

Know Your Client for Banking System using IPFS and Block Chain

Keerthana P¹, Usha M²

Student, Department of MCA, Bangalore Institute of Technology, Bengaluru, India¹

Assistant Professor, Department of MCA, Bangalore Institute of Technology, Bengaluru, India²

Abstract: The term "know your client" (KYC) refers to a rule that requires the financial framework to authorize a client based on identity, propriety, and risk assessment before creating a financial relationship. The KYC cycle can be confusing and expensive to complete for a single client, which is a result of the rising security concerns. By combining InterPlanetary File System (IPFS) and blockchain innovation, we offer a cheap, quick, safe, and easy KYC archive check service for banks. According to the proposed technique, using the IPFS organization, a client can create a hash value and share it through the blockchain method after setting up a record at one bank, finishing KYC there, and then releasing the hash using the IPFS organization. By acquiring the IPFS organization's confidential key, the client will be able to get the client's information (i.e., KYC) and securely save it if they choose to have another account with the Bank/monetary association. It is believed that this approach can help save time, money, and tiresome effort during the KYC cycle when a record has to be opened in more than one bank.

Keywords: Decentralization, IPFS, Blockchain, KYC, GPG4WIN and Smart Contact.

I. INTRODUCTION

KYC (Know Your Customer) is commonly used in the banking and financial industries. As a result, the manual KYC process must now be automated. Around the world, numerous initiatives have been launched to improve the KYC verification procedure. Several academics have made suggestions for Blockchain-based solutions. People's attention has recently been drawn to blockchain innovation as a question that prompts the establishment that the sans trust conservative exchange is conceivable with its unmistakable strategy [1], [2]. Bitcoin, Litecoin, and other virtual currencies may be exchanged anonymously and securely because of blockchain, which also preserves transaction details in a data set. The data set is obtained via cryptographic techniques, which also stop the exchange history from changing. Genuine clients can interact with the record by using the confidential key. Blockchain can significantly lower handling and exchange costs while maintaining banking security. Numerous contracts that need for multi-step processing between parties are managed by banks and other financial organizations, such as insurance firms. Additionally, these demand a trustworthy exchange with a quick handling/settlement time. The expert has suggested a number of different stages to address these worries. A blockchain-based circulated stage for monetary exchange administration in the security industry was proposed by Raikwar et al. [3]. A decentralized framework built on blockchain that enables the sharing and reconciliation of any circulated entertainer was presented by Puthal et al. [4]. This will help industry in examining the spread and planning for upcoming improvements. Since Satoshi Nakamoto left and gave other center developers control of developing Bitcoin, sophisticated record innovation has evolved, giving rise to new blockchain applications. An electronic trading mechanism for coins delivered with computerized marks was suggested by Nakamoto [5]. The system can keep track of past transactions and stop double spending. From that point on, experts are working to pinpoint the likely fields in which Blockchain application will be used. By the way, sharing transaction data over bitcoin is expensive. Excavators currently charge about \$7 for every 100 KB of data. It would be too expensive to transfer the KYC records needed for the purposes to the Blockchain network. In this study, an alternative storage method for KYC records is proposed using the IPFS, and archives are subsequently shared throughout the Blockchain organization. A common distributed report structure called IPFS intends to link all registering devices with a same record structure. The IPFS structure allows users to retain their transaction history and hash, which can then be transferred to the Blockchain network as needed. The size of the blockchain information will be drastically reduced as a result of this interaction. The remaining of the article is structured as follows: The writing survey was portrayed in segment II, the technologies utilized to assess the structure were explored in segment III, and a system was suggested in section IV. Segments V and VI each had a distinct discussion of the outcome area and end [6].

