International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
©2021 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

Optimization of the KYC Process in the Banking Sector using Blockchain Technology

Bharti Pralhad Rankhambe and Dr. Harmeet Kaur Khanuja

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

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

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 once for each customer, regardless of the number of financial institutions with which the customer intends to work with. This system provides more efficiency, reduction in costs, improved customer experience and more transparency throughout the process of integrating the customer documents into the bank database.

Keywords : *Blockchain, KYC, Smart Contracts, Interplanetary File System*

Introduction

Blockchain, at present, is the newest buzzword in the industry. It is a revolutionary technology that has its roots 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 and others are exploring ways to start with it. By definition, blockchain is a logically decentralized and technically distributed ledger, shared individually in a peer to peer network consisting of nodes. This ledger has a sequence of transactions that are encrypted with a secured hashing algorithm. The transactions are added into a block with an agreement mechanism between the peers, called as'Consensus'. There is no mediator to dominate the protocol or the blockchain. The blockchain can be described in short, as a tamper-proof record of all transactions on the network which is accessible to all members of the network which also offers the benefits of working at cheaper costs with reduced security risks, and enhanced efficiency. During the year 2008, banks and financial institutions were facing a major financial crisis on a global level resulting into the loss of the public's faith on financial institutions. 'Bitcoin' - the first application of blockchain was introduced to the world by an unknown programmer, named with the alias "Satoshi Nakamoto". It was introduced in a white paper "Bitcoin: A peer to peer Electronic Cash System" on 31 st October 2008. Ten years later, nobody has knowledge of the real identity of Satoshi Nakamoto, but the world at large knows about Bitcoin. 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.

Literature Survey

Table 1. Literature Survey: Comparison of Papers

Sr.	Title of Paper and Year of Publication	Author Names	Methods and Outcomes
1.	KYC Optimization Using Distributed Ledger Technology (2017)	José Parra Moyano, Omri Ross	The Current KYC Process, Design Science for KYC Optimization, The Redefined KYC Process
2.	Know Your Customer	Chainworks Digital	About Quorum

	- Decentralized Secure Sharing Protocol on Quorum (2019)	LLP	Platform, cKYC and eKYC, Network , Privacy and Consensus
3.	Privacy-preserving KYC on Ethereum (2018)	Alex Biryukov, Dmitry Khovratovich, Sergei Tikhomirov	Centralized and decentralized Identities, KYCE, Privacy-preserving KYC – with mathematical explanation and Use cases
4.	Block Chain Technology (DLT Technique) for KYC in FinTech Domain: A Survey (2018)	Vimalkumar Pachaiyappan, R. Kasturi	Smart Contracts Sample Code, Terminology, R3 Corda
5.	If at First you Don't Succeed, Try a Decentralized KYC Platform: Will Blockchain Technology Give Corporate KYC a Second Chance? (2018)	Kevin Rutter	Corporate KYC Utilities, Examples of KYC Data Requirements, Decentralized KYC Platforms and Models, Benefits, Obstacles and Novel Challenges
6.	Decentralized KYC System (2017)	Prince Sinha, Ayush Kaul	Proposed architecture, Key generation, Sample Contracts (IPFS), Efficiency
7.	Applications of Blockchain Technology to Banking and Financial Sector in India (2017)	Reserve Bank of India	Analysis of the pros and cons, by the RBI.
8.	Applications of Blockchain Technology in Banking & Finance (2018)	Tejal Shah, Shailak Jani	Current pain points and how blockchain can help
9.	Blockchain application and outlook in the banking industry (2016)	Ye Guo, Chen Liang	Internal and external issues of the banking industry, Payment clearing system, distributed clearing mechanism, Obstacles
			in implementing blockchain technology in the banking industry, regulation.
10.	Sovrin TM : A Protocol and Token for Self-Sovereign Identity and Decentralized Trust (2018)	Sovrin Foundation	About the Sovrin Foundation and Hyperledger Indy
11.	RBI Report on Finance Systems in India (2017)	Sudarshan Sen, Nanda Dave, R. Ravikumar, A. Joseph, Sarat Kumar Malik, R. K. Sharma, Rakesh Sharma, A. P. Hota, A. S. Ramasastri, Mrutyunjay Mahapatra, Nitin Chugh, Amish Mehta, Prashant K. Seth	Centralized KYC, Syndication of loans, Aadhaar based e-KYC, Start up Company names in India and the technologies offered by them

The above table shows the comparison table consisting of Paper Title, Author Names, Year of Publication and Different Methods used and Outcomes in the research papers studied for writing this paper.

