ISSN No:-2456-2165

Document Verification using Blockchain

[1]Dr. P. Visalakshi, [2]Shourya Rawat, [3]Prateek sen
Assistant professor (Selection Grade)[1], Final year B.Tech(NWC)[2,3]
Department of network and communications SRM Institute of Science and Technology Kattankulathur campus

Abstract:- In our country, we have a centralized financial system. Customers must now update their information as part of the KYC, commonly known as document verification process. This procedure is used by many businesses and financial institutions to save data for purposes like employee and user validation. The issue with this procedure is that each time a person enters a new institution, he must go through document verification. Even at banks, he needs document verification for a variety of transactions. If he transacts, a number of steps and middlemen are involved. In order to do away with the middlemen and costs related to continuous document verification, we advise consumers to perform one-time document verification. Eventually, users will have access to this information whenever they want, wherever they are, for a variety of reasons, and in different places. The most cutting-edge technology in the world—Blockchain—will be used by our system for this, giving us a distributed environment, user transparency, and no outside interference—all of which increase system security.

Keywords:- *KYC, Blockchain.*

I. INTRODUCTION

The world's ever-evolving technologies have made nearly anything possible. Nowadays, folks only need to make a few clicks to find anything they need. As a result, we are implementing KYC using the most cutting-edge technology currently available: blockchain, to increase the usability and accessibility of user data. Distributed KYC will take the place of the conventional, centralized KYC in banking systems and be made available at financial institutions, businesses, and other comparable regions for user information verification and to reduce the ongoing job of performing KYC. Blockchain is a technology that keeps track of details by using chains of blocks connected by links. Initiatives like Bitcoin, Ethereum, and others have been made possible by the blockchain.The problems associated with centralized administration will be eliminated by the distributed environment used here, making it easier and more efficient. With the help of this technology, information security and transparency are guaranteed.Blockchain has been prepared for use in a temporal setting since Bitcoin was studied. Using a procedure called KYC, banks gather data about consumers' names and addresses. This is how banks obtain the address and identity details of the buyer. KYC could be a tool that helps companies better understand the behavior of potential customers and verify their legality. Authorities may use a method known as "due diligence" to investigate the reliability of prospective purchases. This process helps in preventing the abuse of banking services. This process helps to stop the abuse of bank services. After creating new accounts, the banks should complete the KYC procedure. Additionally, banks are required to keep the KYC data on their clients up to date.For all establishments, KYC may also be tedious, time-consuming, and laborious. Financial institutions will be able to increase efficiency, enhance client knowledge, and improve compliance outcomes by exchanging KYC data on the blockchain.This blockchain, when combined with the KYC chain, may enable decentralized knowledge storage and transparency. Sharing KYC data on the blockchain will enable financial institutions to enhance customer experiences and provide better compliance outcomes. Processing the same client information across numerous banks and financial industries is difficult because of knowledge redundancy and high maintenance costs for sensitive data. Frequently, all of the problems with the traditional approach to KYC verification can be resolved using a blockchain-based methodology. Even though we give the user power over the information, we often eliminate outside interference.

II. LITERATURE SURVEY

Bharti Pralhad Rankhambe et al. [1] developed a distributed ledger technology-based approach to reduce total KYC costs for banks collaborating with a regulatory authority while eliminating duplication of work done by various financial institutions. The integration of customer records into the bank database, along with increased transparency and a sharp reduction in expenses, all contribute to the proposed system's increased efficiency and improved customer satisfaction by doing away with the need for middlemen.

Using the consortium blockchain technique suggested by Ashok Kumar Yadav et al. [2], any company can request the data by giving a service proof of identification. To maintain track of the records, each organization is given an identity. The maintenance costs associated with maintaining duplicate information will also be avoided thanks to data being maintained online on the blockchain, which will also result in a large reduction in paperwork. The suggested method of KYC verification improves security, transparency, and privacy while streamlining the processes for storing, updating, sharing, and accessing data. It accomplishes this by utilizing the blockchain's consensus algorithm, DLT, and cryptography. In addition, it improves consumer satisfaction and encourages customer ownership. In accordance with the suggested strategy, any institution participating as a peer in a consortium network is only permitted to check the specifics—not to change them. Finally, despite the fact that internal processes within each organization are dispersed, they seem to function as a single, coherent unit from the outside. E.

