Hassle - Free and Secure e-KYC System Using Distributed Ledger Technology

Bharti Pralhad Rankhambe
and
Dr Mrs Harmeet Kaur Khanuja

Department of Computer Engineering,
MMCOE, Pune, Maharashtra, India

The blockchain technology is a prominent, reliable and secure technology which is getting into almost every industry. The fundamental essence of blockchain technology offers features like transparency, decentralization, immutability, resilience, disintermediation, collaboration, security and trust. In this paper, we have focused on how the present banking industry, especially the KYC document verification process, can be impacted after using blockchain to store and track the records. The current day banking KYC processes are highly reliable on paper which is an outworn process. It is utmost essential today to have an upgraded KYC system, embedded with a reliable and trustable technology like blockchain, that could withstand frauds, and resolve the scalability and security issues. In the proposed system, the use of blockchain in KYC process restricts the presence of middlemen. This results in a reduction of fraudulent activities and errors that may occur when there are a lot of manual activities involved. Furthermore, the document verification process is only conducted only one time, no matter what is the number of financial institutions with which the customer is working with. This system provides more efficiency, reduction in costs, enhanced customer rendezvous and end-to-end transparency during the process of integrating the customer documents into the bank database.

Keywords: Blockchain, KYC, Smart Contracts, Decentralization, Security

1. INTRODUCTION

Blockchain, at present, is the most novel buzzword within the industry. It is a wide-ranging technology that has its radicles in the financial sector wherein, its first application was a cryptocurrency called Bitcoin. Blockchain has multiple other applications beyond cryptocurrency. Many industries have already adopted it. Blockchain can be defined as a logically decentralized and technically distributed ledger, shared individually in an architecture of a peer to peer network consisting of nodes. This ledger encompasses a sequence of transactions. These transactions are encrypted with a secured hashing mechanism. This mechanism is known as the SHA Algorithm. The transactions are added into a sequence block with an agreement mechanism between the peers, which is known as 'Consensus' which means agreement between the peers. There is no central authority to dominate the protocol or the blockchain. The blockchain can be described concisely, as a tamper-proof record of all transactions on the network, which can be available for access to all members of the network and also offers the advantages of working at low costs with reduced security risks, and enhanced efficiency[13].
'Bitcoin' - the first application of blockchain was introduced to the world by an unknown programmer, named with the alias "Satoshi Nakamoto". The white paper "Bitcoin: A peer to peer Electronic Cash System" published 12 years back on the date - 31 st October 2008 was used as a medium to introduce this technology to the world. Ten years later, nobody has knowledge of the real identity of Satoshi Nakamoto, but the world at large knows about Bitcoin[14].
Bitcoin is not only a cryptocurrency, but it is a collection of concepts and methodologies used to secure that cryptocurrency. These concepts can be reused in other areas, where the applications

are far beyond just a virtual currency. How blockchain can transform the banking industry will be explained in the following sections.

2. LITERATURE SURVEY

Sr. No.	Title and Year	Publisher/ Indexing	Platform Used	Outcome
1	KYC Optimization Using Distributed Ledger Technology (2017)	Springer	Ethereum and R3 Corda	End to end solution for KYC cost distribution system using distributed ledger technology
2	Know Your Customer - Decentralized Secure Sharing Protocol on Quorum (2019)	IIT Bombay	Quorum Blockchain Platform	About Quorum Platform, cKYC and eKYC, Network, Privacy and Consensus
3	Privacy-preserving KYC on Ethereum (2018)	Semantic Scholar	Ethereum	Centralized and decentralized Identities, mathematical explanation, Use cases and Implementation details
4	Block Chain Technology (DLT Technique) for KYC in FinTech Domain: A Survey (2018)	CrossRef	R3 Corda	Smart Contracts Sample Code, Terminology related to R3 Corda platform
5	If at First you Don't Succeed, Try a Decentralized KYC Platform: Will Blockchain Technology Give Corporate KYC a Second Chance? (2018)	R3 Corda White Paper	R3 Corda	Corporate KYC Utilities, KYC Data Requirements, Models, Benefits, Common Obstacles Faced by Both Centralized and Decentralized KYC, Novel Challenges
6	Decentralized KYC System (2017)	Academia.-edu, Cite Factor	Inter - Planetary File System	Proposed architecture, Key generation flowchart, Sample Contracts (IPFS), Efficiency percentage
7	Applications of Blockchain Technology to Banking and Financial Sector in India (2017)	SpringerNature, Reserve Bank of India (IDRBT)	NIL	Analysis of the pros and cons, by the RBI. Official document of the RBI
8	Applications of Blockchain Technology in Banking and Finance (2018)	CiteSeerx	NIL	Current pain points and how blockchain can help.
9	Blockchain application and outlook in the banking industry (2016)	SpringerOpen	NIL	Internal and external issues of the banking industry, Payment clearing system: distributed clearing mechanism, obstacles to implementing blockchain technology in the banking industry, How should blockchains be regulated?
10	Sovrin TM : A Protocol and Token for Self-Sovereign Identity and Decentralized Trust (2018)	White Paper from the Sovrin Foundation	Hyperledger Indy	About the Sovrin Foundation, Hyperledger Indy

Table I: Comparative Study Table of Research Papers

Table I shows the comparison table consisting of Paper Title, Year of Publication, Indexing, Platform used and Outcome.