II. LITERATURE REVIEW

The KYC check procedure is a requirement of the financial industry's regulatory framework. When a client maintains that a monetary exchange with a monetary foundation should begin, the KYC cycle begins. In this paper, Arasa et al [7] estimates the financial implications of KYC based on the degree of consistency needed by a business bank in Kenya, concentrating on four aspects that make up 78.3 percentage of the overall consistency requirement. Our knowledge base is continually growing and now includes KYC records. With an emphasis on Indian banks, Soni and Duggal [8] developed a method based on enormous information logical procedures to handle the massive information issue of KYC. Regtech (administrative innovation), such as Blockchain, has been suggested by Y. Lootsma et al. [9] as a way to ease the KYC cycle's burden on both financial institutions and administrative organizations. Additionally, using the methodology charge detailing should be achievable. However, they did not show how well implemented Blockchain was or how much it would cost to engage with it. If the information provided by a customer is valid, the instalment provider will recognize the individual by his name from the bank when requesting the transaction to be carried out through an instalment provider. Although the developer expressed interest in leveraging blockchain to speed up character and money transfers, they did not offer any use cases for exchanging reports, such as KYC paperwork. As part of a standard KYC system, a customer enters a bank, the bank conducts the KYC, stores the outcome in the Blockchain, provides the customer with a token, and the customer allows access to another bank to review the KYC data. After then, the data obtained from Blockchain is cross-checked by the other bank. Due to various setup boundaries, the blockchain is rather untamed. For instance, due to limitations like the the complexity of the mining process, testnets like Rinkby and Ethereum cannot be altered efficiently. Because it is a highly controllable and adaptable testbed, the developers suggested Grid'5000. Again, the creators failed to provide a reasonable use case scenario and a price range. A unified and decentralized Blockchain KYC system with cost sharing among several institutions was presented by J. Parra Moyano et al. [7]. To lower the price of center KYC certification and boost the customer experience (DLT), they implemented a different strategy based on transmitted records. They concentrated on four primary issues. The one is proportionality: Each company participating in a specific KYC verification process will cover a reasonable fraction of the costs. Furthermore, they focused on Insignificance. In the event that a person avoids the KYC process intentionally, they will not receive any incentive. Privacy came in third place in the center. The KYC check process must be completed so that client security is not contravene. 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. RELATED TECHNOLOGIES**A. Blockchain**

Blockchain is a plainly visible form of internet transaction that enables people to move money between themselves without having to rely on a bank. The hash of each transaction will be added to a proof-of-work chain that is constantly growing. The running block contains the hash of each of these units, each of which is referred to as a block. As a result, the complete cycle is tempered because no further block can be added by a single friend without the verification of the work. The first completely decentralized cryptographic currency was Bitcoin. In addition to sending and receiving data over the Internet and generating computerized money, DLT can also be used to validate online data sharing by means of smart contracts. They will be a part of price, computerized properties, according to the smart contract. Markets Authority [10] and the European Security had a discussion about the potential benefits, potential drawbacks, and challenges that DLT may face in the security market. Although DLT can be implemented in other financial sectors, such as banks, they mainly focused on securities markets.

IPFS

InterPlanetary File System (IPFS), a peer-to-peer (P2P) file sharing system, links devices to share and store documents and data. Using the record's hash code, the substance is widely recognized in the global namespace. The information cannot be verified and will never be distinguished by IPFS if the hash code is modified. Additionally, when many documents with the identical content are stored, IPFS detects duplication. Despite the fact that some people still use it today, AFS [11] has been extremely successful among many others. Over 100 million continuous clients employ the unstructured transmitted P2P document/content sharing standards Napster LimeWire Gnutella, KaZaA, and BitTorrent in particular. In contrast, IPFS follows a client-server approach, which created the question of how we would access the web [12].

B. Gpg4win

A progression in cryptography called Very Good Privacy assures the confidentiality of email, text messages, and record registries. Furthermore, the full circle bearing the advanced mark permits the preservation of records and the reliability of email. The open-source encryption tool GNU Privacy Guard for Windows, often known as Gpg4win, uses GnuGP cryptography for email and records in Microsoft Windows systems.

IV. PROPOSED FRAMEWORK

A. Proposed Work stream

A suggested workflow for using IPFS to share KYC papers is shown in Figure 1. In the course of the work, the scenario of a customer switching between two different banks is used. To complete his KYC, the client initially went to Bank A.