ISSN No:-2456-2165

The blockchain-based method put out by Sai Vikas Reddy et al. [3] reduces the cost of the typical KYC verification procedure. The entire verification process is performed only onece for each of the institutions a customer registers with, regardless of how many of them. By securely sharing the results through DLT, this increases transparency. Here, there is no need for the consumer to register with multiple financial institutions, saving time and effort. Instead, they just need to register with one. Ethereum is employed in this method as a proof of concept (POC). This strategy increases transparency, enhances customer happiness, and reduces administrative expenses.

Syed Azhar Hussain et al. [4] suggested a method based on a self-governed and distributed Know-Your-Consumer (DKYC) architecture that improves customer privacy through the provision of prior permission, makes it easier for regulatory oversight, and enables banks to use accurate and legitimate customer details while lowering the cost of customer acquisition. The Proof of Importance consensus algorithm is used in the scoring system's construction. This makes it possible for present conventional identity establishments, such as Civilian IDs, regulators, National Security Numbers, and other private sector identity stores, to take part and be a member of the network in order to determine the scoring.

A blockchain-based strategy that removes middlemen and enables one-time KYC for users was proposed by Prof. A. L. Maind et al. [5]. Users can access the data whenever they want, from anywhere, and for a variety of reasons. Blockchain technology's security is boosted by its decentralized ecosystem, user transparency, and absence of outside interference. Also, quicker processing is promised.

IPFS is utilized in this suggested KYC document system. We suggest using these technologies to create a platform for KYC document verification in the financial system that is affordable, quick, private, secure, and transparent. The user cant upload KYC documents to the Blockchain network since it is expensive. KYC documents can instead be delivered on the Blockchain Network after being shared using IPFS. The transaction history and hashes of users can be saved to the IPFS network and shared with the Blockchain network as required. The size of the blockchain data will be greatly reduced by this process [6].

We noted in [7] that the existing KYC procedure is incredibly inconvenient and ineffective. Therefore, it is better to use a digital signature to validate the documents in order to prevent duplication and fraudulent transactions.

We found that there are a lot of problems with the current KYC verification process in [8]. Thus, using blockchain technology for KYC verification will undoubtedly assist to reduce costs.