The Blockchain for banking platform helps us to make the e-KYC documents tamper proof and allows the accurate and permanent allocation of this data to the customers. Along with this, the functionality to verify these documents is also offered. It can reduce the overall frauds and tampering of the identity documents, degrees and certificates. Blockchain technology can be used to solve many document verification problems and can help banks as well as customers to monitor the outcomes. The data can be stored securely and in a tamper proof format when it is stored onto the blockchain network. Blockchain can be used in private, public and consortium sectors depending upon the usage and the scope of area of the blockchain. Finance and banking systems can take benefit of this scalability of the blockchain and can be effectively used in the financial sector.

In this paper we have discussed the research gaps in the current KYC process, and how they can be mended using Distributed Ledger Technology. In the Proposed Work section, we will see the objectives of this research work. Moreover, we will study the advantages and limitations in using Blockchain as a solution to the existing system. Further, in the same section, we will see the Mathematical Model used to distribute the verification costs across the financial institutions working with the customer. In the Proposed Methodology section, we will study the assumptions and conditions considered for this research. In the following sections, we will be discussing the System Architecture, System Workflow, Hardware and Software requirements, and finally the Result Analysis, Conclusion and Future Work.

3. RESEARCH GAPS IN THE CURRENT KYC PROCESS

Since ancient times, ledgers have been like the nucleus of all economic transactions. They have been used since generations to log payments, contracts, deals and also for movement of assets. The journey which began with noting down information on clay tablets or papyrus surfaces has now escalated to the invention of paper. Over the last couple of decades, computers have very conveniently and speedily provided a way to store records in a digital form. Today, with the advent of innovation, the digital information storage is moving towards much higher forms - which should most desirably be cryptographically secured, fast, decentralized and distributed. But, in reality, today's KYC process is a time consuming process which uses manual documentation. It lacks the mechanism to track the throughout process, from start to end and hence has a potential for fraudulent activities. We can see below example to overview the drawbacks of current KYC system[8][17].

If we consider the current financial system, the financial institutions are required to onboard their customers for the verification of their identity. This is an inevitable and essential step in order to avoid fraudulent activities. This process is known as the Know Your Customer (KYC) Document Verification Process[7][11][16]. The Know-Your-Customer process is nothing but interchange or give and take of essential official papers, between a person and the bank of the person. Then, all the important data about the person is kept stored in a database of the bank. This data is collected from official documents having Identity Proof, Address Proof, Photo Proof and sometimes Bio metric data as well [4][7]. In India, a variety of government granted documents can be provided for identification like, Passport, Aadhar Card, PAN Card, Driving License, Voter ID, etc[4][7][11]. When these documents are submitted to the banks, they are undergone a background check to verify the authenticity and credibility of the documents so as to ensure that no fake or illicit data is provided by the customer. Indian Government has made it mandatory

for all banks to undergo verification of all their customers. If these norms are not followed, the banks have to pay heavy fines[7][11][16]]. For example, Reserve Bank of India imposed a penalty of ₹50 lakh each on Punjab National Bank and Allahabad Bank; whereas, ₹25 lakh was fined on Corporation Bank because of non-compliance with certain provisions of directions issued by the Reserve Bank of India on Know Your Customer norms, anti-money laundering standards and opening of current accounts[16].

When a customer intends to open an account in a financial institution, the KYC process gets initiated. Initially, both parties involved, the bank and the customer acknowledge and admit on the terms and conditions of the contract. Subsequently, the required documents are sent to the bank by the customer to initiate the KYC verification process. In this process, the bank scrutinizes the documents and if everything is accurate, generates an internal document which aids as a certificate to assure the regulator whether the status of the customer (validated or rejected) and that the KYC process has been correctly conducted or not[1][3]. Note that this process is repeated every time the customer wants to work with a new financial organization.

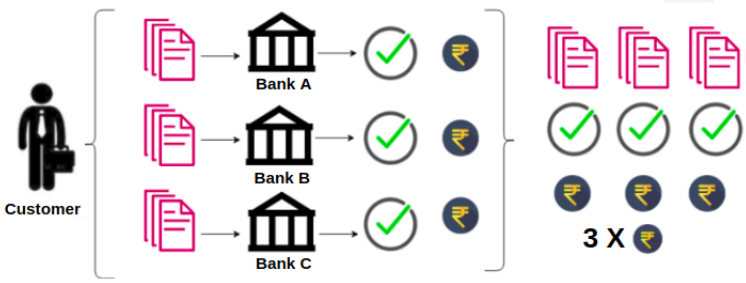

Figure 1: Current KYC Verification Process

Figure 1 shows an illustration of the process that occurs when one customer has to work with three different financial institutions. It can be clearly observed from the diagram that the same process is recurred three times. Also the total verification costs are generated thrice, though the core process is in reality, the same. It is important to note here that the "core" process means the minimum KYC verification that all financial institutes are obliged by law to conduct.

