

STUDY ON KYC FOR BANKING SYSTEM USING IPFS AND BLOCK CHAIN TECHNOLOGY

BENZIGAR ANTONY F¹, RATHI B²

¹Lecturer, Department of Computer Science, College of Applied Science, Vadakkencherry

²Assistant Professor, Department of Computer Science, College of Applied Science, Vadakkencherry

Abstract - In banking system KYC means “Know Your Customer”. It is a process by which banks obtain information about the identity and address of the customers. This process helps to ensure that banks services are not misused. The KYC procedure is to be completed by the banks while opening accounts and also periodically update the same. With the growing concern of security, the KYC process is complex and involves a high cost for completing for a single customer. In this work, we propose an economical, swift, secure, and transparent platform for KYC document verification for the Banking system through Inter Planetary File System (IPFS) and blockchain technology. The proposed system allows a customer to open an account at one Bank, complete the KYC process there, and generate a hash value using the IPFS network and share it using the blockchain technology. 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 when someone tries to open an account at multiple Banks.

Key Words: opening accounts, hash value, blockchain

1. INTRODUCTION

Block chain technology become famous following the introduction of blockbuster cryptocurrencies like BitCoin and Ethereum, which are still the sole applications of blockchains at scale. Bit Coin and Ethereum have attracted the interest of the financial services industry, while at the same time giving rise to the introduction of additional cryptocurrencies (AltCoins) such as LightCoin, PrimeCoin, NameCoin. Moreover, they have driven the emergence of an entirely new concept for funding innovative ideas and products, namely the Initial Coin Offering (ICO) mechanism.

During the last couple of years, there has been a surge of interest in other applications of blockchains beyond cryptocurrencies, notably applications that attempt to exploit the decentralized nature of distributed ledger technologies (DLT), as well as their security, transparency and anti-tampering properties. In many cases applications take advantage of these properties in the scope of permissioned blockchain infrastructures, which offer fine grained authentication and authorization, while

at the same time obviating the need for complex and time-consuming Proof-of Work (PoW) processes. The latter is a key to supporting applications that need to support faster transaction completion than what is supported by conventional public blockchains such as BitCoin and Ethereum. This has given rise to the emergence of platforms destined to support permissioned blockchains such as R3/ Corda and Hyper ledger Fabric, both of which support hundreds of transactions per second (TPS).

Non-cryptocurrencies applications based on permissioned blockchains are currently being explored in many different sectors, such as energy, industry, supply chain management and healthcare. A plethora of such applications are also considered by financial organizations, as part of the wave of FinTech innovations. The use of blockchain technologies enables financial organizations to dismiss several long lasting prominent issues. One of the most notable problems associated to bank credit, is lack of information on credit scoring, causing individuals and SMEs to have difficulties in obtaining loans by financial institutions. Due to lack of sufficient and accurate information, financial institutions are also struggling to conduct accurate customer profiling such that they can efficiently conduct product differentiation and personalization. Along the same lines, insurance products offered by financial institutions encapsulate a complex insurance claims process, requiring the involvement of numerous stakeholders before the finalization and payment of a claim. Finally,

existing critical infrastructures that facilitate the majority of the transactions of financial organizations are primary targets for cyber-attacks. All financial organizations initiate KYC and KYB processes whenever they on-board a customer. As part of these process, the customer is identified and verified against applicable laws and rules set by regulators at national and international level (e.g. Central Banks, Banking Associations, Securities and Futures Commissions).

Moreover, an initial profile for the retail or corporate customer is offered, as means of personalizing service offerings. The KYC/KYB process is dynamic, as both customer information and applicable regulations evolve over time, which makes the process of updating profiles and relevant documentation quite challenging. Furthermore, customers are typically required to provide a batch of documents each time they are on-boarded by a financial institution. To alleviate this need, customer documentation can be maintained centrally by an authority (e.g., a regulator or state organization). This is however a solution vulnerable to cyber-attacks and data breaches. The Know your customer (KYC) is a very common term in the banking and financial sector. At this moment, the manual KYC process is outdated and has become a necessity to automate the KYC verification process. Studies around the world have made several attempts to make a better verification process for KYC. Many academics tried to propose a Blockchain-based solution. Blockchain technology recently

draws the attention of the public, as a dispute that leads to the foundation that the trust-free economical transaction is possible with its distinctive method. The blockchain permits unnamed and secure transactions of virtual currencies (such as Bitcoin, Litecoin, etc) and saves the metadata regarding the transaction details in a database. The database is secured and impedes 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. It proposed a blockchain based distributed platform for financial transaction processing in insurance industry. This will help industry to analyze the spread and plan further development. 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 proposed a 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 is costly. Currently,

miners are charging around \$7 per 100 KB of data.

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



2. RELATED WORKS

[1] This work done by Zehua Wanq, Yao Du, Shuxiao Niao, Victoria Lemieux "Blockchain empowered mobile edge intelligence, machine learning and secure data sharing" in the year 2021.

