasks completely unnecessary, and this delivers far greater cost savings than would any effort to merely make these duplicated tasks more cost efficient). Specifically, DLT enables the creation of a chronological, decentralized, interbank ledger in which financial institutions that need to conduct the same. KYC verification tasks for that customer can verify the result of the process that has already been conducted for that customer, thus avoiding conducting duplicated KYC verification tasks. Moreover, the use of DLT allows the cost of the KYC process to be shared proportionally among the financial institutions that work with a specific customer. In particular, the system allows customers to carry out the full KYC process with only one financial institution, and later on to share the result of that KYC process with any other financial institution that they intend to work with. The DLT acts as a ''single point of truth'', understood as the only source of information, accepted by any involved party should conflict occur.

2. Current KYC process

KYC, as defined by the Reserve Bank of India (2016) is a process by which banks obtain information about the identity and address of the customers. KYC means "Know Your Customer". KYC processes are generally repetitive, inconsistent, and duplicated, leading to high administrative overheads and costs. The process also includes risk management with regard to on boarding new customers, the Monitoring of transactions, and specific customer policies for banks. The process is costly for financial institutions and may expose them to large fines if it is not conducted in accordance with the existing regulations

Figure 1 represents the current KYC process in which each customer has to register the documents three times there by increasing the cost to three times which could have been performed in single time.

With this paper, we planned to reduce the progressive cost of KYC process by tackling the cost problem of KYC from financial institution perspective by using blockchain.

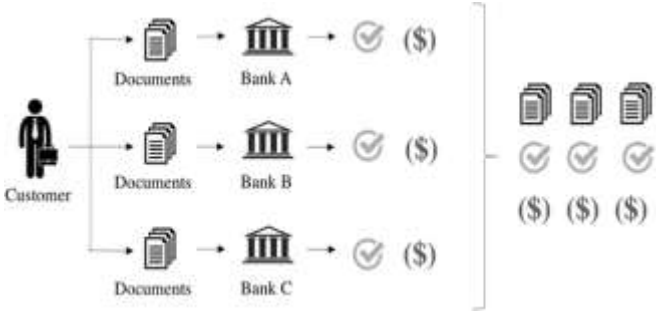


Fig -1: Current KYC Process

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

- **Data integration:** currently, several third-party data providers and external validation agencies offer data and interfaces to extract the required customer information. However, banks struggle to integrate this data to obtain a consolidated view of the customers. This has led to increasing instances of banks' failure to comply with regulatory requirements, resulting in huge penalties and reputational damage.
- **Expensive technology:** post due diligence, banks need to digitize data in the documents to feed it into the repositories. This is an expensive exercise, as it uses advanced technology platforms.
- **Evolving regulation:** the KYC landscape is constantly facing new regulation across different jurisdictions. Therefore, KYC utilities need to keep updating their guidelines. This increases the need for banks to improve their data collection mechanisms for effective risk management and timely compliance.
- **Fragmented approach:** banks do not have a single, unified KYC system for its various lines of business like wealth management, asset management, and brokerage. Maintaining these multiple systems and integrating different interfaces puts banks under immense pressure and adds costs.

3. Blockchain Technology

Blockchains are a digital technology that combines cryptographic, data management, networking, and incentive mechanisms to support the checking, execution, and recording of transactions between parties. Blockchain technology ensures the elimination of the double-spend problem, with the help of public-key cryptography, whereby each agent is assigned a private key (kept secret like a password) and a public key shared with all other agents.