4. PROPOSED WORK

In this paper, emphasis is given on creating and maintaining a Digital Portfolio in determining the value of Online documents (like Aadhaar Card, Pan Card, Passport, Driving License, Marriage Certificate, etc) which are required for KYC verification. Blockchains can help users offer secure and fraudulence-free sharing of documents only to the intended banking institute without the interference of middlemen. Smart contracts can be used to automatically execute agreements once a set of specified conditions are met. These smart contracts have the potential to reduce paperwork in many sectors including the banking domain[11]. It could reduce paper-based processes, minimize fraud, and increase accountability between users and those institutes they wish to share their personal documents with. The most important advantage of using blockchain for smart contracts and transactions is that, the same concept can also be applied towards making the process of business accounting more transparent. In public assistance, the blockchain could

help streamline public assistance system for families. As financial institutions store more data, blockchain could offer safer and potentially cheaper alternatives.

4.1 Objectives

The objectives of this research work are as follows:

✓ To provide an introduction to Blockchain Technology and its core social value proposition.

✓ To identify and engage with the key issues which are influencing policy-makers and other key stakeholders in considering the use of blockchain technology as a value-added proposition within a financial landscape for KYC document verification.

✓ To explain how financial institutions and customers can use the technology as a transparent trusted system for securing, sharing and verifying personal documents required for KYC verification.

✓ To determine if the technology is fit-for-purpose for the recording of KYC banking process within the short-term, and is likely to be taken-up by banks and financial institutions and be deployed as an open standard.

✓ To discuss how blockchain technology may help bridge the legitimate need for banking institutions to safeguard their brands and reputations when issuing banking credentials to individuals.

✓ To identify a set of clear opportunities and challenges for the take-up of blockchain technology in financial institutions for KYC verification.

✓ To make a set of recommendations that may support RBI efforts to open up a different process of KYC in Member States by maximizing the potential for blockchain technologies.

4.2 Advantages and Limitations

The advantages of this system are listed as below:

—This system will bring improvements in auditing and tracking duties of the national regulator as it provides a transparent record of information which may act as the single point of truth in case any disagreements occur.

—The proposed system allows for an alliance between financial institutions which often have trust issues between them. Note that, this system allows for anonymous compensation and document sharing. This anonymity property is most desired and hence supported by financial institutions given that they compete with each other regarding customers' accounts and assets.

—The properties of the distributed ledger allow institutions to exchange information without revealing their identities and ensure (using the protocols) that all institutions follow the same. Thus, all institutions are anonymous and they still proportionately pay the compensation charges utilized for verifying a customer.

—Note that this system proposed is, in essence, a system for inter-bank collaboration. This system, in the future, can be integrated into a broader DLT-based framework, like the very popular r3 Corda project[2][5].

—The proposed system eliminates the high central authority fees.

—This system allows for the automation of the KYC process, acts as a source of information if a dispute should occur, reduces settlement time, and reduces business costs.

The limitations of this system are listed as below:

—The main disadvantage of blockchain is its high energy consumption. In efforts to validate the transactions, the network miners are attempting to solve many solutions per second. This means many nodes are working to solve the same puzzle and hence a lot of work is done in parallel for the same end result[13][14].

—This system uses asymmetric key cryptography which has a pair of public and private keys. This private key is the most critical and must be kept confidential. If this key is lost, the data privacy of the documents is lost[13][14][17].

—Blockchains are susceptible to a type of attack in which, for a blockchain network, if more than half number of nodes in the entire network agree to a fraudulent decision, the other honest nodes can do nothing about it. This is known as the '51 percent Attack'[14].

—It is much more difficult to design and develop a secure blockchain system than a similar centralized system.

4.3 Mathematical Model

The Mathematical Model for the distribution of KYC verification costs can be seen below -

Suppose that n is the total number of banks working together with a government regulator in jurisdiction for this network of KYC validation. c is the fixed average price to be paid for conducting the core document verification of one customer. c is also the cost paid initially by the home branch in the verification of documents of first Customer. The regulator also establishes a new digital currency or token which has a fixed exchange rate against the national currency.

Now, the second bank which intends to work with this customer will have to pay half the amount c. Thus, we can say, the nth bank will have to pay an amount equal to (c/n) to the smart contract.

The smart contract then divides this contribution into $(n-1)$ equal parts and issues the respective amounts to the $(n-1)$ number of institutions working with the customer.

Accordingly, if only one bank works with a customer, only that bank has to bear the full cost c of verification of KYC of the single customer. Other banks need not contribute in paying for a customer who is not working with them. So, for n number of institutes, the other $(n-1)$ institutes pay an amount equal to -

$$\frac{c}{(n-1)}$$

and receive an amount equal to -

$$\frac{c}{n(n-1)}$$

from the last institution to join. Consequently, the cost for each institution equals:

$$\frac{c}{n-1} - \frac{c}{n(n-1)} = \frac{c}{n}$$

To summarize, the verification is undertaken only once for n number of institutions and not n number of times. Also, the total cost for conducting the core KYC verification for single customer is now c and not $(n * c)$ as it is currently in practice[1].