Drawbacks of 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. 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. This process consists of an exchange of documents between the customer and the financial institution that intend to work together. The process includes the collection of basic identity information like Identity Proof, Address Proof, Photo Proof and sometimes Bio metric data as well. In India, a variety of government granted documents can be provided for identification like, Passport, Aadhar Card, PAN Card, Driving License, Voter ID, etc. 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. This verification process itself is very costly for the financial institutions and may expose them to large fines if it is not conducted in accordance with the existing regulations. 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 or anti-money laundering standards and opening of current accounts. When a customer intends to open an account in a financial institution, the KYC process gets initiated. At first, both parties, the bank and the customer agree on the terms of a relationship. 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 customer has been validated or rejected and that the KYC process has been correctly conducted. Note that this process is repeated every time the customer wants to work with a new financial organization.

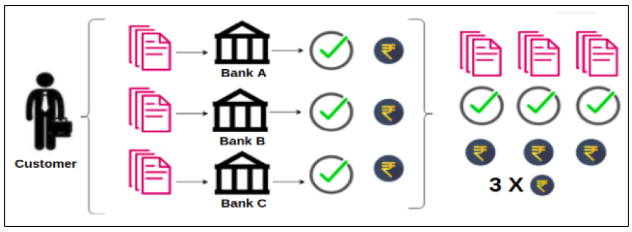

Figure 1. Current KYC Verification Process

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.

Proposed Work

A. KYC Verification Process after Implementation of Blockchain

This paper utilizes a different approach of Distributed Ledger Technology (DLT). 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. 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 above 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.

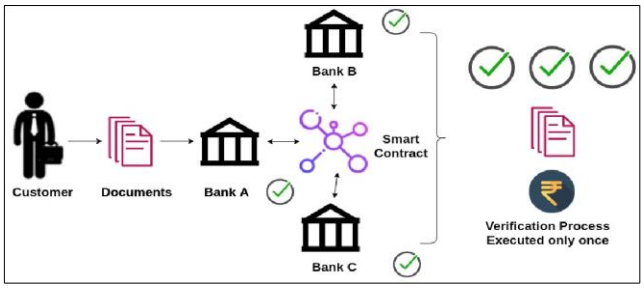

Figure 2. KYC Verification Process after implementation of blockchain

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

B. Assumptions and Conditions:

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

- First, the members of the group of financial institutions functioning in the same nation are required to follow the same KYC regulations and should concur on the same standards for permitting the core KYC verification to a customer.
- Second, all the financial institutions that fraternize in the system agree on a common, average cost for conducting the KYC process. This cost might rely on the complexity of each customer based on factors like client size, volume of documents to be exchanged, etc
- Third, it is essential to have a Government Regulator to maintain the system by approving the financial institutions so as to conduct a more efficient KYC verification process.

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.

- Proportionality Condition:

The sharing of cost of conducting the core KYC verification should be proportional across the financial institutions. This condition ensures that the costs are proportionally shared.

- Irrelevance Condition:

This condition ensures that the financial institution conducting the core KYC verification process does not have any incentive or reason to favor another institution to conduct the KYC verification process instead.

- Privacy Condition:

The privacy standards of the KYC process should be maintained as they are today. The financial institutions in the system cannot know the other financial institutions that the customer is working with, unless this information is revealed by the customer himself. This condition ensures that privacy is maintained among financial institutions.

- No – Minting Condition:

No institution can claim compensation without conducting the core process. Also, no institution can avoid paying for using the information generated by other institutions that are a member of this KYC verification network. This condition ensures that no financial institution can imitate having conducted a core KYC verification process in order to compensate for work that has not been done.

Workflow - kyc verification process

Below, we can see the general workflow of the process which actually happens. It is explained underneath in steps, for better understanding.