The validity of the information stored on a blockchain's ledgers is ensured by the network's nodes with the help of a secure hash algorithm (SHA). Blockchain technology uses an SHA to translate the contents of a block into a cryptographic fingerprint referred to as a 'hash'. An SHA can also be used to generate from a digital document a unique 'fingerprint' of that document, such that this fingerprint cannot be replicated unless it is generated from the exact same document. This ensures that all of a blockchain's participants can easily verify the authenticity of any document previously hashed simply by hashing it again and comparing the hash they generate to the hash that was previously generated using the authentic document. Further, the hash does not reveal any information about the contents of a document, just as analyzing a human fingerprint can help one to prove the identity of an individual but fails to reveal – for example – the features of that individual's face. In a distributed ledger with multiple nodes, the information recorded by the network is stored sequentially in a list of records that is divided into blocks and distributed to all nodes on the network. The information in each individual block is then used by the system's protocol to generate a secure hash that identifies that specific block. Each subsequent block records the hash of the previous block such that all blocks are chained together sequentially making it impossible to change information in one block without changing all previous blocks. If one node alters the information on its ledger and tries to interact with the network using what is, thus, 'false' information, the hash will no longer match the ledger distributed to the other nodes on the network and the transactions that this node attempts to conduct will not be accepted by these other nodes. The process of verifying transactions and ensuring that blocks have not been altered is carried out by the nodes of the network.

4. KYC Process Using Blockchain

This paper solves the problem in current KYC process based on three assumptions: : First, a group of financial institutions, working in the same country and therefore obliged to respect the same KYC regulations, agrees on the standards for granting core KYC verification to a customer. Second, all the financial institutions that collaborate in the system agree on the average costs of conducting a core KYC verification process. This cost might of course depend on the complexity of each individual customer, based on predetermined parameters (e.g., client size, volume of documents exchanged, etc.). Third, the national regulator maintains the system and approves financial institutions to work with the system in order to conduct a more efficient and transparent KYC verification process. These three assumptions are necessary to ensure a correct incentive structure across the participating financial institutions.

Further, we define a set of four conditions that must be fulfilled by the artifact. It should make sure the proportional sharing of the cost of conducting the core KYC verification process; It must maintain the privacy standard for KYC process; Must ensure that without conducting core process no institution should charge; No institution can access other member institution without paying for using information. The Ineffectiveness Condition ensures the financial institution that is conducting the KYC core verification process has no Incentive to prefer the core conduct of a different institution Verification of KYC, and vice versa. Unless the customer reveals the information the system cannot know whether the customer is working with other financial institution.

The artifact consists of two parts. The first part is permissioned database that guarantees confidentiality of stored documents. The second part is a distributed ledger that serves as an immutable record and clearing system via which to proportionally distribute the costs of the KYC

process among the participating institutions. The Regulator implements and controls the system that enable Database and DLT infrastructure. The regulator plays a central role in the system by developing and maintaining the fabric layer.

The smart contract contains the documents' hash codes, the public key of the home bank, the certificate of approval, which conveys that the customer has been validated, and an array called ''onboarded'' with all the public keys of the financial institutions that have paid the proportional compensation amount to the home bank.

The system ensures that the customer should be registered with institution they wish to but its results can be used by other financial institutions. Suppose if the customer wants to work with X financial institution then core KYC verification will be done only once and if customer wants to work with another financial institution then the KYC details can be fetched from X institution, thereby reducing the time. The cost M of conducting core KYC process for one customer will be not exceed more than X*M.

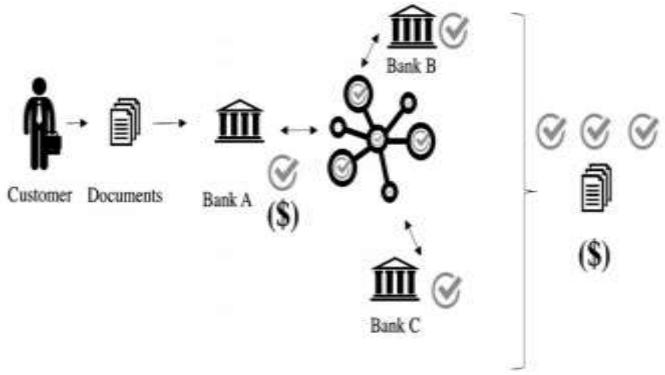


Fig -2: Proposed work flow and cost structure of KYC after the implementation of the artifact

Figure 2 illustrate that the system enables the same customer to work with the same three financial institutions, but now the exchange of documents and the core KYC verification process only occur once and the costs are reduced to a third.