III. ARCHITECTURE DIAGRAM

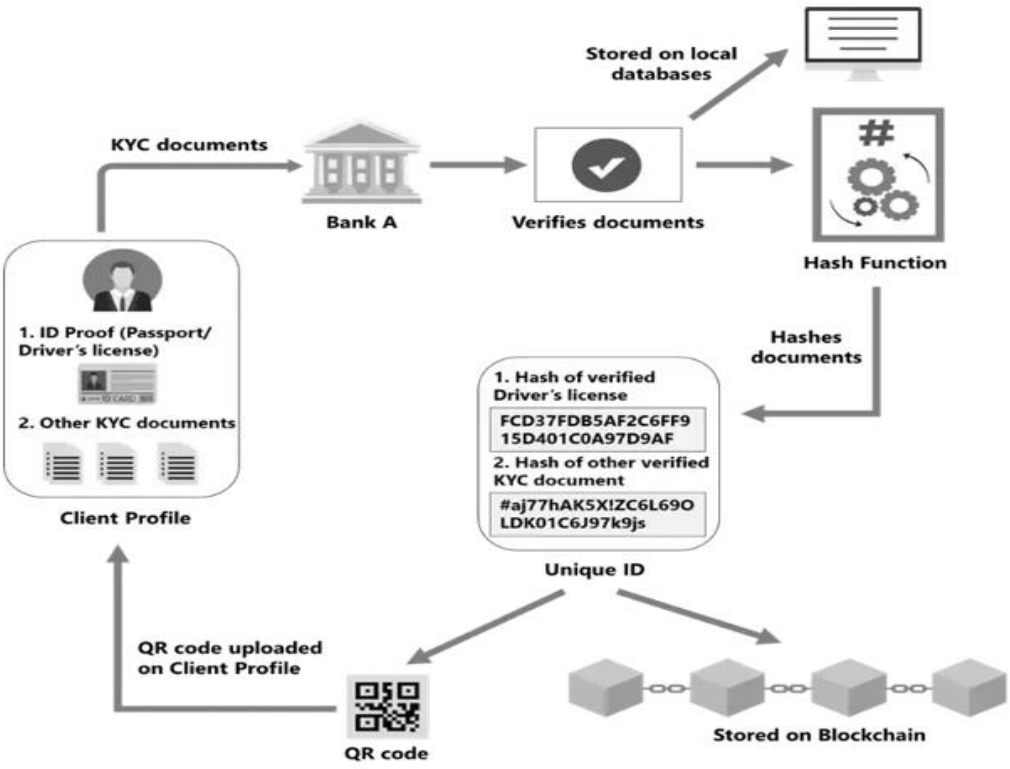

Fig. 1: Architecture Diagram

IV. PRELIMINARY CONCEPTS

Although they are closely related but not the same, blockchain, decentralization, and Web 3.0 must first be distinguished from one another before being discussed in relation to document verification. Before we discuss issues and remedies, we should also review recent advancements in document verification in India and the rest of the world. As a result, this part provides a basic overview of the ideas we will be discussing.

A. Blockchain

Blockchain is a decentralized, unchangeable database that makes it easier to track assets and record transactions within a business network. A physical asset may be tangible or intangible. All stakeholders see a reduction in risk and an increase in efficiency when using a blockchain network to record and transfer nearly anything of value [21]. As it offers real-time, shareable, and transparent data that is maintained on an immutable ledger and only accessible to users of a permissioned network, blockchain is the best solution for information sharing. The ability to trace orders, payments, accounts, and production is one of the many features of a blockchain network. Blockchain enables electronic recordkeeping, validation, and verification without the need for a middleman. Everyone who is a participant has access to the information, what is known about them is transparent, and the records are unchangeable and cannot be changed or deleted. Accountability, responsibility, openness, adaptability, accessibility, usefulness, manageability, and sustainability are its guiding principles. [2].

Blockchains could be centralized or decentralized. Yet it's important to distinguish between distributed and decentralized systems. Despite being fundamentally decentralized, a blockchain is inherently distributed (multiple parties retain copies of the ledger). [22]

B. Decentralization

Decentralization, in its most fundamental sense, is the distribution of power among many different entities. This structure is employed by many organizations to provide a more stable and power-balanced structure.

Decentralization, as used in the context of blockchain, is the transfer of power and decision-making from a centralized entity to a dispersed network. Decentralized networks are designed to reduce the amount of trust users must have in one another and to avoid user intervention that can harm the network's functionality. [23].The capacity to establish a trustless environment where users are not dependent on a central authority for the availability and caliber of resources is one of the numerous advantages of decentralization. A decentralized structure reduces the likelihood of a single point of failure. An environment where there is more accountability and transparency leads to a meritocratic system. In order to develop systems that are more dependable and sophisticated, this strategy might be developed to incorporate cutting-edge concepts like artificial intelligence. [13].

C. Web 3.0

Web 3.0 is, to put it simply, the idea of decentralization and blockchain applied to the web. Giving users ownership power instead of a centralized organization—apps, finances, and even internet services that don't need any central oversight—is a very effective concept.

