Metadata of the chapter that will be visualized online

Chapter Title	Blockchain and IPFS-Based Solution for KYC	
Copyright Year	2024	
Copyright Holder	The Author(s), under exclusive license to Springer Nature Switzerland AG	
Author	Family Name	**Phatangare**
	Particle	
	Given Name	**Sheetal**
	Suffix	
	Organization	Vishwakarma Institute of Technology
	Address	Pune, Maharashtra, India
Author	Family Name	**Patil**
	Particle	
	Given Name	**Omkar**
	Suffix	
	Organization	Vishwakarma Institute of Technology
	Address	Pune, Maharashtra, India
Corresponding Author	Family Name	**Patil**
	Particle	
	Given Name	**Pratik**
	Suffix	
	Organization	Vishwakarma Institute of Technology
	Address	Pune, Maharashtra, India
	Email	pratik.patil201@vit.edu
Author	Family Name	**Patil**
	Particle	
	Given Name	**Tanishk**
	Suffix	
	Organization	Vishwakarma Institute of Technology
	Address	Pune, Maharashtra, India
Author	Family Name	**Waghmare**
	Particle	
	Given Name	**Pranav**
	Suffix	
	Organization	Vishwakarma Institute of Technology
	Address	Pune, Maharashtra, India
Abstract	We use a centralised financial system in India. The 'Know Your Customer' (KYC) process, which requires customers to update their	

credentials, has just begun. Other companies and business institutions are using this approach to store data for user authentication and staff verification, among many other things. The challenge with this system is that the users must complete KYC each time they visit a new institution for various reasons. They require KYC even at banks for various transactions. If they transact, there are several procedures and intermediaries involved. We recommend a solution where users complete a one-time KYC to eliminate the intermediaries and expenses associated with the ongoing KYC. Later, users will be able to access this data at any time and from any location for multiple purposes. Our system will use blockchain, the most advanced technology in the world, for this purpose, providing us with a distributed environment, transparency for the user and no outside intervention, boosting its security. Throughout the user onboarding process, this technology enables efficiency improvements, cost savings, improved client experiences and increased transparency.

Keywords (separated by "-")	Blockchain - Ethereum - KYC - HyperLedger - Solidity

Blockchain and IPFS-Based Solution for KYC

Sheetal Phatangare, Omkar Patil, Pratik Patil, Tanishk Patil, and Pranav Waghmare

1 Introduction

Almost everything today is accessible owing to the world's ever-evolving technologies. People can now access anything they wish with only a few taps. Hence, we are integrating 'Know Your Customer' (KYC) using the leading technology, blockchain, to make things clearer and more useful for accessing user information. With distributed KYC, which will be available at financial institutions, companies and other similar places for user details authentication, the old centralised KYC in banking systems will be replaced, which will minimise the ongoing effort of doing KYC.

Under the proposed approach, the KYC procedure can be completed only once by each user, as opposed to once by each bank that works with that user, which is an advantage over the present method. As a result, the entire cost of the KYC procedure is dropped in a nation without impacting system security, user privacy or increased openness in the case of a dispute.

The idea of the proposed design is to create an efficient KYC blockchain system for maintaining user KYC data. The system may be deployed in several businesses that want KYC verification of their users. Blockchain is becoming increasingly important in the world of cybersecurity applications. The essential aspect of the blockchain idea is distributed ledger technology (DLT). DLT provides a decentralised system in which data copies are accessible through a network of linked nodes and these data copies are exchanged across the nodes and are constantly synced. Everybody can access any type of data stored in a blockchain and it

S. Phatangare · O. Patil · P. Patil (✉) · T. Patil · P. Waghmare
Vishwakarma Institute of Technology, Pune, Maharashtra, India
e-mail: pratik.patil201@vit.edu

E. S. Gopi, P. Maheswaran (eds.), *Proceedings of the International Conference on Machine Learning, Deep Learning and Computational Intelligence for Wireless Communication*, Signals and Communication Technology,
https://doi.org/10.1007/978-3-031-47942-7_16

will always be tamper-proof. Before any data is uploaded to the blockchain, the agreement of all DLT network nodes is necessary.

