IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

KYC Transparency and Security for Banking using Block Chain and IPFS

Dhanraj Kadam, Varad Joshi, Dhiraj Khairnar, Gayatri Kolhe
Department of Computer Technology
K.K Wagh Polytechnic, Nashik, Maharashtra, India

Abstract: *Know Your Customer or Know Your Customer (KYC) is a financial institution's guideline for identifying customers using identity, compliance and risk assessment to build relationships in banking. With security concerns, the KYC process has become difficult and costly for a client. In this work, we propose an efficient, fast, secure and transparent platform for KYC authentication for banking institutions through the Interplanetary File System (IPFS) and blockchain technology output. The application process allows customers to open an account at a bank, complete the KYC process there, and use the IPFS network to generate a hash and distribute it using blockchain technology. After obtaining the private key, any bank/financial institution can obtain the customer's information (eg.For example KYC) If a customer wants to open another account with a bank/financial institution, use IPFS network for security. A planned process can save time, money and redundancies in the KYC process when trying to open accounts at multiple banks.*

Keywords: KYC, Blockchain, IPFS , SHA , DLT etc

I. INTRODUCTION

Banks often serve large customers in retail and commercial establishments. The "Know Your Customer" process, also known as KYC, helps organizations verify the identity of their customers. KYC is a regulatory and legal requirement that a business or financial institution must meet for new and existing customers. The main challenge of the banking industry is to control the cost of the KYC process, which negatively affects the business. The purpose of this article is to propose a new KYC verification process.

We have developed a DLT-based system that provides a solution to the additional cost of the KYC process and the lack of customer satisfaction. The main reason we use DLT is because it allows us to monitor the KYC fee structure across all financial institutions in the jurisdiction and on a consolidated basis for inefficiencies from similar transactions. In all organizations involved (for example, DLT frees us from doing all the repetitive tasks and saves more money than trying to simplify these repetitive tasks).

KYC is the process by which banks obtain information about the identity and address of the buyer. Due diligence to identify the client is a process followed by regulators. This process ensures that the bank's services are not abused. It is the company's responsibility to complete the KYC process when opening an account. Banks are also required to regularly update customers' KYC information.

KYC can be manual, time consuming and repetitive in organizations. Sharing KYC information on the blockchain will enable financial institutions to achieve better results, increase efficiency and improve customer experience. The KYC blockchain system provides transparency and immutability, allowing financial institutions to verify the authenticity of available information on DLT platforms. The decentralized KYC process is an easy way for users to access new information securely and quickly.)

II. SYSTEM ARCHITECTURE

In our proposed system, we share kyc documents with the blockchain so that documents and user details remain secure. In the above architecture, we can see that we have created a secure IPFS system, so users keep their documents and details here. In the second part, when a user needs to make a transaction from one bank to another, our system will help to provide simple KYC to send the amount easily and securely. In the image we can see that there is a strong security algorithm, so we encrypt on the one hand and decrypt on the other.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

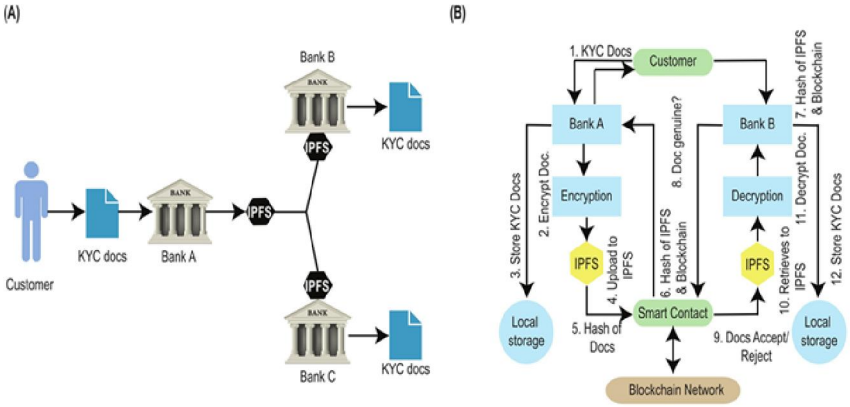
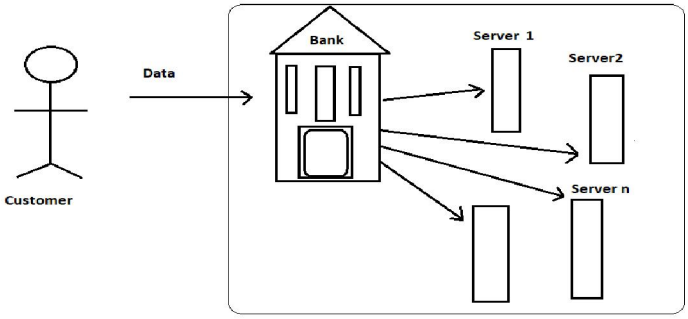


