Application of Blockchain in KYC Compliance

Shashank R. B., Chirag Chhabra, and Nagaraj G. Cholli

Abstract—The current process of Know Your Customer (KYC) used by banks is time-consuming, expensive, and redundant in practice. A Thomson Reuters Research states that while banks globally spend around 60 million USD on an average, this number may go up to 500 million USD for some banks [1]. Hence, to improve the efficiency of this process, the use of a blockchain-based mechanism is suggested. The use of smart contracts also provides scope for adding features that cannot be achieved by the current process. The paper majorly discusses the advantages and disadvantages of using blockchain for performing KYC processes.

Index Terms—Blockchain, KYC, Smart Contracts, Smart-KYC.

I. INTRODUCTION

Blockchain is the latest technology to take up the world by storm. Its most successful application, namely Bitcoin has time and again proved its security capabilities with the bitcoin network not getting hacked in 12 years of its inception, despite being a public network and having a bounty of approx. 250 million USD. Blockchain is just a chain of blocks linked together secured using cryptography, which contains the information of the transaction, the participants involved in the transaction, and the hash, which connects the previous block to the current block. By connecting blockchain-based applications, to smart contracts, there is significant improvement in the effectiveness and security of the current systems, which thus lessens the general expenses for organizations. A person's identity can be confirmed without much of a stretch by official records, for example, drivers’ licenses, passports or social security cards. Be that as it may, building up a validation factor of other recognizable proof sources bears a significant test for regulators. Blemishes in the security of such systems has prompted regular instances of monetary extortion and illegal tax avoidance. Setting up KYC (Know Your Customer) processes inside an association is a required, dreary technique. A lot of administrative work is done related with such methods, an absence of transparency in regards to the utilization of the individual information that is gathered from clients has prompted wasteful aspects in examining novel mechanisms. The advantages of blockchain include transparency, real-time tracking, immutability, security, and cost reduction compared to traditional approaches to the same applications. Blockchain will take into consideration, the gathering of information from various authority service providers into one single, cryptographically secure database. KYC validation through this sort of design can be quicker, more secure and more effective than current validation systems.

II. LITERATURE SURVEY

A. Paper: [2]
Type of Blockchain: Private
Regulation Compliant to Countries: India
Revocation of Access: No Provision
Consensus Algorithm: Proof of Concept

Key Takeaways:

a. When a user wants to deactivate his/her account, there is no proper solution provided. The KYC stored is a case of wasted memory as block is immutable.
b. Suppose a case where a bank fraudulently accepts an invalid KYC, and another bank uses it and a financial crime happens, who is to blame or hold liable?
c. What if a client’s phone is hacked by a rival bank and KYC approval is initiated? An approach to solve this could be: signing with private key by user should be done.
d. The approach in the paper doesn't describe anything about mining of the blockchain and the conditions for a block to be valid.
e. The suggested method utilizes the smart contracts to validate the KYC via Aadhar/PAN API’s.

B. Paper: [3]
Type of Blockchain: Permissioned
Regulation Compliant to Countries: American Union
Revocation of Access: Provides revoke access but doesn’t explain how
Consensus Algorithm: Not mentioned

Key Takeaways:

a. The paper suggests the use of access control systems to provide different levels of KYC related information to third parties.
b. Instead of storing the document itself, it proposes to store the hashes of KYC on chain.
c. The method initially accesses the government database to check the identity of individuals, and verify if they are prohibited from availing any financial services.
d. To prevent the duplication of data when customer registers with two different banks, can be provided by adding an IsVerified bool data structure in the block which is associated with the unique id of the individual.
e. Addresses the revocation of access to KYC in case the user no longer wishes to share it.

C. Paper: [4]
Type of Blockchain: Permissioned
Regulation Compliant to Countries: Singapore
Revocation of Access: Provides revoke access by generating new AES keys every time a customer revokes access for the bank whose access has been revoked
Consensus Algorithm: Proof of Concept
Key Takeaways:
  a. Since storage of confidential information is done, the paper leans towards the use of a permissioned blockchain.
  b. Advocates to make the relationship between a customer and the banks anonymous when a third party tries to access the KYC information from the bank that approved the KYC by using a pseudonym allotted by a PKI.
  c. An approach that paper suggests is that KYC documents be encrypted with a symmetric key, which in turn is encrypted by the initial KYC validating bank public key.
  d. Proposes the use of a consent record off-chain which is in turn linked to the blockchain, so as to ensure banks no longer have access to a user's KYC if he/she wishes so.
  e. A working mechanism should be devised to ensure that regulators are not exempted from information, if the relationship between the banks and customers are anonymized for third-parties.