1. As the all the personal and official documents in this KYCModel are sovereigned by the owner itself, the customer himself sends the documents to a Government Regulator. This is an essential role as one mediator is necessary to verify the credibility of the hard copy of the documents.
2. The Government Regulator then utilizes the alreadyestablished Government portals like the Aadhar e-portal (Website - https://uidai.gov.in/) and PAN Verification portal by the Income Tax Department of India (Website – https://www.incometax indiaefiling.gov.in/e-FilingGS/Services/ VerifyYourPanDeatils.html?lang=eng). On these portals, any Aadhar or PAN Number can be verified. By just entering the ID, the website electronically generates the entire authentic, document of the customer. This system is secure because the document generated requires consent of the customer as it uses OTP for the registered mobile and the document is password protected and encrypted.

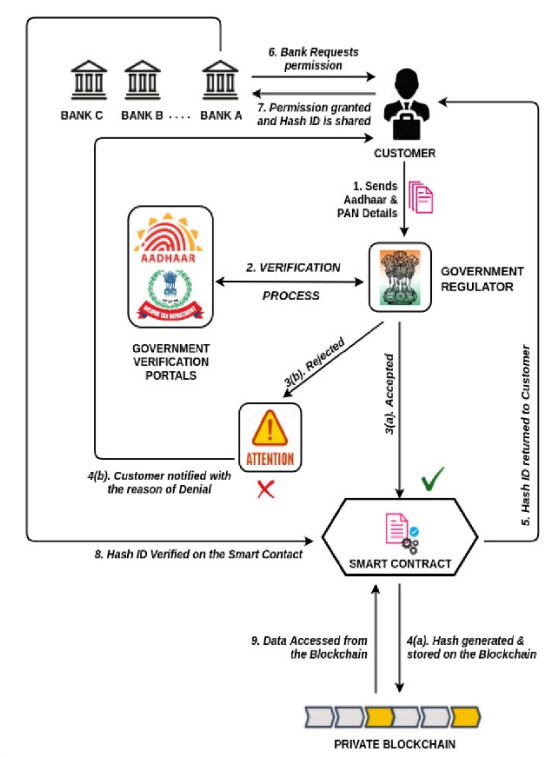

Figure 3. Workflow - KYC Verification Process

3. After the Verification process is executed, the GovernmentRegulator is provided with the results of the verification. The documents of the customer are either -

3(a) Accepted OR

3(b) Rejected

4. If accepted, the process transcends further to step 4(a) -

4(a). The core of this model – The Smart Contract undertakes the major task of generating a cryptographic hash of the Documents and storing on the blockchain. This hash value existing on the blockchain itself acts like the receipt of the authenticity of the already verified documents. Thus, the blockchain does not store the actual documents, but an alphanumeric value which is proof enough of the genuineness of the documents.

4(b). If rejected, the customer is notified the reason for denial via an email or a text message on the registered mobile number.

5. After step 4(a), once the cryptographic hash is stored on theblockchain, the same hash value is returned back to the customer. It is critical to keep this value confidential by the customer. It is this value that the customer will share in the future with the banks or financial institutions that the customer wants to work with. This step concludes the final step of the actual verification of the customer's documents.

Please note that steps 1 to 5 are undertaken only once and not multiple times for every bank the customer holds an account with. In short, till step 5, the customer's document data is stored on the blockchain. In the further steps, it will be made clear how the customer shares these documents with financial institutions.

6. Bank requests permission from the customer to view thereceipt of the authenticity of his documents already stored on the blockchain (Cryptographic Hash).
7. The customer proclaims consent to the bank to view his HashID on the blockchain by issuing his Hash ID to the bank for cross checking.
8. With the Smart Contract monitoring the process, the bankviews the Hash ID from the blockchain. Smart Contract plays an important role here by noting down the names of the institutes which are accessing the customer's data on the blockchain. This is for security of the customer's documents for cross verifying which institutes have accessed his data.

This is the detailed workflow of the KYC Verification Process. After step 8, the customer can directly share his Hash ID to number of banks. Thus, the repetitive procedure of verification by all banks for each and every customer is avoided thus, massively saving costs.

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 contact, 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 4.The components will be discussed in detail below. 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.

