

Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology

Rashmi A P¹, B M Bhavya²

Dept of MCA, P.E.S College of Engineering, Mandya, Karnataka, India¹

Assistant professor, Dept of MCA, P.E.S College of Engineering, Mandya, Karnataka, India²

Abstract: Know your client (KYC) is a rule for the financial framework to approve a client based on character, propriety, and risk assessment when establishing a financial relationship. With the growing concern about security, the KYC cycle is perplexing and includes a significant cost for completing for a single client. Through InterPlanetary File System (IPFS) and blockchain innovation, we propose an affordable, quick, secure, and simple stage for KYC archive check for the Banking framework. The proposed framework allows a client to open a record at one bank, complete the KYC cycle there, and generate a hash value using the IPFS organization and distribute it via the blockchain method. After obtaining the confidential key, any Bank/monetary association can recover and securely store client information (i.e., KYC) utilizing the IPFS organization if the client wishes to open another account with that Bank/monetary association. The proposed framework can save time, money, and tedious work during the KYC cycle when someone tries to open a record at multiple banks.

Keywords: Blockchain, Smart Contract, KYC, IPFS, Gpg4win, and Decentralization

I. INTRODUCTION

Know your customer (KYC) is a very common term in the banking and financial industry. The manual KYC process is now obsolete, and there is a need to automate the KYC check process. Several efforts have been made around the world to develop a better KYC verification process. Many academics attempted to propose a Blockchain-based solution. People's attention has recently been drawn to blockchain innovation as a question that prompts the establishment that the trust conservative exchange is conceivable with its unmistakable strategy [1], [2].

The blockchain enables anonymous and secure exchanges of virtual monetary forms (such as Bitcoin, Litecoin, and so on) and stores transaction metadata in a data set. Cryptography strategies obtain the data set and prevent changes to the exchange history. Using the confidential key, the genuine client can communicate with the record. Blockchain is secure in banking and can significantly reduce handling/exchange costs. Banks and other financial institutions, such as insurance companies, manage numerous contracts that require multi-step handling between parties. Furthermore, these necessitate a reliable exchange with a short handling/settlement time. To address these concerns, the specialist has proposed a series of dispersed stages. Raikwar et al. [3] proposed a blockchain-based circulated stage for monetary exchange administration in the security industry. Puthal et al. [4] presented a decentralized structure based on blockchain that allows for the sharing and reconciliation of every circulated entertainer. This will help industry investigate the spread and plan future improvements [5].

Since Satoshi Nakamoto left the scene and handed over Bitcoin development to other center engineers, advanced record innovation has evolved, resulting in new blockchain applications.

Nakamoto [1] proposed an e-exchange system for coins delivered with computerized marks. The framework can track the exchange history and prevent double spending. From that point forward, experts are attempting to identify the anticipated areas for Blockchain application. Sharing transaction data over bitcoin is, by the way, expensive. Right now, excavators charge around \$7 per 100 KB of data [7].

The KYC records for the purposes cannot be transferred to the Blockchain network because it would be prohibitively expensive. Following that, as an alternative solution, KYC records sharing utilizing the InterPlanetary File System (IPFS) is proposed in this paper, and archives are then shared over the Blockchain organization. The IPFS is a common distributed report structure that aims to connect all enrolling registering gadgets with a comparable record arrangement [8]. Clients can save their transaction history and hash to the IPFS organization and then gaze it to the Blockchain network when needed. This interaction will significantly reduce the size of the blockchain information [9]. The rest of the article is organized as follows: segment II depicted the writing survey, segment III examined the technologies used to determine the structure, and section IV proposed a system. The outcome area and end were discussed separately in segments V and VI.

II. LITERATURE REVIEW

The KYC check process is a required piece of regulation for the financial industry [10]. When a client maintains that a monetary exchange with a monetary foundation should begin, the KYC cycle begins [11]. Arasa et al. [12] direct an examination of the cost of KYC based on the complexity level of the consistency expected for the example of business banks in Kenya, focusing on four factors that explain 78.3 percent of the consistency requirements. The information available to us is gradually expanding, including KYC records. Soni and Duggal [13] proposed a solution based on massive information logical procedures to address the massive information issue of KYC with a focus on Indian banks.

