International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

TRANSPARENT KYC MECHANISM AND SMART SECURE DOCUMENT MANAGEMENT FOR BANKING USING IPFS AND BLOCKCHAIN TECHNOLOGY

Tanishq Walzade[1], Sumesh Shaji[2], Prof. S. B. Patil[3] , Ashwini Naik[4], Aishwarya Sutare[5]

Department of Computer Engineering
Jawahar Education Society's, Institute of Technology, Management and Research, Nashik

---

Abstract - The know your customer or know your client (KYC) is guideline for the banking system to validate customer using identity, appropriateness, risk assessment in establishing banking relationship. With the growing concern of security, the KYC process is complex and involves high cost for completing for single customer. In this work, we propose an economical, swift, secure, and transparent platform for KYC document verification for the banking system through user portal, Interplanetary File System (IPFS) and parts of blockchain technology. The proposed system allows customer to register on user portal, generate has value, visit said bank with original set of documents for verification and complete the KYC process. Upon receiving the private key, any Bank/financial organization can retrieve, store customer data (i.e. KYC) securely using IPFS network if the customer wishes to open another account in that Bank/financial organization. The proposed system can save time, money, and repetitive work during the KYC process when someone tries to open an account at multiple banks.

***Key Words*:** Blockchain Technology, KYC, IPFS, User-Portal, Decentralization, SHA-256, P2P, DLT

I. INTRODUCTION

The Know your customer (KYC) is very common term in the banking and financial sector. At this moment, the manual KYC process is outdated and has become necessity to automate the KYC verification process. Studies around the world have made several attempts to make better verification process for KYC. Many academics tried to propose Blockchain-based solution. Blockchain technology recently draws the attention of the public, as dispute that leads to the foundation that the trust-free economical transaction is possible with its distinctive method [2].

The blockchain permits unnamed and secure transactions of virtual currencies (such as Bitcoin, Litecoin, etc) and saves the metadata regarding the transaction details in database. The database is secured and impede the alteration in the transaction history by cryptography techniques. The legitimate user can write to the file using the private key. In banking, blockchain is safe and can reduce processing/transaction costs considerably. The banks or other financial organizations such as insurance industries maintain diverse policies and require multi-steps processing between parties. Besides, these require a secure transaction, short processing/settlement time. To facilitate these concerns, the researcher has proposed various distributed platforms. Raikwar et al. [3] proposed blockchain based distributed platform for financial transaction processing in insurance industry. Puthal et al. [4] introduced decentralized framework using blockchain which allows sharing and integration of all distributed actors. This will help industry to analyze the spread and plan further development [5]. Ever since Satoshi Nakamoto exited the scene and handed over Bitcoin development to other core developers, the digital ledger technology has evolved resulting in new applications that make up the blockchain History.

Nakamoto [6] proposed e-transaction system of coin produced using digital signatures. The system is able to track the transaction history, and it can prevent double spending problem. Since then, researchers are trying to find the potential sectors to apply the Blockchain. Nevertheless, sharing transaction information over bitcoin in costly. Currently, miners are charging around $7 per 100 KB of data [7].

The uses' KYC documents cannot be uploaded to the Blockchain network as it will be expensive. Thus, as an alternative solution, KYC documents sharing using the Interplanetary File System (IPFS) is proposed in this paper, and then documents are shared over the Blockchain network. The IPFS is shared dispersed document framework that looks to associate all registering computing devices with similar system of files [8]. User can store their transaction history and hash to the IPFS network, and then stare it to the Blockchain network when required. This process will reduce the blockchain data size significantly [9].

The rest of the article is written as follow- section II depicted the literature review, section III discussed technologies used to formulate the framework: Section IV proposed framework. Section and section VI talked about the result section and conclusion respectively.

II. LITERATURE REVIEW

The KYC verification process is an integral part of regulation for the financial industry [10]. The KYC process is started when client wants financial transaction with financial institution to begin [11]. Arasa et al. [12] direct an investigation of the expense of KYC dependent on the complexity level of the compliance required for the instance of business banks in Kenya, building up to four variables that clarify 78.3% of the consistence necessities. The data around us is increasing day by day, including the KYC documents. Soni and Duggal [13], proposed solution using big data analytic techniques to solve the big data problem of KYC focused on Indian banks.

Abdullah Al Mamun, Sheikh Riad Hasan, Md Salahuddin Bhuiyan, M. Shamim Kaiser and Mohammad Abu Yousu [1] proposed to implement concept of blockchain in banking sector using IPFS. Based on that approach we understood and implemented and enhanced this concept further to improve banking sector.

Y. Lootsma et al. [14] proposed to implement the Regtech (regulatory technology) like Blockchain in the banking sector to reduce the burden of the KYC process for financial institution as well as the regulatory institution. Using the approach tax reporting can also be done. However, they did not show the full implementation of Blockchain and the cost involved with the process.