2 Literature Review

Syed Azhar Hussain et al. [1] proposed a DKYC model, providing advantages including lower transaction costs, higher provenance, immutability and transparency in transactions, based on DLT. DKYC, in contrast to traditional KYCs based on the pull model, supports both push (customers sending information to the service provider) and pull models (banks or service providers seeking an update on customer profiles), with the customer's consent on what, where and with whom he or she would like to share the information. DKYC shall be a public blockchain based on the data uploaded and the score shall be awarded to the user, incrementing with every category of data uploaded.

Nikita Singhal et al. [2] proposed a system to improvise the 'storage' component of KYCs using the interplanetary file system (IPFS) and by eliminating third parties. Sunitha et al. [3] proposed a blockchain-based approach that eliminates intermediaries and enables one-time KYC for users. Users have access to the data at any time, from any location and for a variety of purposes. Blockchain technology's decentralised ecosystem, user transparency and lack of third-party meddling increase its security. In addition, faster processing is guaranteed.

AQ2

The total cost of the KYC procedure in a blockchain ecosystem is lower than the conventional methods. The dual advantage of lower costs for the organisations and improved client experience was the proposed solution's ultimate efficiency gain [4].

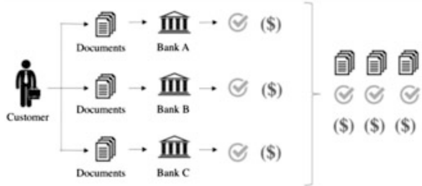
Every FI must adhere to the KYC procedure before working with a new customer. It is composed of several routine tasks. Due to the rising cost of KYC, the use of blockchain technology has encouraged the development of new systems aimed at improving the efficiency of the KYC process and co-operation among FIs [5].

3 Methodology

A blockchain is a decentralised, encrypted and immutable ledger that keeps track of transactions in the form of blocks and distributes them over many networks using a peer-to-peer (P2P) network. Each block has a distinct hash value, which makes the chain more secure in terms of encryption. The concept of blockchain was introduced in 2009 by Satoshi Nakamoto and his team in his paper. He introduced the concept of cryptography or digital cash systems which gave birth to bitcoin.

The IPFS is a distributed hypermedia P2P system. A protocol is created to serve as an all-encompassing file system for computers. It is also open source. It is a difficult and ambitious programme that will significantly affect the future organisation of the Internet. The P2P protocol uses a set of hashed files that are

Fig. 1 Current KYC process



stored on each node. A straightforward abstraction layer is offered to any client that wishes to retrieve any of these files. To obtain the file, only the file's hash needs to be called.

3.1 *Current KYC Process*

Financial institutions, such as banks, are required by regulatory norms to onboard their clients before involving them in any activities to prevent illegal activities. Personal information is gathered from all available sources to search for illegal activity. Risk management, which may also comprise transaction monitoring, is another aspect connected to onboarding new clients. Financial institutions may even be subject to significant fines if this process is not done in compliance with legislation. For instance, the RBI fined 13 banks in 2016 for breaking regulatory directives, instructions and recommendations, including those relating to KYC standards.

Figure 1 illustrates how the transfer of documents and core KYC validation for a consumer must be performed three times, resulting in increased costs for this customer that are three times greater than a single KYC process.

3.2 *Proposed KYC System*

The proposed system uses these capabilities to introduce blockchain for the concept of KYC so that we can ease the process of KYC verification. The application proposed is a decentralised application that will use a Ganache-based local blockchain as the primary blockchain for recording and managing transactions related to the bank account, bank and KYC information. MetaMask is its local wallet. The system was built using Solidity because it supports the concept of smart contracts, that allow users and service providers to manage modifications and keep data records secure. Smart contracts can set rules and have them enforced automatically through programming. The smart contract cannot be removed after it has been deployed and the changes associated with it are immutable, so the blockchain is also called the immutable ledger. Therefore, the record of transactions conducted with the smart contract is immutable and can be accessible to only users registered on the blockchain network.