5. PROPOSED METHODOLOGY

This paper utilizes a different approach of Distributed Ledger Technology (DLT)[1][2]. A distributed ledger can be defined as a record of transactions, maintained in a decentralized format, which is also distributed across different locations or nodes. Every node of this distributed network owns the same, consistent copy of the ledger. This distribution eliminates the need for a central authority who has to monitor activities in order to avoid fraudulent activities. Instead, the validation of activities is done by all the nodes in the network thus eliminating the need to provide incentives to the middlemen[4] [5].

In Figure 1, three sets of the same documents were verified thrice, thus adding to redundancy of actions. It generated costs which were again in multiples of three. In the earlier model, if the customer had to open accounts in ten banks, the costs generated would be in denominations of ten, i.e, number of banks. This is utter wastage of money, resources and energy as well. Now, if we see Figure 2, the model from Figure 1 changes dramatically after application of blockchain technology. Here, the verification process is conducted only once for any number of banks, provided that those banks are operating in the same jurisdiction that uses blockchain. This new model for KYC verification allows for massive cutting down in costs for the banking institutes. Customers have the advantage of not having to make frequent trips to banks to manually provide the documents for verification.

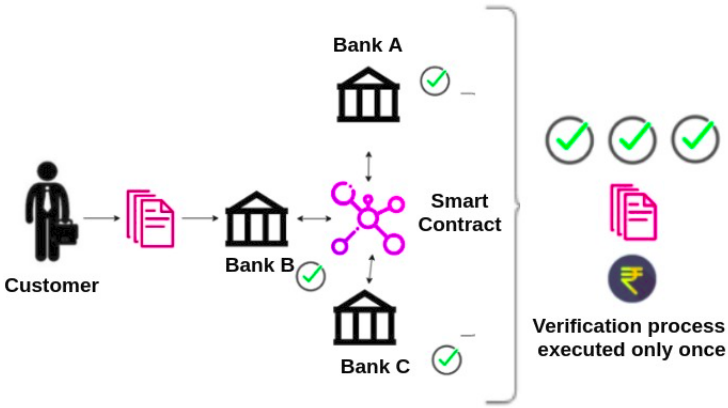

Figure 2: KYC Verification Process after implementation of blockchain

All the information stored on the distributed ledger is secured using cryptography. This information can be accessed using keys and cryptographic signatures[14].

5.1 Assumptions and Conditions:

There are a few assumptions that this KYC process needs to rely on [1]. They are described as follows:

✓ First, the members of the group of banks functioning in the same country should follow the same rules and regulations for KYC and should stick to the same standards for permitting the core KYC verification to a customer.

✓ Second, all the financial institutions that fraternize in the system should consent to a specific cost for conducting the KYC process. This cost might rely on the complexity of each customer based on various factors like type of document, etc.

✓ Third, it is essential to have a Government Regulator. This regulator can be like the Aadhaar Portal of Government of India to monitor the system and approve the new financial institutions.

These three presumptions are obligatory so as to warrant an appropriate incentive structure across the participants of the network.

There are four more conditions defined further, which need to be fulfilled by the proposed architecture [1].

✓ Balance Condition:
The cost of conducting the core verification should be balanced across the financial institutions. This condition ensures that the costs are balanced throughout the institutions.

✓ Insignificance Condition:
No financial institution should have any reason to favor another institution to conduct the KYC verification process instead.

✓ Isolation Condition:
The privacy standards of the KYC process should be maintained as they are today.

✓ No – Counterfeiting Condition:
No institution can claim compensation without conducting the core process.

6. SYSTEM ARCHITECTURE

The proposed architecture comprises of two major sections. First is the Application Layer and next is the Code Base. The application layer is more related to the user interface. It has different clients set up for managing the artifact. These clients are known as 'Artifact Client' and every bank has an artifact client of his own. The actual programming happens in the next major section which the code base section. The code base section consists of a separate local database for each bank, the common permissioned database, the smart contract, which acts like the heart of this entire architecture, the government regulator and the blockchain which is of permissioned and private nature. All these components of the architecture can be seen in Figure 3.

The components will be discussed in detail below[1].

Artifact Clients – This component lies in the application layer. Hence most of its duties are related to the user interface. The actual interaction between the bank and the smart contract happens through this client.

Local Databases – Every bank has its own local database. When the bank is considered as the home bank for the customer, this local database is used to store the documents submitted by the customer for verification, before the smart contract is generated. The documents package is also stored here by each bank for their home customers.