D. Paper: [5]
Type of Blockchain: Multichain
Regulation Compliant to Countries: Luxembourg
Revocation of Access: No provision
Consensus Algorithm: Proof of Work
Key Takeaways:
  a. The paper proposes the use of multichain, which is a permission blockchain, so as to allot varying levels of permissions to different banks.
  b. The paper utilizes a consensus mechanism over other mechanisms due to its scalable nature and extreme resistance to 51% attacks when scaled.
  c. Using Grid5000 testbed platform, the blockchain nodes were distributed geographically to various locations to ensure real life simulation of a blockchain.
  d. Being decentralized, the paper proposes the use of IPFS to store the documents off-chain and hence not being vulnerable to single point of failure.

E. Paper: [6]
Type of Blockchain: Private
Regulation Compliant to Countries: India
Revocation of Access: No provision
Consensus Algorithm: Proof of Concept
Key Takeaways:
  a. There is absence of mechanism to ensure if a user tries to upload his/her own KYC but mistypes the number, and it turns out to be a valid number, but not of the user.
  b. Since retrieval time includes decompression time, the time taken to retrieve is greater than the time taken to input into blockchain.
  c. Gas usage (Gas alludes to the cost important to play out an exchange on the system. Miners set the cost of gas and can decline to process an exchange in the event that it doesn't meet their value) to be paid to miners is also less in case of decompression when compared to compression as compressed data is less in size.
  d. The need for compression and decompression will not arise, if we store documents off-chain and the hash of the documents on-chain. The resulting blockchain will be blazing speed.
  e. The paper utilizes an AES symmetric algorithm which is used to encrypt KYC data, but what if symmetric encryption is used and the application is hacked (as KYC server is the other party that contains the symmetric key). An approach to solve this could be: use asymmetric encryption.

III. BLOCKCHAIN FOR KYC

A. Advantages
a. Blockchain-based KYC utilities give individuals more control over their identity than traditional methods, that is self-sovereign identity.

b. Automation and standardization of operations: Considering the continuous progression achieved on KYC procedure regulation and the ever-growing data being assembled, it is presently feasible for blockchain to utilize smart contracts for the execution of control and operational procedures. KYC workflow can be coded into smart contracts and institutionalized over the business, along these lines streamlining the methodology.

c. Communication and Transparency: Blockchain-based KYC stages will null over the dynamic seeing of everything from account openings to ordinary trades. At the point when joined with smart contracts that are related with fated criteria to spot bogus development and these new stages will have the alternative to make banks mindful of any awful practices.

d. Suspicious Activity Reporting: In present day, the banking KYC process takes days or even weeks. Along these lines, the cost realized by money related foundations in keeping up regulatory consistence is rising rapidly as the business endeavors to stay before budgetary fraudsters or dread based oppressors. With a mutual record, where different monetary establishments are keeping up the record, the methodology of KYC could be conveniently adjusted and checked by all social events. Any change or update to a client's data would be open to all gatherings.

B. Disadvantages
a. Trusted Parties: The trust factor in blockchain takes into account that the officials inserting data into the blockchain are doing it with due diligence. If the
participating banks collude to add falsified information on the blockchain, then it is of no use.

b. Privacy: As blockchain is immutable, it would be challenging to realize the option to be forgotten once the association with a particular bank is over.

c. Standardization of the processes: Since banks are spread all across the world, the usage of blockchain will be more efficient, but since each country has its own regulations, it would be tough to implement a standardized procedure for the same.

d. Liability: If a bank uploads an illegitimate KYC on the blockchain and the same is used by another bank, once the account with the false KYC is involved in an illegal transaction, laws as to who should be accounted for are not defined.