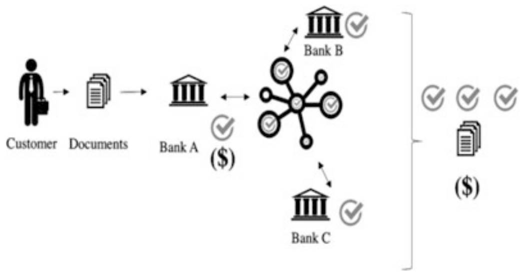


Fig. 2 System overview

Table 1 KYC security requirements and the KYC features in our system

Security and privacy requirements	Feature of our e-KYC TrustBlock
Verification of customer identification information	Our scheme allows any form of POI to be registered and signed by the customer. We also have a smart contract to support secure verification of the encrypted documents. The authenticity of the customers is firmly verified through their digital signatures while the examination of the documents is vetted by FI's officer.
Protection of customers' credentials	All customers' credentials are protected based on AES and RSA encryption.
Auditing feature	All e-KYC transactions are recorded in the blockchain with the encrypted format.

4 System Architecture (Fig. 2)

The system has two use cases: a user, i.e., an account holder, and a bank. Account holders and banks will be able to interact with the blockchain-based smart contract system and modify just the attributes that are available to them under the proposed system. The suggested solution is built on the Ganache local blockchain, which is decentralised. The blockchain manages backend-based data in the Ethereum architecture, implying that blockchains serve as the client's backend database.

The current KYC verification systems are centralised and can be attacked by hackers, which can lead to data leaks. The suggested KYC-verification system is a decentralised system built on the blockchain that ensures it is secure and easy to use.

As indicated in Table 1:

- Customers' login information or PII should be kept private. PKI-based encryption and digital signing should be used.
- The login information and PII of customers should be kept confidential. Digital signature and encryption based on PKI should be employed.
- Customers' approval is required before collecting their 'credentials'.

The proposed system requires tools like Ganache, Remix IDE, Web3 JS and the MetaMask crypto wallet. The proposed KYC verification system will allow customers to upload their documents and personal information on web pages so

Fig. 3 Blockchain in KYC

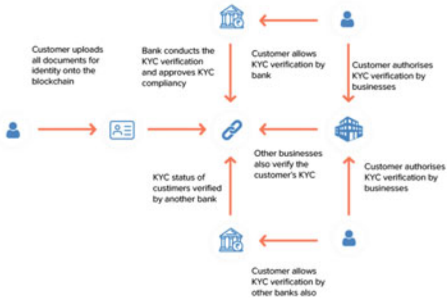


Table 2 Description of functions in KYC

Functions	Description
AddBank and AddCustomer	Administrator can add new banks and new bank accounts to the network
addNewCustomerRequest	Initiate a new KYC request for the customer
DownVoteCustomer	Reject the KYC request of the customer
getCustomerKycStatus	Get the status of users' KYC request
UpVoteCustomer	Accept the KYC request of user
ModifyCustomer	Change the data associated with user
removeBank and removeCustomer	Administrator can remove banks and bank accounts in the network

that the bank can verify them and accept or reject KYC requests from customers. We will also attempt to incorporate some basic banking functions into this project (Fig. 3).

Each bank will have its smart contract, with functionality like adding or modifying information or viewing listed accounts (see Table 2). All the actions will be recorded and moved onto the blockchain. When a user uploads documents to IPFS, it sends their hash. The hash will be stored on the blockchain using a deployed smart contract.

5 Workflow of Proposed System

5.1 Enrolment on the System

The bank account and bank can be added to the blockchain by the system admin. The admin has all the access initially; he/she can add banks and accounts on the blockchain. The account holder in the bank can access the blockchain for sending a hash of documents. The bank has access to the blockchain for adding new accounts and accessing information about accounts (Fig. 4).