Between 1990 and 2004, there was a read-only web known as Web 1.0. It could not be interacted with; it was merely a means of sharing information. Web 2.0, the next stage of the web's evolution, debuted in 2004 and has been around ever since. It has made it possible for users to communicate with one another as well as with businesses. As a result, it was a read-write web, with the only negative being that it was dominated by large monopolies and corporations. Web 3.0 is about creating a read-write web that gives users control over their content [24].

Blockchain technology is being used by Web 3.0 to transform how information is stored, traded, and owned. A blockchain-based web may conceivably change the monopoly on who controls information, who makes money, and even how networks and organizations function. Theoretically, Web3 will restore democracy to the web and usher in a new era of the internet by creating new online economies, product categories, and services. In conclusion, Web3 is a cryptocurrency extension that uses blockchain in novel ways to achieve novel goals [25].

V. METHODOLOGY

Secondary research, a literature review, interviews, and case studies—all good research techniques—were used to collect the data for this study. using a recognized technology like blockchain. The server must first receive the candidate documents. The college to which the candidate belongs has verified the uploaded documents. In the wake of the verification, these papers are maintained on IPFS. The document hash is delivered by IPFS to the server and is saved in the blockchain network with the help of smart contracts. These documents are easily seen by anyone with the proper authentication. Since the recruiter has access to these verified documents, they may rapidly investigate the employee's background. This leverages blockchain technology to streamline the hiring procedure.In a non-financial sense, it makes use of blockchain technology.

The participating banks collaborate to create a single self-verifying network, each of which operates its own systems. Following are descriptions of one such system's components.

A. Geo-address validation

For addresses located in Luxembourg, the Luxembourgish government provides a geo-address validation API that is available online. A percentage represents how close one address is to another address already in existence. Moreover, GPS information can be used for additional checks and to have the system automatically enter the correct address.

B. Peer Nodes

Peers are nodes responsible for managing network transactions. Those who want to transact are connected to these peers. There may be several peer organizations.

C. Certificate Authority

The certificate authority must present the participant's certificates. The network participants can be verified using these certificates. Each certificate authority is associated with a certain business.

D. Orderer

To ensure that every peer in the network is willing to add transactions, orderers are in charge. When a peer commits, the order is notified of the new transaction, and it immediately sends and commits that block to all adjacent peers.

E. Ganache

Its job is to safely store transaction data. By default, it includes the Hyperledger Fabric framework. These are the nodes that together comprise the organization. This concept is utilised to handle the problem with user identification and verification in our application.

VI. IMPLEMENTATION

We are developing a KYC verification solution for blockchain that will produce a block for each bank. The client is required to provide the KYC information after creating a block for each bank. The client account then uses the client account to create and store an account on the blockchain network. When you ask your bank to open an account, the data is then saved on the blockchain. In highly decentralized blockchains, highlights are usually changed or edited solely by the client, which is possible with the client's permission beforehand. When a read request is performed on the customer profile, only the chosen bank or administrator will be able to see the customer's KYC documents.Requests sent to a customer's profile can be approved or denied by them. If the client consents to the read request, the blockchain can grant the bank or administrator a complete read. to verify the validity of the customer's formal KYC documentation. Security is the primary reason for storing this customer data on the blockchain. In this market, Ganache has previous business expertise. The terminal window for your system has opened, and the Smart Remix contract is already live. Furthermore, it uses MetaMask, a very secure bitcoin wallet, to carry out transactions.

The initial step is to open a terminal and type ganache-cli on the command line. Go to the default directory in a subsequent terminal. After starting the init.js command node, execute the init.js file. In a matter of seconds, a 20-byte address is generated for the built smart contract. Open a text editor and look for the rootjscontractdetails.js file. Next, whenever you open a text editor, navigate to ContractDetail.js and enter the 20-byte address that denotes the address of the contract instance supplied in the contract variable. Here, the default text of the contract variable—which specifies the location of the contract instance—is what we want to alter. Set the addresses of the final 20 computer memory blocks after using the first 20 blocks.This program is currently available. Make sure the ganache is usable. a neighborhood Ethereum network. There are two gateways in the system: Users and Banking/Admin. Its most useful feature is the bank's or first manager's registration via a block with the bank's or first manager's name, manager's password, and registration number. There is some faint text on the ganache. It is necessary to copy and paste this signature. With the bank's or administrator's name and your signature, log in after a successful registration. Now that your bank teller or manager is logged in, you're ready to read the fine print, view your KYC, add your KYC, and update your KYC.