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. This hash includes the result of the KYC verification process, whether it was verified or rejected. 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 with a constant exchange rate against the national currency. This is a solely responsible component which actually makes the decision whether the documents provided by the customers are true or not.

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.
For the cost distribution, the architecture works as follows:

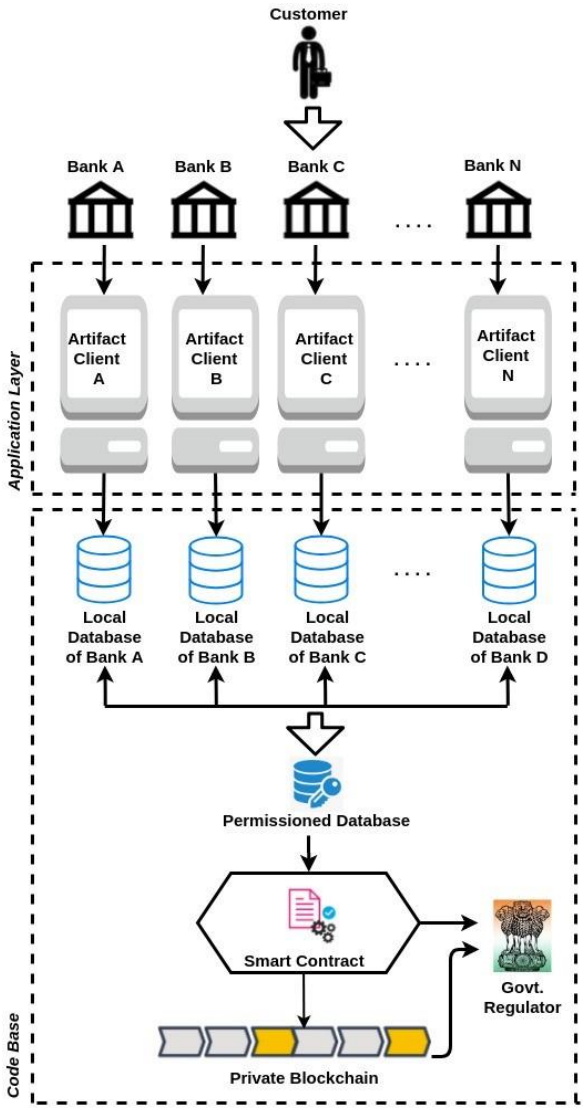

Figure 4. System Architecture

1.A certain number of financial institutions (say *n*, where $n > 3$) and the government regulator agree to implement the new KYC verification process. First, they need to set the average cost of conducting the core KYC verification process. The regulator sets up a digital token or currency with a constant exchange rate against the national currency. Thus, at this stage, a value 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 of each financial institution.
2.As soon as the customers approach a financial institution toopen 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 shareshis public key, and the KYC 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. This includes the result of the KYC verification process, whether it was verified or rejected. Additionally, the home bank stores a hash of each document used for the KYC verification on the distributed ledger.

5.Finally, the home branch creates the customer's 'DocumentPackage' 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). This document package is also stored on the bank's local database and also the permissioned database that the central regulator supervises. Note that, at this phase, only two entities, the customer and the home bank possess the documents package.

6.Additionally, the home bank creates another smart contractfor this customer which contains a list of the public keys of the wallets of the financial institutions which intend to check the KYC verification status of this customer, but only after these banks have paid their corresponding share of verification cost. This list of banks will be termed as "Onboarding Banks". This list can later be updated depending on the customer interactions with other institutions.

7.When a customer approaches other institutions than thehome 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. Additionally, the customer can grant access to this institution to view his documents from the documents package stored in the permissioned database by the home bank.

8.The new financial institution can comprehend from thesmart contract, how many other institutions have worked with this customer so far. This is a principal stage, as depending on the number of public keys of institutions listed in the smart contract, this financial institution has to pay the proportional part of verification cost. It will be described below in the next section, how this distribution of costs takes place.