Fig. 4 Deployed contract

5.2 *Uploading Documents*

For the user to submit documents or provide KYC, they must upload them to IPFS, a decentralised file storage system, so that the banks can access them and ensure that the data being verified cannot be altered, as access to the documents is only possible using the document's hash. Registered account holders can add their documents on IPFS. Then added documents' IPFS hash is collected and stored on the blockchain with the help of the sendHash function in the deployed smart contract.

5.3 *KYC Verification*

KYC verification will be the last step that is done by the bank. A bank can initiate the KYC request for the customer and check the KYC status for the respective customer. A bank accesses the data of a customer in this step. After the KYC is completed, a bank can remove the KYC request and set the customer KYC as true.

6 Result and Discussion

With a focus on solving the issue of repetitive processes and the possibility of errors associated with the conventional KYC framework, along with people submitting false data and issues of redundancy, this work discussed a blockchain-based KYC framework.

The prototype presented has two components: an account holder (the customer) and the service provider (the bank). Once the account holder and service provider get registered in the KYC environment, the documents must be submitted by the customer and stored over IPFS, from which service providers (banks) can access and verify the same. Once the documents are submitted and verified, the customer is no longer required to take any further action for future KYC compliance, except for updating critical data as required for regulatory compliance. The system shall

Fig. 5 Transaction logs

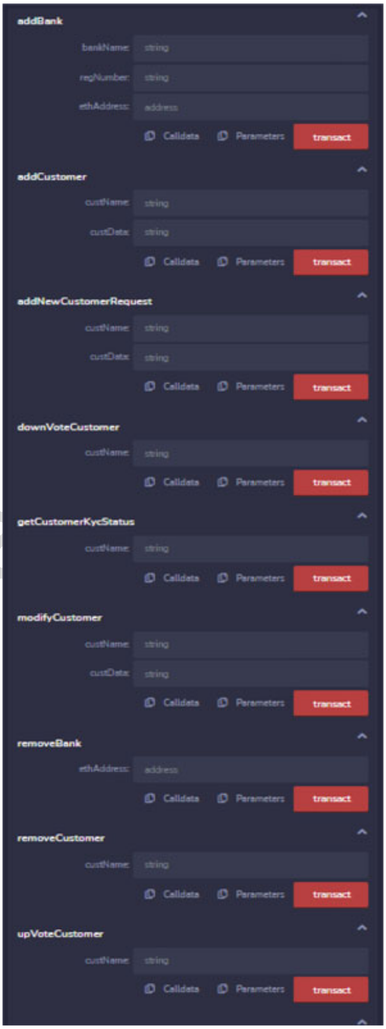


Fig. 6 Deployed contract for banks

enable single-time verification of a person, which will help not only the customer's interests by avoiding multiple verifications for the same parameters but also serve the service provider's interests by eliminating data redundancy or cases of forgery (Figs. 5 and 6).

7 Conclusion and Future Scope

With a vision for a decentralised, yet secure environment, blockchain-based solutions show a high level of benefit. The flaws of the long, inefficient conventional KYC systems can be addressed via a properly designed and implemented solution. An efficient KYC system will not only make it easier for customers to deal with repetitive work for any service needs, but it will also improve the working efficiency of the organisations, and thereby saving time, effort and money and, ultimately, improving customer services. The system can be made more secure, and the verification data can be made available to the company as per demand.

The prototype can be extended to form a cognitive verification system, based on technologies like artificial intelligence, for checking the authenticity of customer-submitted documents. There are no standard KYC procedures in the industry; a document-wallet approach based on the technologies discussed above can help counter the issue, making it more useful beyond just the use-case of banks as discussed in this work. Sufficient emphasis is needed on a resilient and secure design while putting the system to actual use.

Acknowledgement We are very thankful to Prof. S. A. Phatangare of the Department of Computer Engineering, VIT Pune, for her encouragement and guidance in carrying out this research work.