IV. SMART KYC

We have surveyed five eminent IEEE papers related to the topic and have come up with comparisons to the ideas suggested and their key takeaways. In the subsequent section of the paper, we have come up with an improved mechanism (Smart-KYC) that addresses some of the limitations of the five papers taken into comparison.

A. Structure of the Block

The contents of the block are as shown in the figure. The actual KYC documents are stored off-chain, and the hashes are stored on-chain to prevent bloating of the network. It also contains the public keys of the bank who have been granted access to the KYC and a nonce to induce randomness. Each block is signed with the private key of the individual, and hence until the private key is manipulated, his KYC documents are secured from misuse.

![Fig. 1. Structure of the Block](image)

B. Smart Contracts

Smart contracts are bits of code that self-enforces a contract digitally without the reliance of a trusted third party. With the usage of smart contracts, the KYC access can be revoked if the user wishes to have a predefined short-term relationship with the bank.

V. MECHANISM

Fig. 2 describes the process of performing KYC using blockchain, which follows:

1. The user uploads his valid documents to the bank to become KYC compliant on the bank portal. The bank portal meanwhile generates the private key for the respective documents algorithmically for the user.
2. Bank first checks whether the user is on the list of persons blacklisted by the government from accessing banking services.
3. The bank verifies the documents and, if legitimate, submits a transaction to append the hash of the KYC document on the blockchain.
4. Participating banks can form a consensus on the KYC done whether the above transaction is legitimate or not, which similar to the proof of work mechanism. For a KYC to be legitimate, more than 51% of the banks need to approve in favor of it. A rating system can be put in place to discourage malpractice.
5. The actual KYC document is stored in the InterPlanety File System (IPFS), therefore off-chain. IPFS leverages cryptographic hashes to store the records, and access control can be controlled using smart contracts.
6. Each time a third party wants to access the details of the KYC, it can do so by requesting read-only access of the completed KYC via an API.
7. The user can grant access by signing the request with his private key which is updated on the blockchain.
8. Customer can revoke access to his identity to a bank which in turn generates a new hash for the bank with the updated list of KYCs accessible to a bank on the blockchain. The bank has access to only the latest list which ensures that it no longer has access to revoked documents.

![Fig. 2. Mechanism used in Smart KYC.](image)

VI. FUTURE CHALLENGES

The challenge here is to devise a mechanism according to Indian laws and regulations (since only two of the five papers are of Indian context but they don’t take rules and regulations into consideration) which are beyond the scope of this paper. In addition, laws must be devised as to who is responsible in case a bank uses the KYC details that were wrongly verified by another bank and a financial crime is committed by the client. Moreover, regulatory watchdogs must also keep a sharp watch on the participating banks so as to prevent collusion and insider trading of customer’s confidential documents.
VII. CONCLUSION

To increase the efficiency of the current banking procedures in the KYC of clients, blockchain can be a solution. Its inherent properties of immutability, security and decentralization can lead to prevention of redundancies in the existing process. From the five papers surveyed, we have found the procedures of [3] to be the best when compared to others as it addresses the challenges of revocation of access of the KYC data. Moreover, [6] shows the fact that the usage of compression and encryption of the KYC data can lead to optimization of the blockchain [4] suggests a mechanism to anonymize the relationship of banks with users but this cannot be extrapolated to all countries since each one has varying privacy laws. But since the blockchain industry is very novel as a whole, it is unpredictable as to how sustainable are these approaches when implemented in the real world as we have only simulations available at present. An increase in the adoption and education of the masses about blockchain technology will go a long way in improving the bridge between the blockchain and finance industry. Only then, we could see the use of blockchain being streamlined into the current mechanisms of KYC validation.

ACKNOWLEDGMENT

We are indebted to our guide, Dr. Nagaraj G. Cholli, Associate Professor, Department of Information Science and Engineering for his wholehearted support, suggestions and invaluable advice throughout our project work and also helped in the preparation of this thesis. Our sincere thanks to Dr. B.M. Sagar, Associate Professor and Head, Department of Information Science and Engineering, RVCE for his support and encouragement. We express sincere gratitude to our beloved Principal, Dr. K. N. Subramanya for his motivation towards this project work. We thank all the teaching staff and technical staff of Information Science and Engineering department, RVCE for their help.

REFERENCES