Y. Lootsma et al. [14] proposed using Regtech (administrative innovation) such as Blockchain in the financial sector to reduce the burden of the KYC cycle for a financial institution as well as the administrative organization. It should also be possible to use the methodology charge detailing. Nonetheless, they did not demonstrate the full implementation of Blockchain and the cost associated with the interaction. When a client maintains that they should do the monetary exchange through an installment supplier, they will truly look at the client character by his name from the Bank assuming the given data is correct through Blockchain brilliant agreement [15]. The creator expressed an interest in using blockchain to facilitate character and monetary exchanges, but they provided no use case for report sharing, such as KYC documents. A typical KYC system might be that a client goes to a bank, the bank performs KYC, stores KYC in the Blockchain, gives the client a token, and then the client gives access to another bank to look at the KYC data. The data from Blockchain is then cross-checked by the other bank [16]. The blockchain is somewhat wild as a result of a range of setup boundaries. For example, testnets like Rinkby and Ethereum can't be changed effectively because of constraints like gas limit, mining difficulty, and so on. Grid'5000 was recommended by the creators because it is a highly controllable and reconfigurable testbed. Once again, the creators failed to provide a reasonable use case scenario with cost estimation.

J. Parra Moyano et al. [17] proposed a unified and decentralized Blockchain KYC arrangement with cost sharing among various banks. They proposed another plan based on conveyed record innovation to reduce the cost of center KYC confirmation and further develop the client experience (DLT). They concentrated on four major issues. The first is proportionality: the cost will be shared fairly among all organizations involved in a specific KYC check process. Aside from that, they focused on Irrelevance.

The person who keeps a strategic distance from the KYC cycle will not receive a motivator. Privacy came in third place in the center. The KYC check process must be completed so that client security is not jeopardized. They finally settled on No-stamping. Because the interaction is taking place online, they must ensure that no misrepresentation is made during the KYC check. When someone tries to change any piece of KYC information, the altering interaction is automatically void from the definitive side. Their proposal was very viable, with the exception of two issues, which are as follows:

- Over time, the size of the block information will grow, as will the cost of including it.
- If a client opens a record at only one bank, that bank must bear the entire cost.

III. BACKGROUND TECHNOLOGIES**A. Blockchain**

Blockchain is a straightforwardly shared variant of online transaction in which a client sends money to others without the assistance of a monetary association. All transactions will be hashed to a continuous proof-of-work chain. Each of these is referred to as a block, and the running block contains the hash of all previous blocks. As a result, the entire cycle is tempered confirmation, because a single friend can't add another block without the verification of-work [18]. Bitcoin was the first fully decentralized cryptographic currency. While the primary goal of DLT was to make computerized money and send and receive data over the Internet, the innovation can also be used to confirm online data sharing through smart contracts. The astute contract anticipates including them in properties that are costly and computerized [19].

The European Security and Markets Authority [20] discussed the potential benefits, challenges to those benefits, and impediments of DLT in the security market. While they only focused on the security market, they provided a rule to apply DLT in other monetary areas such as banks.

B. IPFS

The InterPlanetary File System (IPFS) is a peer-to-peer (P2P) file sharing convention that connects processing gadgets for sharing/storing documents/information. Using the hash code of the record, the substance is extremely recognized in the global namespace. If the hash code is changed, the information cannot be confirmed and will not be distinguished by IPFS at any point. Furthermore, IPFS recognizes duplication when documents with the same content are stored. Among many others, AFS [21] has achieved widespread success, despite the fact that it is still used by some today.

Specifically, Napster, LimeWire, Gnutella, KaZaA, and BitTorrent are unstructured conveyed P2P document/content-sharing conventions used by over 100 million concurrent clients. In contrast, IPFS follows a client-server model, which raised the question of how we would access the web [20].

C. Gpg4win

Very Good Privacy is a cryptography (especially protection and verification) progression that ensures the security of record registry, text, and email. Additionally, the entire circle with the advanced mark It enables the non-renunciation of records and email's trustworthiness.

GNU Privacy Guard for Windows, abbreviated Gpg4win, is an open-source encryption package for email/record in Microsoft Windows environments that employs GnuPG cryptography.

IV. PROPOSED FRAMEWORK

A. Proposed Work stream

Figure 1 depicts a proposed work process for sharing KYC documents using IPFS. The case of a customer moving toward two distinct banks is used in the work process. In the initial stage, the client went to Bank A to provide his KYC.