References

1. Hussain, S.A., Usmani, Z.-u.-H.: Blockchain-based decentralized KYC (know-your-customer). In: The Fourteenth International Conference on Systems and Networks Communications ICSNC 2019, Valencia, Spain, 24–28 Nov 2019
2. Singhal, N., Sharma, M.K., Samant, S.S., Goswami, P., Reddy, Y.A.: Smart KYC Using Blockchain and IPFS (2020). https://doi.org/10.1007/978-981-15-3125-5_9. https://www.researchgate.net/publication/340995551
3. Sunitha, V.: KYC verification using blockchain. Int. J. Res. Appl. Sci. Eng. Technol. **10**, 861–865 (2022). https://doi.org/10.22214/ijraset.2022.45156
4. Yadav, P., Chandak, R.: Transforming the know your customer (KYC) process using blockchain. In: 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), pp. 1–5 (2019). https://doi.org/10.1109/ICAC347590.2019.9036811
5. Parra-Moyano, J., Thoroddsen, T., Ross, O.: Optimised and dynamic KYC system based on blockchain technology. Int. J. Blockchains Cryptocurrencies. **1**, 85 (2019). https://doi.org/10.1504/IJBC.2019.101854
6. Biradar, R.R., Dakshayini, M.: Blockchain enabled KYC solutions using Hyperledger Fabric. In: 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), pp. 1–3 (2020). https://doi.org/10.23919/ICOMBI48604.2020.9203407
7. Yadav, A.K., Bajpai, R.K.: KYC optimization using blockchain smart contract technology. Int. J. Innov. Res. Appl. Sci. Eng. **4**(3) (2020). https://doi.org/10.29027/IJIRASE.v4.i3.2020.669-674
8. Mamun, A.A.I., Yousuf, M.A., Shamim Kaiser, M.: Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology (2020). https://doi.org/10.1109/TENSYMP50017.2020.9230987

9. Ullah, N., Al-Dhlan, K.A., Al-Rahmi, W.M.: KYC optimization by blockchain based Hyperledger Fabric network. In: 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), pp. 1294–1299 (2021)
10. Vitalik Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", 2014

AQ7

11. Huang, Y., Wang, B., Wang, Y.: Research and application of smart contract based on Ethereum blockchain. J. Phys. Conf. Ser. **1748**, 042016 (2021). https://doi.org/10.1088/1742-6596/1748/4/042016
12. Biryukov, A., Khovratovich, D., Tikhomirov, S.: Privacy preserving KYC on Ethereum. In: Prinz, W., Hoschka, P. (eds.) Proceedings of the 1st ERCIM Blockchain Workshop 2018 (2018). https://doi.org/10.18420/blockchain201809. ISSN 2510-2591
13. Kulkarni, V., Singh, A.P.: Sustainable KYC through blockchain technology in global banks. Annals of Dunarea de Jos University of Galati Fascicle I Economics and Applied Informatics. (2019). https://doi.org/10.35219/eai1584040929
14. Rankhambe, B.P., Khanuja, H.K.: Optimization of the KYC Process in the Banking Sector Using Blockchain Technology, 8 Feb 2021, E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
15. Sai Vikas Reddy, E., Suhag, N., Manjunath, S.: Know Your Customer (KYC) process through Blockchain. Int. Res. J. Eng. Technol. **7**, 6 June 2020, p-ISSN: 2395-0072, e-ISSN: 2395-0056

AUTHOR QUERIES

AQ1. Please check if edit to the "Abstract" text is okay.
AQ2. Please check if edit to sentence starting "The total cost of the KYC . . . " is okay.
AQ3. Please confirm the inserted citation for Figs. 2–6.
AQ4. Additional artworks "Figure 7 and Figure 8" provided in the manuscript folder. The artworks "Figure 5 and Figure 7" are the same. Hence, the repeated artwork Figure 7 has been ignored. Please confirm if okay. Also confirm the additional artwork Figure 8 can be included in the chapter.
AQ5. Please provide better quality artwork for Figs. 1, 2, and 6.
AQ6. References [6–15] were not cited anywhere in the text. Please provide in text citation or delete the reference from the reference list.
AQ7. Please provide publisher name for Ref. [10].