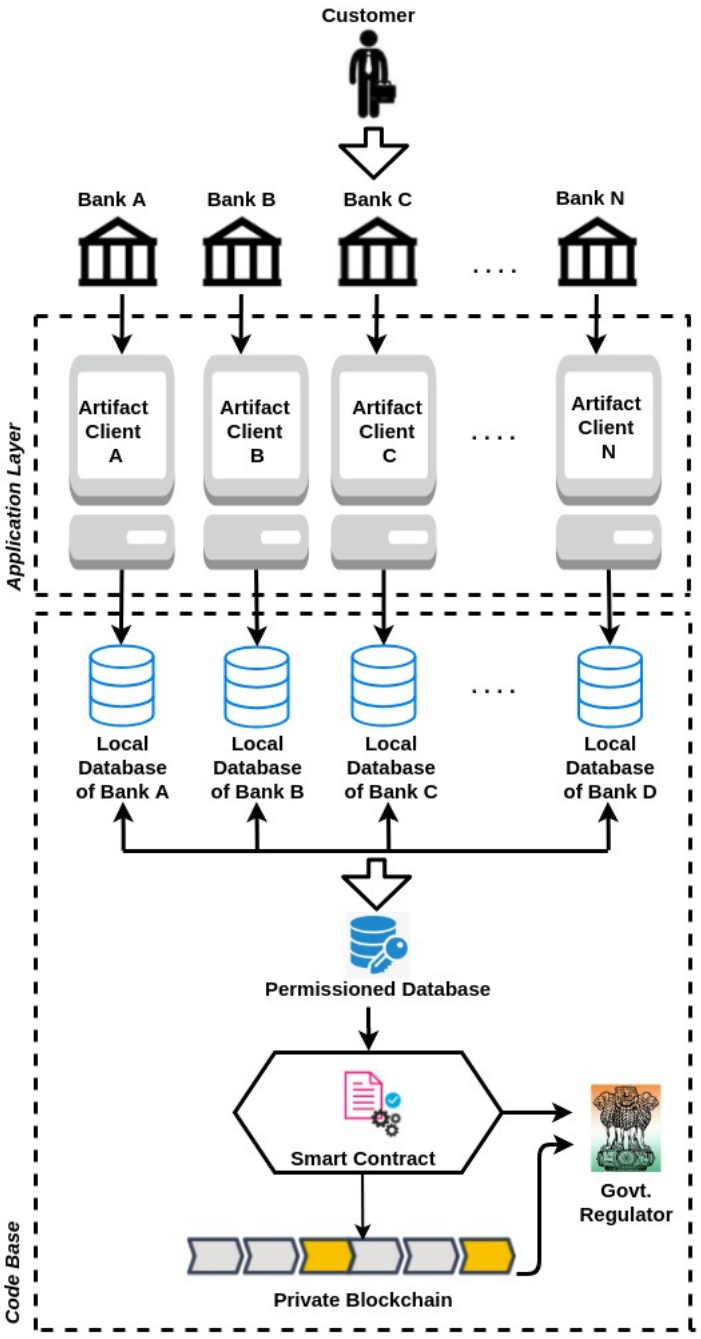

Figure 3: System Architecture

Permissioned Database – The permissioned database is controlled by the government regulator. This is used for the storage of private documents of the customer. A copy of the documents package is also stored here for all the customers of all banks.

Smart Contact – This contains a hash which contains a digitally signed document with the

customer's public key[14]. The clearing of the dues for all banks contributing to the KYC verification for single customer is carried out by the smart contract.

Government Regulator - The government regulator enables the database and sets up a digital token or currency[11]. This is a solely responsible component which actually makes the decision whether the financial institutions are reputed and credible enough to work in this jurisdiction for KYC verification.

Private Blockchain – This is a ledger of tamper-proof records and acts as a clearing house through which the KYC costs are proportionally distributed among the participating institutions. Here, the digitally signed, hashed format of the document package is also stored.

The architecture works as follows[1][2]:

(1) A certain number of financial institutions (say n, where $n > 3$) and the government regulator agree to implement the new KYC verification process. At this stage, a value (amount of money) is assigned to the token in the system. This works like a virtual currency scheme, wherein each financial institution can exchange their tokens and receive the national currency in return which can later be compensated with other member financial institutions for the verification processes undertaken by them. Note that, the government regulator runs the system, and hence only he has the knowledge of the individual activities.

(2) As soon as the customers approach a financial institution to open an account, they are handed over a public and a private key. The first bank which performs the KYC verification of a customer will be referred as a 'Home Bank'.

(3) After the account has been granted to the customer, he shares his key, and the documents to be analyzed with the home bank. To retain the confidential nature of the customer's documents, this exchange of documents take place externally and not in the distributed ledger. This is why, a local database is used by the home bank for storage of these documents.

(4) After the verification is done, a smart contract is generated, containing a digitally signed document with the customer's public key. Additionally, the home bank stores a hash of each document used for the KYC verification on the blockchain.

(5) Finally, the home branch creates the customer's 'Document Package' which contains the hashed format of the documents of the customer along with the digitally signed hash, which is the compressed form of the summary of the entire KYC verification process, including the result of the core KYC verification (accepted or rejected).

(6) Additionally, the home bank creates another smart contract for this customer which contains a list of the public keys of the wallets of the financial institutions.

(7) When a customer approaches other institutions than the home bank to work with him, he has to share his public key and the address of the original smart contract created by the home bank in which the result of the KYC verification is written.

(8) The new financial institution can comprehend from the smart contract, how many other institutions have worked with this customer so far.

This workflow can be seen in Figure 4.