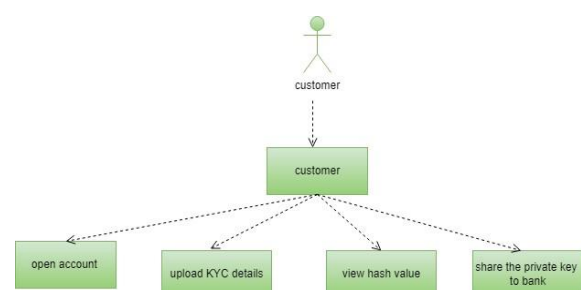
Driven by recent advancements in machine learning, mobile edge computing (MEC) and the Internet of things (IoT), artificial intelligence (AI) has become an emerging technology. Traditional machine learning approaches require the training data to be collected and processed in centralized servers. With the advent of new decentralized machine learning approaches and mobile edge computing, the IoT on-device data training has now become possible. However, those distributed frameworks of edge intelligence also introduce some new challenges, such as user privacy and data security. To handle these problems, blockchain has been considered as a promising solution. As a distributed smart ledger, blockchain is renowned for high scalability, privacy-preserving, and decentralization. This technology is also featured with automated script execution and immutable data records in a trusted manner. In recent years, as quantum computers become more and more promising, blockchain is also facing potential threats from quantum algorithms. In this chapter, we provide an overview of the current state-of-the-art in these cutting-edge technologies by summarizing the available literature in the research field of blockchain-based MEC, machine learning, secure data sharing, and basic introduction of post-quantum blockchain. We also discuss the real-world use cases and outline the challenges of blockchain-empowered intelligence.

3. PROPOSED SYSTEM

With population of India crossing the 1.38 billion mark and over 300 million banks account to be administered, banks are finding it difficult to manage the tedious paperwork involved. The old KYC process comprised of the user sharing

necessary identity documents with the banks or financial institutions such that the bank carries out background check and verification for the same which involves replication of the provided documents multiple times thus increasing paper work and risk factor. Owing to the risk and cost involved the old system is not to all efficient. With the advent of new technologies each day many researchers have proposed solution to the above problem quite recently.

We planned to reduce the progressive cost of KYC process by tackling the cost problem of KYC from financial institution perspective by using blockchain. currently, several third-party data providers and external validation agencies offer data and interfaces to extract the required customer information. However, banks struggle to integrate this data to obtain a consolidated view of the customers. This has led to increasing instances of banks' failure to comply with regulatory requirements, resulting in huge penalties and reputational damage. : post due diligence, banks need to digitize data in the documents to feed it into the repositories. This is an expensive exercise, as it uses advanced technology platforms.



3.1. ADVANTAGES OF PROPOSED SYSTEM

Decentralization. This is the main feature of blockchain technology, and the strong point is that to authenticate transactions or operations no other instance is required to act as an intermediary, reducing transaction validation times.

Network distribution. This point provides, at the same time, several benefits since, by having this network distributed, in the first instance, no one owns the network, allowing different users to always have multiple copies of the same information.

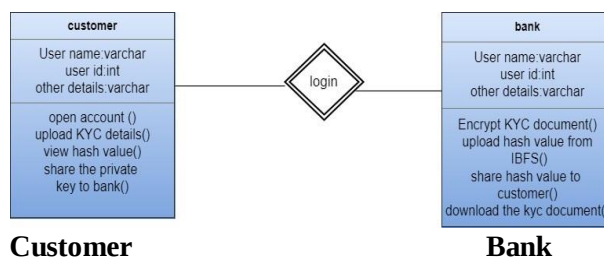
This characteristic makes it resistant and resilient to any type of failure since the fact that a node fails does not imply generalized failures in the network.

Having a distributed network means that there are practically no errors because the information must be verified by many participants in this network.

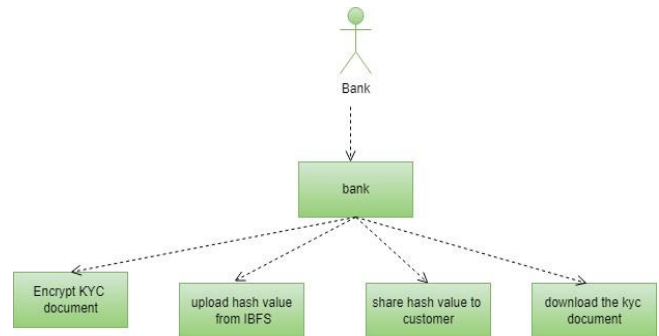
Low costs for users. The decentralized nature of Blockchain, allows for the validation of person-to-person transactions quickly and securely. Eliminating the need for an intermediary reduces costs for users.

4.USE CASE DIAGRAM AND CLASS DIAGRAM

4.1. USE CASE DIAGRAM



4.2. CLASS DIAGRAM



5. RESULTS AND OBSERVATION

Blockchain can completely change and transform the banking services because it has High security, high transaction transparency, decentralized system and can achieve transactions more efficiently.

6. CONCLUSION

To implement a platform for easy KYC document verification through a document-sharing platform called IPFS. We used different operating systems within PCs to test our works. The key generation and encryption processes were very smooth. We easily uploaded the encrypted file using the desktop app of IPFS using the command line interface of Windows Power Shell, and successfully uploaded and retrieved at PC2. Our research focused on a real scenario of a customer going to work with two financial institutions. The paper also showed the way of sharing the KYC docs without many difficulties between financial organizations through the wish of the customer.

REFERENCES

- [1] F. Glaser, "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3052165, Jan. 2017.
- [2] A. Rahman, S. Roy, M. S. Kaiser, and M. S. Islam, "A lightweight multi-tier s-mqtt framework to secure communication between low-end iot nodes," in 2016 5th International Conference
- [3] M. Raikwar, S. Mazumdar, S. Ruj, S. Sengupta, A. Chattopadhyay, and K.-Y. Lain, "A Blockchain Framework for Insurance Processes." 2018 HIP 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 IoT Framework for Neuroscience Applications," Cognitive Computation, vol. 10, no. 5, pp. b64–b73, Oct. 2018. [Online]. Available:
- [6] D. Tonin, "Money Button CEO: How to upload large files to Bitcoin SV blockchain," Mar. 2019, library Catalog: coingeek.com Section: Tech. [Online].
- [7] 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].