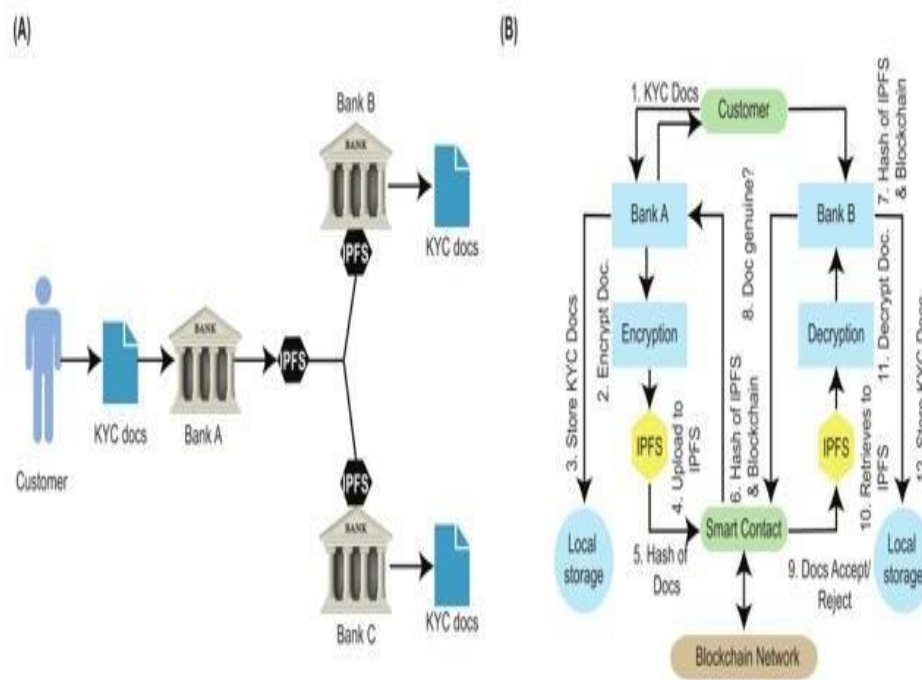


Fig. 1. (A)The work process of KYC docs sharing utilizing IPFS. (B) BlockDiagram of Proposed KYC Solution

Report for verification Bank A examines our proposed framework plan and provides the client with a hash value and an individual unscrambling key. The client will then take these two keys to Bank B and Bank C, and the two banks will instantly confirm the KYC doc. We used the IPFS organization to transfer and retrieve KYC documentation at the banks' end. In any case, before distributing KYC documents to the IPFS organization, we considered scrambling the record for added security and to reduce document size. Because anyone with access to the IPFS network can obtain the KYC documents simply by realizing their hash values. We used the well-known encryption software gpg4win in the Kleopatra stage so that people would have encrypted KYC documents.

B. Proposed Block Diagram

The proposed KYC arrangement is depicted in Fig. 2 using the example of a client visiting two traditional banks. We considered a scenario in which a client went to Bank A to open a record during the primary stage. The client presented the bank with the record data as well as the KYC documents. The bank then noticed the entire data, which, if seen as correct, will be encoded utilizing the framework's application (a well-known encryption device, gpg4win, and IPFS in our case) which will be accessible to all banks to impart records to other banks and store a duplicate to a nearby data set. Following that, bank A will store the encoded record in the secure IPFS network. The bank will then transfer the

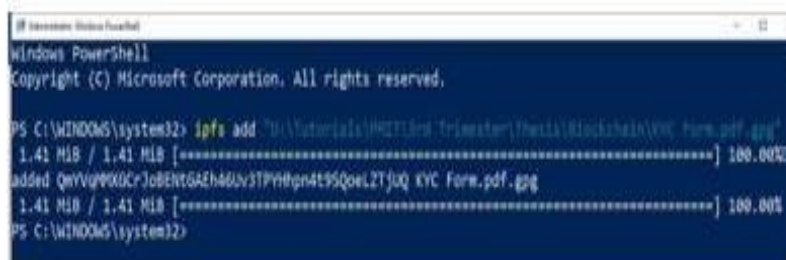
hash value from IPFS, a small in- memory size, to the Blockchain organization. Bank A also keeps a copy of the client's KYC documents in its local data set. Finally, Bank A will share the hash value of Blockchain and IPFS with the client. Later on, the client can gain access to the KYC doc bundle by simply sharing the hash value with the other establishment he intended to work with. Nonetheless, the client can now go to another bank to open a new account. The client will reveal his hash value from IPFS to Blockchain and Bank B. Because the client will grant Bank B access to the hash value of the report bundle, the Bank will gain access to the Blockchain network for the required hash esteem. As a result, the bank will use the hash value recovered from Blockchain to download the encoded KYC documents from the IPFS network. Finally, using the client's confidential key, the bank will recover the KYC documents and save a duplicate of the KYC documents to the bank's neighborhood data set. In the proposed arrangement in the national bank, the administrative bank is characterized.