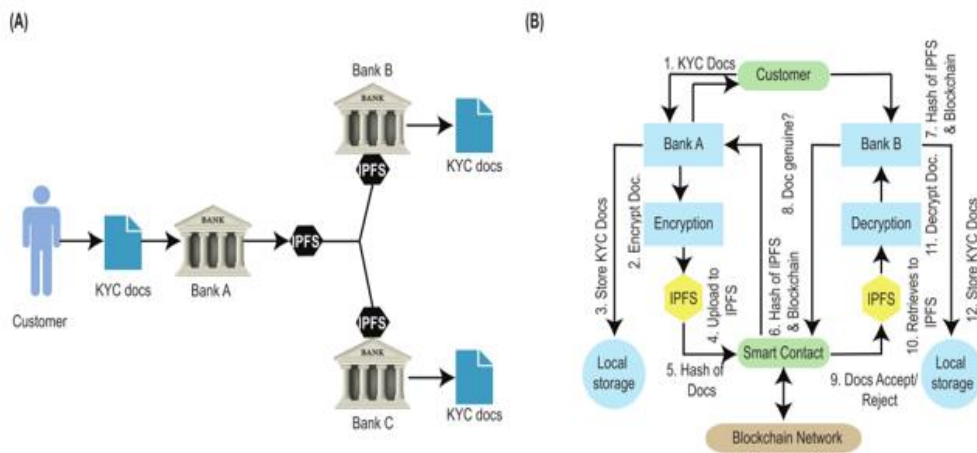


Fig 1. (A) An IPFS-based method for sharing KYC documents. (B) Schematic Representation of Proposed KYC Approach

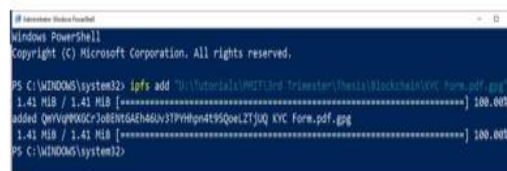
After reviewing our recommended architecture, Bank A formally offers our client with a hash value and a special key to unlock the data. These two keys will then be sent by the client to Bank C and Bank B, who will both verify the KYC document instantly. To transfer and retrieve KYC documentation at the banks' end, we used the IPFS organization. To be safe, we thought about scrambling the record before sending the KYC paperwork to the IPFS organization to increase security and make the document smaller. since anyone with access to the IPFS network can receive the KYC documents by simply knowing their hash values. In the Kleopatra stage, we employed the well-known encryption programme gpg4win so that users could have encrypted KYC documents.

B. Proposed Block Diagram

A consumer visiting two conventional banks is the example used in Fig. 2 to show the suggested KYC system. In one instance, a client opened a record at Bank A during the preliminary phase. The information from the records and the KYC documentation were submitted by the customer to the bank. The bank then noted the complete data, which, if believed to be accurate, will be encoded using the framework's application (Using the well-known encryption programme gpg4win and IPFS as our instances), As a result of the new system, all banks will be able to exchange records and the storing of a copy to a nearby data collection. Bank A will thereafter keep the encrypted record in the safe IPFS network. The bank will subsequently send the hash value from the Blockchain organization's modest in-memory IPFS storage. A copy of the client's KYC documents is likewise kept by Bank A in its local data collection. The hash value of IPFS and Blockchain will also be disclosed to the client by Bank A. The client will then be able to use the KYC doc bundle by providing a hash value to the other establishment he intends to interact with. However, the customer can now open a new account with a different bank. It is the customer's responsibility to reveal his respective hash value. By granting Bank B access to the report bundle's hash value, the bank will have access to the blockchain network for the desired hash value. To get the IPFS network's encrypted KYC documents, the bank will make use of the hash value it was able to retrieve from Blockchain. The bank will then retrieve the KYC papers using the client's private key and save a copy of the recovered documents to its local data set. The administrative bank is defined in the national bank's planned arrangement.