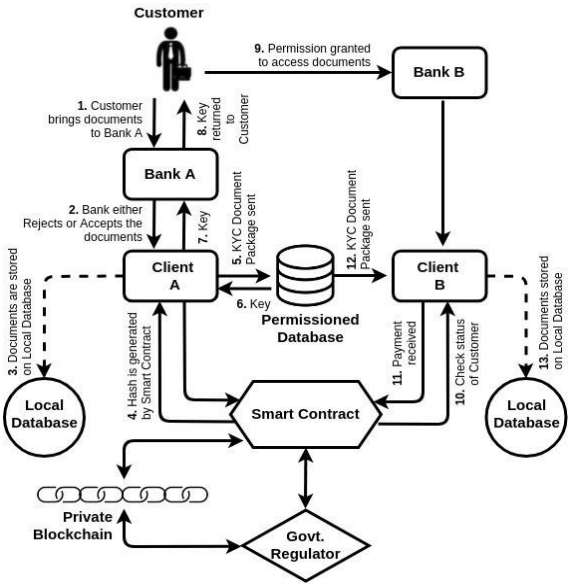

Figure 5. Cost Distribution after Verification of Documents

Mathematical Model

As mentioned in the eighth point above, for the new bank to be added to the onboarding banks list, that bank has to pay the required cost, which is equal to the equally divided verification cost. This can be formulated as follows: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 Customer 1. 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 has to pay half the amount c. Thus, we can say, the n^{th} bank will have to pay an $\frac{c}{}$ amount equal to n to the smart contract. The smart contractthen 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 withthem. So, for n number of institutes, the other $(n - 1)$ institutes $\frac{c}{}$ pay an amount of $n-1$ and receives an amount equal to $\frac{c}{n\ (n-1)}$ from the last institution to join. Consequently, the cost for each institution equals:

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

To summarize, the smart contract holds the public key of the home bank, the hash code of the documents, the certificate of approval and the "onboarded" array which lists out the public keys of all the financial

institutions that are working with the customer and have paid the proportional price of the compensation amount. This system guarantees that the core KYC process occurs only once by the first institution the customer starts working with, which is termed as home bank here. The result of the process done by that home bank can be utilized by all the financial institutions that the customer wants to work with in future. Thus, 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.

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 are have a common benefit of being modular in nature. The following platforms fall under the Hyperledger Umbrella – Fabric (used for businesses), Sawtooth (used for Supply Chain Management), Indy (used for Certification and Identity management), Iroha, Grid, Burrow and the newest platforms Besu and Aries. All these platforms differ in the consensus mechanisms, permissions and other protocols. Other blockchain development platforms that have been developed over the years are r3 Corda (used for enforcing business agreements between trading partners), Hedera Hashgraph (Public ledger for decentralised applications) and Quorum (designed for enterprise agreements) and so many more. Out of all these, Hypeledger Fabric is a stable and widely accepted framework for blockchain development

Advantages And Disadvantages

Advantages and disadvantages of this system are listed as below:

A. Advantages:

- 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 [12].
- 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. *B. Disadvantages:*
- The main disadvantage of blockchain is its high energy consumption. In efforts to validate the transactions, the 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 [1][4][5].
- 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].
- 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% Attack' [1] [4].
- It is much more difficult to design and develop a secure blockchain system than a similar centralized system.

Challenges

A. Popularity:

If we observe the news these days, it is Bitcoin and other popular cryptocurrency which steal most of the headlines today. But it is an unquestionable fact that blockchain as a technology and a framework is growing exponentially, both, in the usage and legitimacy [20]. People generally relate blockchain to bitcoin and its objectionable status in most countries, and therefore flag the technology itself as inappropriate or disagreeable. Every emergent technology faces challenges before complete acceptance by the community. Blockchain can be analogous to the internet, which also faced acceptance problems in its early days in 1996 when it was launched. Just like email is one application or product of the internet, cryptocurrency is just one aspect of the blockchain

technology. Internet today has innumerable applications or products, which are beneficial to mankind. Similarly, the characteristics offered by blockchain are rapidly gaining popularity in programming community. Various prestigious companies are supporting blockchain development. Common examples include – The Linux Foundation, IBM, Accenture, Tech Mahindra, and so on. Their growing blockchain programming requirement is evident on job portals where we can see their massive job openings for Blockchain Developers, Blockchain Architects and Blockchain Analysts. In due time, with the growing success of blockchain, people will realize the potential of blockchain, and soon enough, blockchain will be a part of our day-to-day lives just like Internet. The Government of Estonia - a small country from Northern Europe, has already accepted blockchain for the digitization of their data [21]. All their Identity Documents, Proof of Birth Date, Proof of Address, Social Security Number exist digitally on their govenment blockchain.