Figure 1.1: System Architecture.

Know your client (KYC) is a guideline for the banking system to validate a customer using identity, appropriateness, risk assessment in establishing a banking relationship. With the growing concern of security, the KYC process is complex and involves a high cost for completing for a single customer. sharing of confidential KYC data must be authorized by customers, and a bank-customer relationship must be kept secret from network



III. LITERATURE SURVEY

The purpose of project Pervasive Decentralization of Digital Infrastructures: A Framework for Block chain Enabled System and Use Case Analysis and their author is F. Glaser he publishes a Social Science Research Network Rochester NY SSRN Scholarly Paper ID 3052165. Is in year of Jan. 2017. And the mean purpose is Block chain 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 and it's more secure.

A lightweight multi-tier s-mqtt framework to secure communication between low-end IOT nodes and their author is A. Rahman, S. Roy, M. S. Kaiser and M. S. Islam and they publish in the

Year of 2018 5th International Conference on Networking Systems and Security. we discuss a detailed analysis of data & devices security issues and present an enhanced security model with a view to improving the security issues and its more complex

A Blockchain Framework for Insurance Processes the author is M. Raikwar, S. Mazumdar, S. Ruj, S. Sengupta, A. Chattopadhyay and K.-Y. Lam they publish in 2018 9th IFIP International Conference on New Technologies Mobility and Security. we focus on the design of an efficient approach for processing insurance related transactions based on a block chain-enabled platform and its less applicable

The Blockchain as a Decentralized Security Framework and the author D. Puthal, N. Malik, S. Mohanty, they publish IEEE Consumer Electronics Magazine, in 2018.the overview of this technology for the realization of security across distributed parties in an impregnable and transparent way and it's more costly. M. Mahmud, M. S. Kaiser, M. M. Rahman, M. A. Rahman, A. Shabut, S. Al-Mamun, et al.

This author publishes Cognitive Computation, vol. 10 in oct 2018 the TMM utilizes both node behavioral trust and data trust, which are estimated using ANFIS, and weighted additive methods respectively, to assess the nodes trustworthiness and its more time consuming

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

1. Continuous Decentralization of Digital Infrastructure :
A Blockchain-Enabled System Framework and Use Case Analysis:
Technological innovation and resulting decentralization are drivers of continuous development and increasing openness digital infrastructure and services. One of the most discussed and arguably most disruptive innovations is the distributed database technology known as blockchain. Although still in its technological infancy, experimental adoption and adaptation appears well advanced in several potential application areas, ranging from distributed computing and storage networks to global financial services. However, the technology and its development path still involve unknowns common to many practitioners and researchers.
In particular, questions about how to modify the technology or integrate it into existing digital services, processes and infrastructure.

2. Lightweight multi-layer S-MQTT framework to secure communications between low-end IoT nodes.
Internet of Things (IoT). Due to the convergence of Wireless Sensor Networks (WSN) and Internet technologies, the Internet of Things has evolved to come closer to the vision of smart cities. In the Internet of Things, in order to maintain device-to-device communication, the HTTP protocol has been used for remote monitoring and data analysis of a large number of sensing elements, but the consumption of 'energy is large, the transmission efficiency is relatively low, and it cannot be effectively used system bandwidth.
Therefore, MQTT (Message Queuing Telemetry Transport), AMQP and CoAP protocols are quite capable of handling wireless sensor traffic under very low bandwidth and limited network conditions. Security is also another major concern as IoT applications collect private data and provide access to various control functions over the internet.