When client wants to do the financial transaction through payment provider, they will check the customer identity by his name from bank if the provided information is correct through Blockchain smart contract [15]. The author provided an assumption on using the blockchain to make the identity and financial transaction through blockchain, though they did not provide any use case for document sharing like KYC docs.

A typical KYC framework could be that client goes to bank, the bank performs KYC, stores KYC in the Blockchain, give customer token and then customer give access to another bank to check the KYC information. The other bank then crosschecks the information from Blockchain [16].

Because of range of configuration parameters, the blockchain is somewhat uncontrollable. For example, testnets like Rinkby, Ethereum cannot be adjusted easily because of their parameters like Gas limit, Mining difficulty and so on. Authors suggested using Grid'5000, as they found it highly controllable and reconfigurable testbed. Again, the authors did not provide practical use case scenario with cost calculation.

J. Parra Moyano et al. [12] has shown the design of centralized and decentralized Blockchain KYC solution with the division of processing cost among different banks. To minimize the cost of core KYC verification and improve the customer experience, they proposed new scheme based on distributed ledger technology (DLT). They Focused on four main points. The first is proportionality: the cost will be shared proportionally by all the institutions involved with particular KYC verification process. They focused on irrelevance secondly. The one who avoids the KYC process will not get any incentive. The third point of focus was Privacy. The KYC verification process has to be secured so that user privacy is not violated. Finally, they focused on No-minting. As the process is online-based, they need to focus that no false can be made during KYC verification. Whenever someone tries to edit any portion of KYC data, that editing process will automatically be void from the authoritative side. Their proposal was much effective except few problems, which are as follows:

- The block data size will increase over time, and hence the cost involving it.
- If customer open account only at single bank, then the whole cost has to bear by that bank.

III. BACKGROUND TECHNOLOGIES

A. BLOCKCHAIN

Blockchain is purely peer-to-peer version online transaction, where customer directly sends money to others without the help of financial organization. All transactions will be hashed to an ongoing proof-of-work chain. Each of this called block; the running block contains the hash of previous all blocks. Therefore, the whole process is tempered proof, as single peer cannot add new block without the proof-of-work [6]. Bitcoin was the first fully decentralized cryptocurrency. While the central purpose of DLT was to create digital money and sending and receiving via the Internet, the technology can also be used to authenticate online document sharing using smart contracts. The smart-contract aims to involve them in properties, which are expensive and controlled in digital manner [17]. The European Security and Markets Authority [18], dis- cussed the possible benefits, challenges to those benefits and limitations of DLT applied to the security market. While they only focused on the security market, they provide guideline to apply the DLT in another financial sector like Bank.

B. IPFS

The Interplanetary File System (IPFS) is peer-to-peer(P2P) file-sharing protocol connecting computing devices for sharing/storing files/data. The content is uniquely recognized in the global namespace using the hash code of the file. If the hash code is altered, the data cannot be verified which will be identified by IPFS. Besides, IPFS identifies duplication if files with the same content are stored. Among many, AFS [19] has succeeded widely and still used by many today. Most especially, Napster, LimeWire, Gnutella, KaZaA, and BitTorrent are unstructured distributed P2P file/content-sharing protocol used by more than 100 million 100 million concurrent

users. In other way, IPFS follows client-server model which pointed out how do we access the web [20].

C. SHA-256

SHA-256 stands for Secure Hash Algorithm 256-bit and it's used for cryptographic security.

Cryptographic hash algorithms produce irreversible and unique hashes. The larger the number of possible hashes, the smaller the chance that two values will create the same hash.

SHA 256 is a part of the SHA 2 family of algorithms, where SHA stands for Secure Hash Algorithm. Published in 2001, it was a joint effort between the NSA and NIST to introduce a successor to the SHA 1 family, which was slowly losing strength against brute force attacks.

The significance of the 256 in the name stands for the final hash digest value, i.e. irrespective of the size of plaintext/cleartext, the hash value will always be 256 bits

D. P2P:

A peer-to-peer network is designed around the notion of equal peer nodes simultaneously functioning as both "clients" and "servers" to the other nodes on the network. This model of network arrangement differs from the client–server model where communication is usually to and from a central server. A typical example of a file transfer that uses the client-server model is the File Transfer Protocol (FTP) service in which the client and server programs are distinct: the clients initiate the transfer, and the servers satisfy these requests.

E. DLT:

Distributed ledger technology (DLT) is the technological infrastructure and protocols that allow simultaneous access, validation, and record updating across a networked database. DLT is the technology blockchains are created from, and the infrastructure allows users to view any changes and who made them, reduces the need to audit data, ensures data is reliable, and only provides access to those that need it.