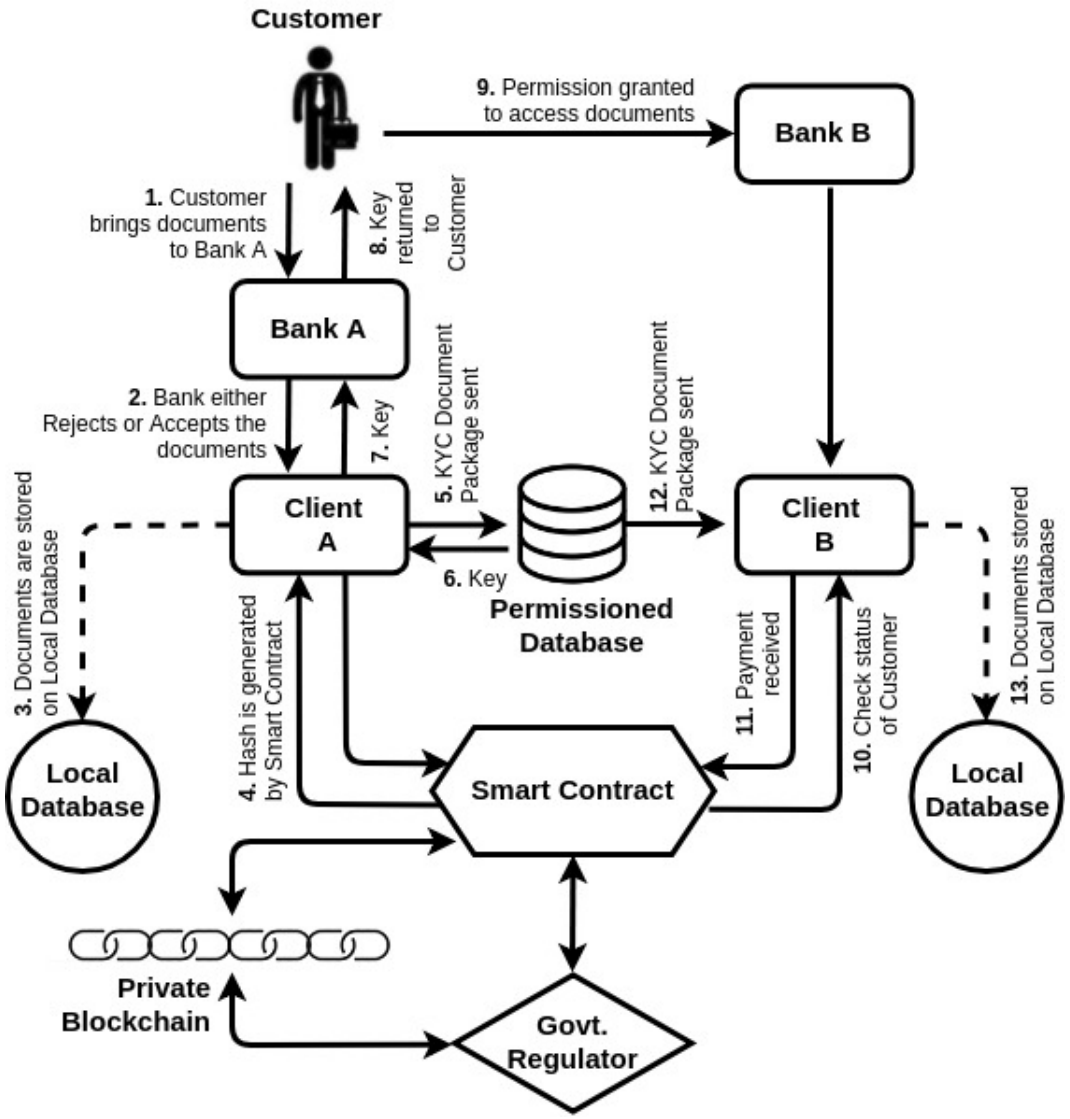

Figure 4: System Workflow

7. HARDWARE AND SOFTWARE REQUIREMENTS

The proposed model is one use case of the blockchain platform. There are many leading platforms that support programming for blockchain technology. Ethereum is one of those platforms which has already gained popularity in the blockchain crowd. It provides both public and private networks.

The Linux Foundation has developed Hyperledger which has seven more open source blockchain platforms, categorized based on different functionalities they provide. All Hyperledger platforms have a common benefit of being modular in nature.

The following platforms fall under the Hyperledger Umbrella like Fabric - used for businesses, Sawtooth - used for Supply Chain Management", Indy - used for Certification and Identity management and Quorum - designed for enterprise agreements. All these platforms differ in the

consensus mechanisms, permissions and other protocols[10][17][18].

Hyperledger Fabric is one of the most stable and widely accepted frameworks for blockchain development.
Quorum is a permissioned development platform which is based on the Ethereum blockchain.
Here the question arises, why not use Ethereum instead? The reason being Quorum offering the advantage of having private networks.
It also lets us have a choice of consensus algorithms, like Raft-based Consensus and Istanbul Byzantine Fault Tolerance Consensus Algorithm[19].
Indy can also be used to implement this project as it concentrates basically on having a unique decentralized identity that can exist digitally[10][18].

8. RESULT ANALYSIS

Blockchain, also known as Distributed Ledger Technology (DLT) is a centralised digital database that can be shared with many people at the same time. This means that, this data is divided between the members and not copied. Thus, it forms a decentralised distribution system allowing access to all the documents on the network.

This system enables the smooth changing process. It is a promising technology that helps in reducing risks, preventing frauds and providing transparency in operations.