V. RESULTS AND DISCUSSION

We attempted to carry out the KYC documents check and make them available to a financial organization with the assistance of IPFS and Blockchain organization. We demonstrated a scenario in which a client went to a bank to open a record. The bank scrambles the confirmed KYC documents with Gpg4win and then transfers the documents to the IPFS network depicted in fig. 2.

A similar client then went to another bank to make a monetary transaction, expecting to have a similar interaction. Fortunately, for our situation, he recovers the hash from the Blockchain organization and the KYC docs from the IPFS network using the hash keys he obtained from the primary bank.

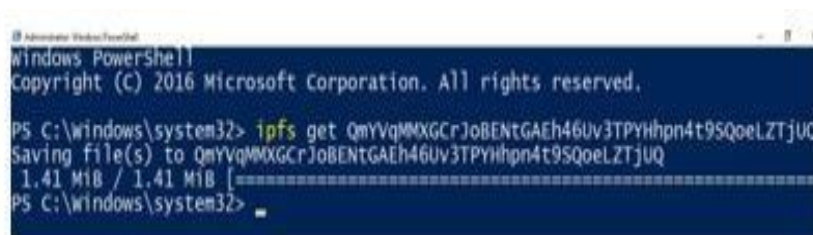
Regardless of the methodology we have chosen to work with, whether private or public Blockchain, our discoveries offer various possibilities for increasing the effectiveness of the current monetary framework. Furthermore, such a stage could guarantee a significant decrease in cost during KYC report check for standard participating organizations and less trouble for the client. Furthermore, the proposed framework will ensure cash, efficient, and professional funding for financial institutions.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> ipfs add "W:\Tutorial\IPFS\2nd\Trimester\The1\Blockchain\KYC_Form.pdf.gpg"
1.41 MiB / 1.41 MiB [=====] 100.00%
added QmYVqMMXGCrJoBENTGAeh46Uv3TPYHhpn4t9SQoelZTjUQ KYC_Form.pdf.gpg
1.41 MiB / 1.41 MiB [=====] 100.00%
PS C:\WINDOWS\system32>
```

Fig.2. The KYC documents are being transferred in the IPFS network.



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\windows\system32> ipfs get QmYVqMMXGCrJoBENTGAeh46Uv3TPYHhpn4t9SQoelZTjUQ
Saving file(s) to QmYVqMMXGCrJoBENTGAeh46Uv3TPYHhpn4t9SQoelZTjUQ
1.41 MiB / 1.41 MiB [=====]
PS C:\windows\system32>
```

Fig. 3. Recovering KYC Documents from the IPFS Network

VI. CONCLUSION

The paper attempted to carry out a stage for simple KYC report check using an IPFS record sharing stage. To test our work, we used two different operating systems on two different PCs. The two computers were running Windows 10 64-cycle operating systems. We discovered that gpg4win with Kleopatra stage and IPFS for Windows had been installed on the two PCs. The vital age and encryption processes ran extremely smoothly. We easily transferred the scrambled document using the IPFS workstation application and the order line point of interaction of Windows Power Shell, and successfully transferred and recovered at PC2. Our investigation focused on a real-life scenario involving a client who was going to work with two financial foundations. The paper also demonstrated how to divide KYC



documents without much difficulty among financial organizations based on the client's desire.

This work can be expanded in the future by dissecting various testing exhibits, such as idleness tests, load tests, stress tests, and so on.

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 on Networking, Systems, and Applications (ICNSA), Oct. 2016.
- [3] K.-Y. Lain, "A Blockchain Framework for Insurance Processes." 2018 HIP International Conference on New Technologies, Mobility and Security (NTMS), 2018.
- [4] 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:
- [5] 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.