IV. Motivation

We were motivated to work on this project when we ourselves faced issue of doing physical KYC process each and every time when opening account in different bank. We thought that automating things will make it easier for customer as well as people working in banking sector. Aims to be accomplished in our project are as follows: We propose a solution based on Blockchain technology, which reduce the traditional KYC verification process cost. The Major addition to it is that the whole verification process is conducted only once for each customer, irrespective of the number of institutions they register and thereby increasing the transparency by securely sharing the results through DLT. This approach involves proof of concept (POC) with Ethereum. This process reduces cost overhead, improved customer experience and increases transparency. The 'Know Your Customer' process, also known as KYC, which helps the institution to verify identity of client. KYC is a Regulatory and legal requirement that must be fulfilled by the companies or financial institutions for both new and existing clients.

V. METHODS

A. Existing System Design

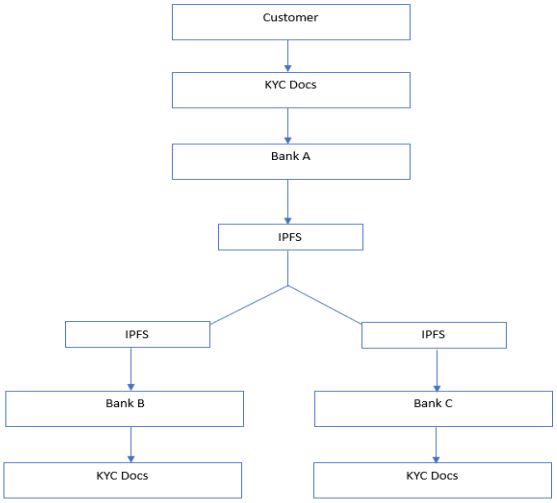

Fig -1: Architecture of Existing System

Drawbacks:

- User does not have control over their data/documents.
- High complexity due to Gpg4win
- Works only using hash-value, verification cannot be done by uploading physical documents.
- No Fund Transfer limit.
- Bank portal not elaborated.

B. Proposed System Design

In our proposed system we are sharing KYC documents with blockchain, so user document and details keep safe and secure.

In above architecture we can see we have created one secure IPFS system so user here kept their documents and details.

In Second part when user required to done transaction from one bank to other bank that time our system will help to provide easy KYC to send amount easily and securely.

In Diagram we can see there is strong security algorithm so on one side we are doing encryption and other side doing decryption.

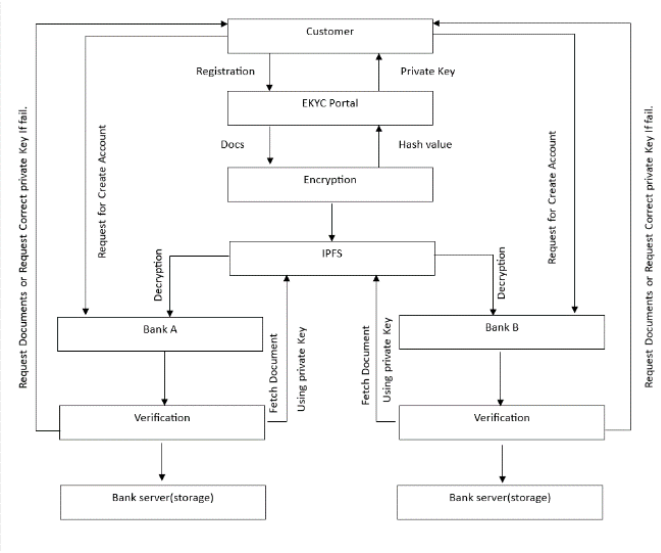

Fig -2: Architecture of EKYC

VI. CONCLUSIONS

Our project is prototype of this concept, as blockchain cannot be implemented in such short time we have illustrated how this concept can work in future on a huge scale Blockchains represent the future of transactions and are beginning to transform entire industries. Consequently, there is considerable interest in exploring blockchains for various industry use cases. They are particularly useful in supporting multi-party business transactions where the entities need not trust each other. The immutable, cryptographically secured, and replicated, ledger, consensus to validate transactions, and permissioned access are all attractive salient attributes for enterprises to consider blockchains as the future transaction network.

VII. FUTURE SCOPE

Our concept can be further extended in various aspects when blockchain will become cheaper and easy to use as compared to today with help of RBI and government. When bitcoin/ any other cryptocurrency will be made a legal tender in India such type of virtual currency can also be transferred using our suggested platform.[1]

REFERENCES

[1]Abdullah Al Mamun, Sheikh Riad Hasan, Md Salahuddin Bhuiyan, M. Shamim Kaiser and Mohammad Abu Yousuf “Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology” 2020 IEEE Region 10 Symposium (TENSYMP), 5-7 June 2020, IEEE, 2020.