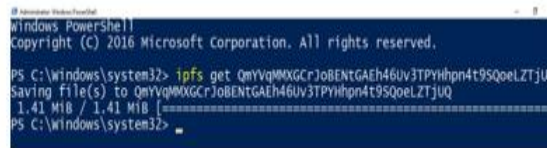
V. RESULTS AND DISCUSSION

With the aid of an IPFS and blockchain organization, we made an effort to carry out the KYC document check and provide the results to a financial organization. We gave the case of a client who went to a bank to open a record. As seen in figure 2, the bank encrypts the KYC documents using GPG4Win before delivering them to IPFS. The same customer then conducted a financial transaction with a different bank, hoping for a similar outcome. In the end, he was able to retrieve the hash from the Blockchain organization and the KYC documents from IPFS using the hash keys he had received from the main bank. We found that there are a number of opportunities to enhance the effectiveness of the current monetary system, no matter what approach we choose, whether it is a private or public Blockchain. Additionally, such a platform might ensure a large decrease in cost for participating firms during the KYC report check and less hassle for the client. The proposed framework would also make sure that financial institutions are funded in a timely, effective, and professional manner.



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

PS C:\WINDOWS\system32> ipfs add "D:\Material\IPFS\and Transaction\hash\Blockchain\kyc form.pdf.gpg"
1.41 MiB / 1.41 MiB [=====] 100.00%
added QmYVqMxGCrJoBENTGAeh46Uv3TPYihpn4t9SQoelZTjUQ 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 QmYVqMxGCrJoBENTGAeh46Uv3TPYihpn4t9SQoelZTjUQ
Saving file(s) to QmYVqMxGCrJoBENTGAeh46Uv3TPYihpn4t9SQoelZTjUQ
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. We used two distinct operating systems on two different PCs to evaluate our work. The Windows 10 64-bit operating systems were installed on the two machines. On the two computers, we discovered that gpg4win had been configured with Kleopatra stage and IPFS for Windows. The crucial ageing and encryption processes went off without a hitch. Using the Windows Power Shell order line point of interface and the IPFS workstation application, we successfully transferred and recovered the scrambled document at PC2. Our inquiry centred on a genuine case study with a client who intended to collaborate with two financial foundations. The report also showed how KYC documents might be easily distributed around financial institutions in accordance with client preferences. The work can be extended in the future by examining different test exhibits, such as idleness tests, load tests, stress tests, and so on.

REFERENCES

- [1] "Pervasive Decentralization of Digital Infrastructures: A Framework for Blockchain-Enabled System and Use Case Analysis," SSRN Scholarly Paper ID 3052165, Rochester, NY: Social Science Research Network, January 2017.
- [2] "A lightweight multi-tier s-mqtt framework to secure communication across low-end iot nodes," in 2018 5th International Conference on Networking, Systems and Security (NSysS), pp. 1-6.
- [3] "A Blockchain Framework for Insurance Processes," 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018, by M. Raikwar, S. Mazumdar, S. Ruj, S. Sengupta, A. Chattopadhyay, and K.-Y. Lam.
- [4] "The Blockchain as a Decentralized Security Framework [Future Directions]," IEEE Consumer Electronics Magazine, vol. 7, pp. 18-21, 2018. D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and C. Yang.
- [5] Bitcoin: A Peer-to-Peer Electronic Cash System, by S. Nakamoto, 2010, bitcoin.org.
- [6] "A novel ipfs-based storage model for blockchain," 2018 IEEE/WIC/ACM ICWI, pp. 704–708. Q. Zheng, Y. Li, P. Chen, and X. Dong.
- [7] "KYC Optimization Using Distributed Ledger Technology," Business & Information Systems Engineering, vol. 59, 2017. J. Parra-Moyano and O. Ross.
- [8] "Reducing Risk in KYC (Know Your Customer) for large Indian banks using Big Data Analytics," International Journal of Computer Applications, vol. 97, no. 7, July 2014, pp. 49–53.
- [9] "The newest Regtech application, Initio Blockchain Possibility to Lighten Financial Institutions' KYC Load,"



www.initio.eu is the library catalog.

[10] Library Catalog: www.worldbank.org, "Blockchain & Distributed Ledger Technology (DLT)".

[11] "Scale and performance in a distributed file system", by J. Howard, M. Kazar, S. Menees, D. Nichols, M. Satyanarayanan, R. N. Sidebotham, and M. West, SIGOPS Operational Systems Review, vol. 21, no. 5, p. 1-2, November 1987.

[12] "Describe IPFS. Complete Guide to Interplanetary File System, "accessed on July 31, 2019.