Choose the "Add KYC" option, input the "Non-Public Data" type, and then click the "Submit" button to complete the bank/administrator declaration. When this notification appears with your current manager or bank account type selected, click the OK button. If the user profile is successfully created, a tab similar to this one will appear; choose it by clicking the OK button. Choose the "Read KYC" tab next. Your username will be requested. After inputting the username, the user is presented with a "Access Denied" warning before being asked for authorization. After completing this process, users are then allowed to use some basic functionalities.To use the customer portal, users must provide their customer login and password. The user logs into the new account after successfully registering and continues as needed. Once the action has been entered, the user can see the fine print on the KYC Details tab, and the bank or administrator can raise questions on the Requests tab. Users decide whether or not to allow access to their data. If the user chooses to allow it, the bank or administrator may access the small print because they have permission from the user.

VII. DISCUSSION AND FUTURE WORK

The future of every industry is its complete digital transformation, which can only occur as a result of infrastructure-level upgrades. It is vital to change the core processes in order to boost operating efficiency, and this can only be done by being open to introducing cutting-edge, disruptive technologies. Our proposed solution aims to rethink the present document verification process. The current document verification process's redundancy and inefficiency problems have been fixed, considerably reducing the system's operating costs. We do away with a single point of failure by employing a distributed data storage system and a blockchain-based approach.

Our proposed method also overcomes the problem of data ownership by storing the data in an encrypted format and providing the user access to the keys required to decrypt it in a blockchain-based solution. A variety of factors will determine the kind of blockchain that is employed. The suggested approach is independent of the selected blockchain because we never store the actual customer data there. As implied by the name, anyone with an internet connection can use public blockchains. In contrast to public blockchains, a permissioned blockchain is semi-decentralized and requires an invitation from the network administrator before anybody may join. The network is governed by a variety of companies, each of which may operate a node.

Furthermore, by modifying the smart contract, we can modify the process to be applied as an identification system in sectors that require specific client information. For instance, when providing entrance to patrons in movie theaters and nightclubs, staff members should just be concerned with the patron's age; they shouldn't have to deal with any other PIE. Here, age could be verified precisely thanks to enhanced document validation. The suggested approach might be improved to ensure fair cost sharing among all involved parties for carrying out the basic document verification operation. This can be accomplished by using a token-based incentive scheme. With such a system, it would be vital to ensure that no institution could receive reimbursement without taking the required actions.

- Clients (SMEs) can store documents in a digital data room. Through financial institutions (FIs), they can exchange documents digitally.
- FIs can upload a hash of the documents for a certain SME along with a promise on the outcomes of document verification.
- Participating FIs may purchase the verification information for a specific consumer.
- It would be necessary to ensure that no institution can ask for compensation without going through the primary procedure. They would be prevented from becoming freeloaders by forgoing payment for the use of the data generated by other member institutions.
- The effects of intentional or unintended activity could be explained in terms of liability.

VIII. CONCLUSION

Complete digital transformation, which can only be accomplished through infrastructure enhancements at the infrastructure level, is the key to the future of every industry. To increase operating efficiency, it is imperative to alter core business processes, and this can only be accomplished by being receptive to incorporating disruptive and cutting-edge technologies. Our suggested way to modernize the current KYC process. The current KYC process's redundancy and inefficiency have been fixed, considerably reducing the system's operational costs. This post has offered a way to go about achieving it. We accomplish this by eliminating the possibility of a single point of failure by using a blockchain-based strategy and dispersing the data storage systems.By storing the data in an encrypted format and giving the user access to the keys needed to decrypt it in a blockchain-based system, our suggested method also solves the issue of data ownership. A variety of factors will determine the kind of blockchain that is employed. The suggested approach is independent of the selected blockchain because we never store the actual customer data there. As implied by the name, anyone with an internet connection can use public blockchains. In contrast to public blockchains, a permissioned blockchain is semi-decentralized and requires an invitation from the network administrator before anybody may join. The network is governed by a variety of companies, each of which may operate a node.