[2] A. Rahman, S. Roy, M. S. Kaiser, and M. S. Islam, "A lightweight multi-tier s-matt framework to secure communication between low-end iot nodes." in 2018 5th International Conference on Networking, Systems and Security (NSvsS), 2018, pp. 1-6.

[3] M. Raikwar, S. Mazumdar, S. Rui. S. Sengupta, A. Chattopadhyay, and K.-Y. Lam, *A Blockchain Framework for Insurance Processes." 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018.

[4] D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as a Decentralized Security Framework [Future Directions],"IEEE Consumer Electronics Magazine. vol. 7, pp. 18-21, 2018.

[5] M. Mahmud, M. S. Kaiser,M. M. Rahman, M. A. Rahman, A. Shabut, S. Al-Mamun, and A. Hussain, "A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based loT Framework for Neuroscience Applications," Cognitive Computation, vol. 10, по. 5, pp. 864-873, Oct. 2018. [Online]. Available: https://doi.org/10.1007/12559-018-9543-3

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronie Cash System," 2010, library Catalog: bitcoin.org. Online|. Available: https://bitcoin.org/en/ bitcom-paper

[7] D.Tonin, Money Button CEO: How[O upload large files to Bitcoin SV blockchain," Mar. 2019, library Catalog: coingeek.com Section: Tech. Online]. Available: https://coingeek.com/ money-button-ceo-how-to-upload-large-files-to-bitcoin-sv-blockchain/ Mar. 2019, library Catalog: coingeek.com Section: Tech. Online]. Available: https://coingeek.com/ money-button-ceo-how-to-upload-large-files-to-bitcoin-sv-blockchain/

[8] J. Benet, "Ipfs - content addressed, versioned, p2p file system." arXiv: CSNI, vol. 1407.3561, 2014.

[9] Q. Zheng, Y. Li. P. Chen, and X. Dong. "An innovative ipfs-based storage model for blockchain," in 2018 IEEE/WIC/ACM ICWI, 2018, pp. 704-708.

[10| M. Irvine and D. King. "The Money Laundering Control Act of 1986: Tainted Money and the Criminal Defense Lawyer." McGeorge Law Review, vol. 19. no. 1, pp. 171-192, Jan. 1987. [Online].Available:https://scholarlycommons.pacific.edu/mir/volf9/iss1/9

[11] J. Parra Moyano and O. Ross, "KYC Optimization Using Distributed Ledger Technology," Business & Information Systems Engineering, vol. 59. no. 6. pp. 411-423, Dec. 2017. |Online]. Available: hups://doi.org/10.1007/12599-017-0504-2

[12] J. Parra-Moyano and O. Ross, "KYC Optimization Using Distributed Ledger Technology, Business & Information Systems Engineering, vol. 59. 2017.

[13] A. Soni and R. Duggal, "Reducing Risk in KYC (Know Your Customer) for large Indian banks using Big Data Analytics." International Journal of Computer Applications, vol. 97. pp. 49-53, Jul. 2014. |Online).
Available:
hup://adsabs.harvard.edu/abs/20140CA.971.495

[14] *Initio - Blockchain as the Newest Regtech Application_ the Opportunity to Reduce the Burden of KYC for Financial Institutions library Catalog: www.initio.eu. Online]. Available:https://bit.ly/2YHYhMr

[15] M. Mainelli and M. Smith, "Sharing Ledgers for Sharing Economies:An Exploration of Mutual Distributed Ledgers (Aka Blockchain Technology)," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3083963. Nov. 2015. |Online]. Available: https://papers.ssrn.com/ahstract=3083963

[16] W. M. Shbair, M. Steichen, J. François, and R. State, "Blockchain orchestration and experimentation framework: A case study of kyc," in NOMS 2018 - 2018 IEEE/FIP Nework Operations and Management Symposium, 2018, pp. 1-6.

117| N. Szabo, "Formalizing and Securing Relationships on Publie Networks." First Mondar, vol. 2. no. 9, Sep. 1997. |Online|. Available:https://firstmonday.org/ojs/index.php/fm/article/view/548

118| "Blockchain & Distributed Ledger Technology (DLT)." library Catalog: www.worldbank.org. Online]. Available: https://www.worldbank.org/en/topic/tinancialsector/brief/bloekchain-dlt

[19] J. Howard, M. Kazar, S. Mences, D. Nichols, M. Satyanarayanan, R. N. Sidebotham, and M. West. "Scale and performance in a distributed file system," SIGOPS Oper. Syst. Rev., vol. 21, no. 5, p. 1-2, Nov. 1987. [Online]. Available: https://doi.org/10.1145/37499.37500

[201 What is IPFS? Interplanetary File System: Complete Beginner's Guide," last Accessed 31 Jul 2019. [Online].Available:https://blockonomi.com/interplanetary-file-system/