B. Scalability:

Blockchain scalability can be further divided as Node Scalability and Performance Scalability. As far as node scalability is concerned, the blockchain scales relatively well. In fact, more the number of nodes, more secure is the network. Performance Scalability is the total number of transactions per second which defines the latency of the network. In the case of Bitcoin, the performance scalability is very limited as the average throughput is only approximately 7 transactions per second [4].

Many blockchain scalability solutions have been introduced over the years, broadly classified as Layer 1 and Layer 2 solutions [22]. Layer 1 (a.k.a On-Chain) scalability is achieved when the core processes and components are improved. This introduces us to a new concept of Sharding, which is nothing but dividing the network into smaller groups (shards) without compromising on the network's security and decentralization so as to achieve unlimited scalability. In this case, each group or shard acts as small blockchain in itself and all shards can be operated in parallel. Random validators confirm the transactions whereas the main blockchain just stores the reference of valid state of each shard. Ethereum is based on Proof of Work (PoW) consensus mechanism as sharding with Proof of Stake (PoS) consensus algorithm is not secure. Layer 2 (a.k.a off-Chain) scalability is achieved when independent solutions on top of the existing infrastructure is implemented to solve specific issues. This does not improve the original blockchain. This kind of solution secures the main Ethereum blockchain and promises scalability by allowing transaction off the chain. This introduces us to Plasma which is a framework presented by Joseph Poon and Vitalik Buterin and was published in a paper in August 2017 [22]. Plasma is not a protocol but a design pattern or a technique, which is composed by two parts — the Plasma Root Chain (Ethereum) and the Child Chains. The children chains will have a different consensus mechanism such as Proof of Authority or Proof of Stake. Root Chain has a smart contract which knows all the state transition rules in the Child Chains. It is vital to be noted that plasma specification is evolving and still under development.

C. Interoperability:

The dictionary meaning of the word "interoperability" means, "the the ability of computer systems or software to exchange and make use of information". In context with blockchain, interoperability deals with the fluent and uninterrupted sharing of data across 'different types' of blockchain. How blockchains differ across themselves depends upon the way they have been built. The beauty of the blockchain technology is that, you can tweak the original protocols implemented in 'Bitcoin' as per your need. For example, Bitcoin uses Proof of Work consensus algorithm for mining purpose. However, Ethereum is planning to shift from Proof of Work to another consensus algorithm called Proof of Stake in the year 2020 [4]. The reason behind this being, Proof of Work utilizes immense computational power which results in utter waste of resources. Proof of Stake overcomes this drawback. More details apart, the conclusion here is, though blockchain offers this property to customize the protocols depending on our convenience, it is not that easy to transfer data from one blockchain to another. For example, if a person wants to exchange some Bitcoin for some Ether, he will most probably end up on a platform which is centralized, having a mediator in between. This is because both blockchains use different consensus algorithms as mentioned above.

This was about the cryptocurrency applications of blockchain. In case of blockchain as a coding platform, there are different frameworks like Ethereum, Hyperledger Fabric, r3 Corda, Hyperledger Indy, and so on and so forth. Most platforms offered by Hyperledger are modular in nature. So if anyone intends to reuse the framework between different public blockchains (say, Fabric and Aries), interoperability is an issue because of the same aforementioned reasons. Now, lets consider blockchain as a singular store of data of documents of individuals, for our model of KYC verification. Here, interoperability cannot be seen as an issue, because, the blockchain here in picture is singular in number. We are not importing, nor do we need data from another blockchain as we are creating our new blockchain here after verifying the credibility of the documents before putting the data on our blockchain. This blockchain does not have to deal with protocols, consensus algorithms, mining rewards or transaction costs of other blockchains, hence interoperability issues are not encountered in this model.

Conclusion

This paper has 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 paper 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.