Whereas, Cloud is a service in which different functionalities can be done with your data using the internet. In other words, a cloud system refers to various computing components like software, hardware, and infrastructure that will enable the delivery of many cloud computing services. Few examples are PaaS (Platform as a Service), SaaS (Software as a Service), and LaaS (Infrastructure as Service). Cloud computing services are delivered through a network which is centralized in nature. This network is nothing but the Internet.

It should be noted that Blockchain offers more opportunities compared to Cloud Computing Technology. Blockchain can help in solving third party data usage issues.

8.1 Comparative Analysis between Manual, Cloud and Blockchain based KYC Verification

In Table II, a comparative analysis between Manual KYC Verification, Cloud - Based KYC Verification and Blockchain - Based KYC can be seen.

Sr	Manual KYC	Cloud - Based KYC	Blockchain – Based KYC
1	Completely paper based process.	Distributed, yet centralized network of nodes controlled by a single entity.	Completely decentralized via management by numerous anonymous individuals.
2	Goal is to store hard copies/ print outs of customers' documents.	Goal is to manage sharing/viewing of documents using minimal computing power.	Goal is to manage a ledger of document flow between users.
3	Managed by Bank officials.	Managed by Google Drive, AWS, Microsoft Azure Cloud, etc.	Managed by Authority nodes already existing on the network.
4	Verification is done manually by comparing hard copy with the original document.	No authorized mediating body is involved for verification.	Government Mediator is involved specially for the verification of credentials.
5	No cryptography is used. Documents are collected and kept locked in store rooms.	Documents are password protected or R/W protected.	One way cryptography is used. SHA algorithm makes it impossible to tamper the record.
6	No additional security.	No additional security.	Additional security is offered by the newly added blocks so exising record cannot be changed.
7	No selective disclosure.	No selective disclosure.	Selective disclosure is offered.
8	No security	"Cloud based application" admin can incorrectly modify details about your account without recourse.	Actions taken on a public blockchain application are logged for everyone to see.
9	No server.	Cloud network can go down if the main server is down.	Blockchain network never goes down as some peers can always be online in case a few go down.
10	No tracking.	No tracking.	Efficient tracking of Documents and who viewed them and in what sequence by a permanent audit trail.

Table II: Comparison: Manual KYC vs Cloud - Based KYC vs Blockchain - Based KYC

Another comparison can be seen in Table III, about various document verification platforms based on blockchain.

Leftmost column lists out various blockchain-based certificate verification schemes existing today in the market. In this table, a comparison is made based on parameters like system features, security features and usability features[12].

Scheme	Accreditation	Verification	Revocation	Privacy	Transparency	Accessibility
UNIC	-	PPP	-	PP	PP	PP
Blockcerts	-	PP	PPP	PP	PP	PP
Hypercert	-	PP	PPP	PP	PP	PP
Echo	-	PPP	-	-	PP	PPP
UZHBC	-	PPP	-	PP	PP	PP
EduCtx	PP	PPP	-	PP	PPP	PPP
Blockchain for Education	PP	PP	PPP	PP	PP	PP
Cerberus	PP	PP	PP	PP	PP	PP

PP = Provides property

PPP = Partially Provides Property

- = Does not provide Property

Table III: Summary comparison of various blockchain solutions

9. CONCLUSION AND FUTURE WORK

In this paper, we have suggested a distributed ledger technology based architecture which attempts to minimize the total KYC costs for banks working together in a jurisdiction. With this, the major advantage achieved is the avoidance of redundant tasks by different financial institutions. This research work also gives a solution for the distribution of proportionally divided costs incurred for that group of financial institutions which are working with the same customer. This research suggests many opportunities to increase efficiency in the current financial system. More specifically, this architecture provides more efficiency, significant reduction in costs, improved customer experience and more transparency throughout the process of integrating the customer documents into the bank database, thus improving the customer experience by dissolving the role of middlemen. Furthermore, due to the to the decreased regulatory costs of KYC, the system would lower the barriers to operating a financial institution, thus opening the financial market up to further development and more competition.

The concept of blockchain technology, itself is specifically very advantageous for the banking sector. This is because, the ledger is the actual lifeblood of banks, and blockchain is the most secure ledger that can be offered. Blockchain framework and its protocols offer several features like transparency, decentralization, immutability, irreversibility, resilience and security.

Apart from all the above gains, this system will allow for more efficiency, cost reduction, improved customer experience and elimination of middle-men in the entire procedure, hence reducing hassles for both the client and the financial institution.
Regardless of the chosen approach here, of using the Distributed Ledger Technology, be it a distributed database or a private, restricted, or public blockchain, this research suggests many

opportunities to increase efficiency in the financial system.

This system, as a whole, brings following benefits to all participants:

✓ Users obtain a unified identity which they can use to utilize multiple financial services. Users' personal data is stored only with the KYC Verifier and can be easily updated but only with the User's permission.

✓ Personal data stored on the blockchain is not transmitted to third parties.

✓ Financial services greatly simplify the KYC process: The design lets the banks cut KYC costs while at the same time diminishing risks of handling sensitive data.

✓ Verifying authorities or Governments get an opportunity to stimulate innovation in the financial sector by providing a unified and simple KYC API. The proposed solution can be used in any setting where a smart contract based service wants to limit the set of its users according to some criteria.