3. Blockchain as a decentralized security framework :
Blockchain is becoming one of the most popular and unique cybersecurity technologies. The technology itself is in its infancy, has successfully replaced economic transaction systems in various organizations, and has the potential to revolutionize heterogeneous business models across different industries.
Although it promises to provide a secure distributed framework to facilitate the sharing, exchange and integration of information between all users and third parties, it is important that planners and decision makers thoroughly analyze its applicability in their industrial and commercial applications. Sex is important. Blockchain should only be deployed when it is applicable and offers security a better chance of increasing revenue and reducing costs. This paper describes the technique to provide security between distributed parts in an untouchable and transparent manner (IoT) and cloud computing enable neuroscientists to collect multi-layered and multi-channel brain data to better understand brain function, diagnose diseases and design treatments. To ensure secure and reliable data communication between end-to-end (E2E) devices supported by today's IoT and cloud infrastructures, trust management at the IoT and user level is required.

IV. PROPOSED SYSTEM

In our proposed system, we share KYC documents with the blockchain so that documents and user details remain safe. In the above architecture, we can see that we have created a secure IPFS system, so users keep their documents and details here. In the second part, when a user needs to make a transaction from one bank to another, our system will help with easy KYC to send the amount easily and securely. In the image we can see that there is a strong security algorithm, so we encrypt on the one hand and decrypt on the other.

V. PROBLEM DEFINITION

Know your client (KYC) is a guideline for the banking system to validate a customer using identity, appropriateness, risk assessment in establishing a banking relationship. With the growing concern of security, the KYC process is complex and involves a high cost for completing for a single customer.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

VI. ANALYSIS

Technological development and distribution benefits are the driving forces behind the continued development and increased openness of digital infrastructure and services. One of the most discussed and allegedly disruptive innovations is the distributed ledger technology known as blockchain. While the technology is still in its infancy, testing and implementation appears to be progressing in applications ranging from distributed networks to computing and storage for international financial services. However, technology and its development still have many unknowns for doctors and scientists. In particular, the question of how technology can adapt to or join the existing field of digital services, processes and procedures.

VII. CONCLUSION

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.

REFERENCES

[1]. Implementation of Least Significant Bit Image Steganography with Advanced Encryption Standard Adit Pabbi;Rakshit Malhotra;K Manikandan 2021 International Conference on Emerging Smart Computing and Informatics (ESCI) [2021]

[2]. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," IEEE Symposium on Security and Privacy, 2016, pp 839-858. "Consumer Digital Identity: Leveraging Distributed Privacy Enhancing Technology," (White Paper: Secure Key): https://securekey.com/resources/consumer-digital-identity/

[3]. E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," IEEE Symposium on Security & Privacy (Oakland) 2014,pp 459-474, IEEE, 2014.

[4]. Garman, M. Green, and I. Miers, "Accountable privacy for decentralized anonymous payments", International Conference on Financial Cryptography and Data Security (Barbados), pp. 81-98,2016.

[5]. "Zero-knowledge Security Layer to be Added to Quorum Blockchain Platform", Press Release: https://z.cash/blog/zsl-quorum.html

[6]. A. M. Antonopoulos, "Mastering Bitcoin: Unlocking Digital Crypto Currencies" (1st ed.). O'Reilly Media, Inc., 2014.

[7]. https://www.ibm.com/developerworks/opensource/top-projects/php/

[8]. www.research.ibm.com/labs/africa/project-lucy.shtml

[9]. www.idc.iitb.ac.in/projects/student/project-areas.html

[10]. www.iitr.ac.in/departments/ECE/pages/Academics+BTech_Projects.html

[11]. www.nic.in/projects/government-eprocurement-solution-nic-gepnic-20