References

[1]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," www.bitcoin.org, p. 9,2008.

[2]. José Parra Moyano, Omri Ross, "KYC Optimization Using Distributed Ledger Technology" 2017, SSRN Electronic Journal, 15 November 2017,DOI:10.2139/ssrn.2897788

[3]. https://economictimes.indiatimes.com/news/economy/policy/rbi- imposes-rs50-lakh-fine-on-pnb-for-delay-in-reporting-fraud-in-kingfisher-airlines-account/articleshow/70511380.cms?from=mdr

[4]. Andreas M. Antonopoulos. 2014. Mastering Bitcoin: Unlocking DigitalCrypto-Currencies (1st ed.). O'Reilly Media, Inc.https://bitcoin.org/en/

[5]. Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin,Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, GariSingh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, Jason Yellick, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains", 17 April 2018, https://arxiv.org/pdf/1801.10228.pdf https://hyperledger.github.io/composer/v0.19/installing/installing-prereqshttps://unbounded.network/

[6]. Sovrin Foundation, "Sovrin TM : A Protocol and Token for Self- SovereignIdentity and Decentralized Trust", 2018, White Paper from the Sovrin Foundation Version 1.0 January2018

[7]. Chainworks Digital LLP, "Know Your Customer - Decentralized Secure Sharing Protocol on Quorum", 2019, Third Workshop on Blockchain Technologies and its Applications, Information Security Research & Development Centre (ISRDC) Department of Computer Science and Engineering IIT BOMBAY, February 04 – 07,2019

[8]. Alex Biryukov, Dmitry Khovratovich, Sergei Tikhomirov, "Privacypreserving KYC on Ethereum ", 2018, W. Prinz & P. Hoschka (Eds.), Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies (ISSN 2510-2591), DOI: 10.18420/blockchain2018 09

[9]. Vimalkumar Pachaiyappan, R. Kasturi, "Block Chain Technology (DLTTechnique) for KYC in FinTech Domain: A Survey", 2018, International Journal of Pure and Applied Mathematics, Volume 119 No. 10 2108, 259-265 ISSN: 1311-8080 (printed version); ISSN: 1314- 3395

[10]. Kevin Rutter, "If at First you Don't Succeed, Try a Decentralized KYCPlatform: Will Blockchain Technology Give Corporate KYC a Second Chance? ", 2018, R3 Corda White Paper, July2018

[11]. Prince Sinha, Ayush Kaul, "Decentralized KYC System", 2017, InternationalResearch Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056, p-ISSN: 2395-0072

[12]. Reserve Bank of India, "Applications of Blockchain Technology to Bankingand Financial Sector in India", 2017, Institute for Development and Research in Banking Technology(IDRBT)

[13]. Tejal Shah, Shailak Jani, "Applications of Blockchain Technology inBanking & Finance", 2018, 86651.

[14]. https://doi.org/10.13140/RG.2.2.35237.96489

[15]. Ye Guo, Chen Liang, "Blockchain application and outlook in the bankingindustry", 2016, Financial Innovation (2016) 2:24, DOI 10.1186/s40854-0160034-9

[16]. Sovrin Foundation, "Sovrin TM : A Protocol and Token for Self- SovereignIdentity and Decentralized Trust", 2018, White Paper from the Sovrin Foundation Version 1.0 January2018

[17]. Sudarshan Sen, Nanda Dave, R. Ravikumar, A. Joseph, Sarat Kumar Malik, R. K. Sharma, Rakesh Sharma, A. P. Hota, A. S. Ramasastri, Mrutyunjay Mahapatra, Nitin Chugh, Amish Mehta, Prashant K. Seth, "RBI Report on Finance

[18]. Systems in India", 2017, November, Reserve Bank of India, Central Office,Mumbai

[19]. Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander, "Where Is Current Research on Blockchain Technology?— A Systematic Review", 2016, PLOS ONE DOI: 10.1371/ journal.pone. 0163477

[20]. "Estonia – the Digital Republic Secured by Blockchain", © 2019 AktsiaseltsPricewaterhouse Coopers.

[21]. Joseph Poon, Vitalik Buterin, "Plasma: Scalable Autonomous SmartContracts", August 2017