Apart from this, all other functionalities of the original Blockchain Protocol, if implemented in banking can transform the banking field altogether. Blockchain will bring sustainable development for sure and hence it is most probably the future of Banking Industry.

References

Moyano, J. and Ross, O. 2017. KYC Optimization Using Distributed Ledger Technology. *SSRN Electronic Journal DOI:10.2139/ssrn.2897788*

Chainworks Digital LLP. 2019. Know Your Customer - Decentralized Secure Sharing Proto col on Quorum. *Third Workshop on Blockchain Technologies and its Applications, Informa tion Security Research and Development Centre (ISRDC) Department of Computer Science and Engineering IIT BOMBAY*

Biryokov, A., Khovratovich, D. and Tikhomirov, S. 2018. Privacy-preserving KYC on Ethereum. *Proceedings of the 1st ERCIM Blockchain Workshop, Reports of the European Society for Socially Embedded Technologies (ISSN 2510-2591), DOI: 10.18420/blockchain2018 09*

Kasturi, R. and Pachaiyappan, V. 2018. Block Chain Technology (DLT Technique) for KYC in FinTech Domain: A Survey. *International Journal of Pure and Applied Mathemat ics, Volume 119 No. 10 2108, 259-265 ISSN: 1311-8080 (printed version); ISSN: 1314-3395*

Rutter, K. 2018. If at First you Don't Succeed, Try a Decentralized KYC Platform: Will Blockchain Technology Give Corporate KYC a Second Chance? *R3 Corda White Paper*

Kaul, A. and Sinha, P. 2017. Decentralized KYC System. *International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056, p-ISSN: 2395-0072*

Reserve Bank of India, 2017. Applications of Blockchain Technology to Banking and Finan cial Sector in India. *Institute for Development and Research in Banking Technology (IDRBT)*

Jani, S. and Shah, T. 2018. Applications of Blockchain Technology in Banking and Finance. *https://doi.org/ 10.13140/ RG.2.2.32 37.96489*

Guo, Y. and Liang, C. 2016. Blockchain application and outlook in the banking industry. *Financial Innovation 2:24, DOI 10.1186/s40854-016-0034-9*

Sovrin Foundation, 2018. Sovrin TM : A Protocol and Token for Self-Sovereign Identity and Decentralized Trust. *A White Paper from the Sovrin Foundation Version 1.0*

Chugh, N., Dave, N., Hota, A., Joseph, A., Mahapatra, M., Malik, S., Mehta, A.,

Ramasastri, A., Ravikumar, R., Sen, S., Seth, P., Sharma, R. and Sharma, R. 2017. RBI Report on Finance Systems in India. *Reserve Bank of India, Central Office, Mumbai*

Ali, S., Haq, H. and Tariq, A. 2019. Cerberus: A Blockchain-Based Accreditation and De gree Verification System. *arXiv.org-cs-arXiv:1912.06812*

Rankhambe, B. and Khanuja, H. 2019. A Comparative Analysis of Blockchain Platforms – Bitcoin and Ethereum. *IEEE's ICCUBEA - 5th International Conference On Computing, Communication, Control And Automation, 10.1109/ICCUBEA47591.2019.9129332*

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic, Cash System. *Blockchain White Pa per*

https://metamask.io

https://economictimes.indiatimes.com/news/economy/policy/rbi-6 imposes-rs-50-lakh-fine-on-pnb-for-delay-in-reporting-fraud-in- kingfisher-airlines-account/articleshow/70511380.cms?from=mdr

Antonopoulos, A. 2018. Mastering Ethereum: Building Smart Contracts and DApps

Swan, M. 2015. Blockchain: Blueprint for a New Economy

Stebila, D. and Paterson, K. 2019. Selected Areas in Cryptography

Desrosiers, L., Gaur, N., Novotny, P. and Ramakrishna, V. 2018. Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger

Bharti Pralhad Rankhambe is an Assistant Professor for the discipline Bachelors in Computer Engineering (Computer Science). She has completed her Post Graduation from Department of Computer Engineering in Marathwada Mitramandal's College of Engineering, Karve Nagar, Pune and her Bachelors in Computer Engineering from Sinhgad College of Engineering, Vadgaon (Bk), Pune in 2012. Her first paper which has been published and indexed on IEEE Explore is titled as "A Comparative Analysis of Blockchain Platforms – Bitcoin and Ethereum" DOI: 10.1109/ICCUBEA47591.2019.9129332.

Dr. Mrs. Harmeet Kaur Khanuja is a recognized Post-Graduate Teacher in Com-puter Engineering, SPPU, Pune. She has completed Ph. D from Rashtrasant Tukadoji Maharaj, Nagpur University on the topic, Design and Development of Effective tool for Database Forensics through Evidence Preservation". She has worked for Post Graduate Research Project on "Disease Informatics and Analytics" in National Institute of Virol-ogy, Pune during the year 2008-2009. She has established 'Center of Innovation' cell in Computer Engineering Department to promote students research activities and presen-tations of Innovative Projects developed in recent technologies.She has 13 publications in International Journals, 7 in International Conferences, and 1 chapter in Security in Computing and Communications, pp 201- 210, vol 467. Springer, Berlin, Heidelberg