This type of blockchain can be used when sensitive data cannot be accessed via the public internet. The fact that a public blockchain makes it easier for smaller groups to join the network without the requirement for significant lobbying power to do so makes it more democratic, which is another important factor. The recommended method can also be used as an identity system in fields where fraud using identifying documents is common but verification is impractical. In such a case, a system that currently exists and has a single source of truth would be a more workable solution. By altering the smart contract, we may also adapt the procedure to be used as an identity system in industries that demand specific client information. For instance, in bars and theaters, employees should just check a patron's age to admit them; they should not be concerned about any other PIE. Here, age would be effectively checked using the improved KYC. The suggested approach can be enhanced to guarantee that each participating member pays their fair share of the costs associated with carrying out the main KYC verification procedure. A token-based incentive system can be used to achieve this. It would be crucial to make sure that no institution could request compensation in such a system without going through the essential steps.

REFERENCES

[1.] Bharti Pralhad Rankhambe and Dr. Harmeet Kaur Khanuja, “Optimization of the KYC Process in the Banking Sector using Blockchain Technology”,International Journal of Current Engineering and Technology, Special Issue-8 (Feb 2021)

[2.] Ashok Kumar Yadav and Ramendra Kumar Bajpai, “KYC Optimization using Blockchain Smart Contract Technology”,International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE) Volume 4, Issue 3, September 2020

[3.] E. Sai Vikas Reddy, Nikhil Suhag and Manjunath S, “Know Your Customer (KYC) Process through Blockchain”,International Research Journal of Engineering and Technology (IRJET),Volume: 07, Issue: 06 ,June 2020

[4.] Syed Azhar Hussain and Zeeshan-ul-hassan Usmani, “Blockchain-based Decentralized KYC (Know-YourCustomer)”,The Fourteenth International Conference on Systems and Networks Communications,ICSNC 2019

[5.] Prof A. L. Maind, Pallavi Vijay Gedam, Snehal Kashinath Chavan and Chitrali Dnyaneshwar Shinde, “Kyc Using Blockchain”,International Journal for Research in Engineering Application & Management (IJREAM), Special Issue – ICRTET-2018

[6.] Abdullah Al Mamun, Sheikh Riad Has, Md Salahuddin Bhuiyan, M.Shamim Kaiser and Mohammad Abu Yousuf, “Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology”, 2020 IEEE Region 10 Symposium

[7.] Nikita Singhal, Mohit Kumar Sharma, Sandeep Singh Samant, Prajwal Goswami and Y.Abhilash Reddy, “Smart KYC Using Blockchain and IPFS”, Springer Nature Singapore Pte Ltd. 2020.

[8.] Dr. Manoj Kumar, Nikhil, Parina Anand, "A Blockchain Based Approach For An Efficient Secure KYC Process With Data Sovereignty ", International Journal Of Scientific & Technology Research Volume 9, Issue 01, January 2020.
[9.] IBM. (n.d). What is blockchain technology? https://www.ibm.com/in-en/topics/what-is-blockchain
[10.] Rutland, E. (2017). Blockchain Byte. FINRA. R3 Research, 2.
[11.] AWS .(n.d). What is Decentralization in Blockchain? https://aws.amazon.com/blockchain/decentralization-in-blockchain/
[12.] Ethereum. (2023, Jan 20) Introduction to Web3. https://ethereum.org/en/web3/
[13.] Stackpole, Thomas. (2022, May 10). What is Web3? Havard Business Review. https://hbr.org/2022/05/what-is-web3