This system fulfills the four previously defined conditions: proportionality, irrelevance, privacy, and no minting. With regard to privacy since each financial institution only uses one account for each customer, and it is therefore not possible to identify which institution is behind which public key, privacy for customers and financial institutions is ensured. Only if one customer would work with all the institutions in the system would all the institutions be able to infer that this was the case. However, since financial institutions use only one account per customer, their privacy would still be guaranteed with regard to the rest of the customers. The no-minting condition is fulfilled, since only by paying an institution be added to the onboarding institutions list of a customer that approaches it. Since the action of compensating other institutions for the core KYC verification process that has been conducted can only be triggered by a real customer approaching an institution, no institution has an incentive to fake smart contracts claiming that it has conducted a core KYC verification process, since in such a case there would exist no genuine customer behind such a process that would subsequently approach another institution and ask to be verified.

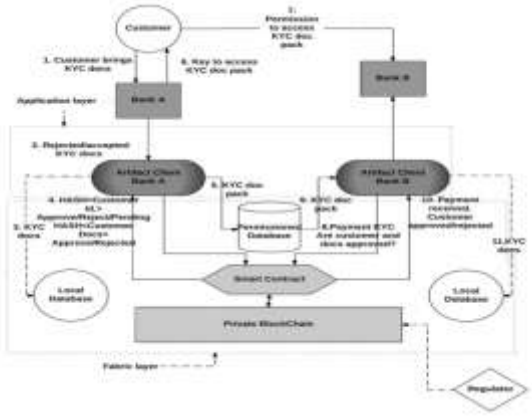
5. Implementation of KYC

In this section we discuss the implementation of redefined KYC solution based on blockchain.

Implementation of this system will have significant impact on financial sector therefore it needs close coordination with regulator.

5.1 Design of a KYC Solution

The system proposed in Figure 3 explains the new KYC process through the example of customer who approaches two financial institutions. Here the customer provides the required KYC documents for verification to the home bank. The home bank uses application in order to handle the document exchange with the customer outside of distributed ledger and to store these documents in its local database. The document will be stored on Distributed edger once the document is processed by the home bank. Once the customer is validated the home bank creates a document package. This document page can be used to grant the verification process. Further if the customer wishes to work with other financial institution they can share this document package .The next financial institution can validate the customer through application that communicate with smart contract to obtain customer details. Now this financial institution can hold the copy of document package since it has been granted.



5.2 Smart Contracts

Smart contracts are self-executable code written inside blockchains. These are similar to conventional business contracts that are used for code of conduct agreement between two parties. The smart contracts execute automatically when the defined conditions are met. Smart contracts help to carry out agreements and transactions in a trusted manner among the untrusted or unknown parties without the requirement of central authority.

Smart contracts are written using Solidity language. It is an object-oriented language, and its syntax are similar to JavaScript or Python. Smart contracts have several benefits over conventional contracts like cost saving, and improved efficiency. Smart contracts are popular as they are easily verifiable by all users and ensure trust among parties.

5.3 Benefits

- Banks find the whole process extremely cost-effective.
- The process is much smoother for customers as they need to upload their details only once.
- The scope of popular KYC methods like eKYC is limited to India but this solution can be applied globally without any restrictions.

6. OBSERVATION AND RESULTS

This paper provides a solution that reduces the total cost compared to traditional KYC process. Here customer registers with single financial institution there by reducing the redundancy task by avoiding the registration with multiple financial institutions. The ultimate efficiency gain of our proposed solution was the dual benefit of reduced cost for the institutions and better experience for the customers.

7. Future Scope

With the current rate of growth of the banking sector, such an approach really has the ability to bring about big improvement and shared gain to all of concerned stakeholder. We can include this research to payment wallet where the framework can be used to conduct KYC process for the customer.

REFERENCES

[1] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.

[2] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[3] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[4] K. Elissa, "Title of paper if known," unpublished.