KYC VERIFICATION USING BLOCKCHAIN TECHNOLOGY

Nisarga Bhaskar,Prarthana Rajapurohit,Vineetha B,Prasad B Honnavalli

Semester,Department of Computer Science,

PES University ,Bengaluru

nisarga.bhaskar02@gmail.com

prarthana358@gmail.com

vineethab@pes.edu

prasadhb@pes.edu

Abstract— KYC or Know your customer is a procedure that is used for the verification and identification of the financial details and background of a bank's clients. KYC processes are used by most financial companies and banks to help in their anti-money laundering efforts. One of the major problems right now is that different institutions are using their methods and ways, leading to the lack of standardization in the processes, along with each customer finding it extremely annoying to go through this procedure with them and every bank he/she wishes to open an account in. This also means that companies cannot track the transactions done on other platforms which make each institution have its own set of incomplete data. A good amount of redundancy in the form of opportunity, maintenance, customer verification cost etc can be seen. Digitization of KYC processes has to some extent reduced the time and effort for both the customers and the service providers, but even this system comes with its flaws. The processes currently in use have a high risk of error, are tiresome, long, and repetitive creating a troublesome experience for customers. Despite all their efforts, the data is still susceptible to being stolen and misused. According to appentive.com estimates, the amount of KYC spending rose to up to $1.2 Billion in 2020 on a global level. With such huge amounts like mentioned above being spent on KYC processes one would expect them to be unhackable and issues-free. But despite this KYC processes tend to be inefficient, time-consuming, and labor-intensive to date. In this paper, we have proposed a KYC verification system that uses blockchain technology to overcome the drawbacks of the system currently in use. Distributed ledger technology (DLT) is used withdraw and cut-out the access of different third-party or mediator external agencies. Smart contracts are utilized to design the way data is handled throughout the process and how we go about it. Blockchain technology provides a safer medium of transaction over insecure methods through its security features like hashing encryption, traceability of data, and proof of work algorithm. We've used Solidity programming language that provides tools to develop smart contracts, run on Ethereum.

Keywords—KYC,Blockchain,Ethereum,Smart Contracts,Solidity

I. Introduction

New age computational automation and technologies namely Machine Learning, IoT, and Big Data, provide an optimal solution for storage, management and access problems. However, data breach is a major problem in these systems. Security, transparency, and privacy are important and paramount concerns in this day and age.Blockchain technology can provide us with efficient results with the aid of its inbuilt features of distributed ledger technology with the help of which privacy on an insecure network,reliability and accountability can be improved. Blockchain- an indestructible, unchangeable, decentralized chain of blocks managed by multiple people, across multiple blocks with the feature of recording nearly all values.Blockchain technology helps the distribution of data, utilizing data with integrity, the immutability of the data entered, security and privacy of the data.The blocks are a collection of records which are cryptographically encrypted.These records can be financial transactions or personal information or any data which can be stored in a database. Blockchain can be adjusted to work in numerous demanding areas. Here in this paper we discuss it with regard to banks, since the financial institutions can indirectly have an

impact on other domains to get more trustability and profit.

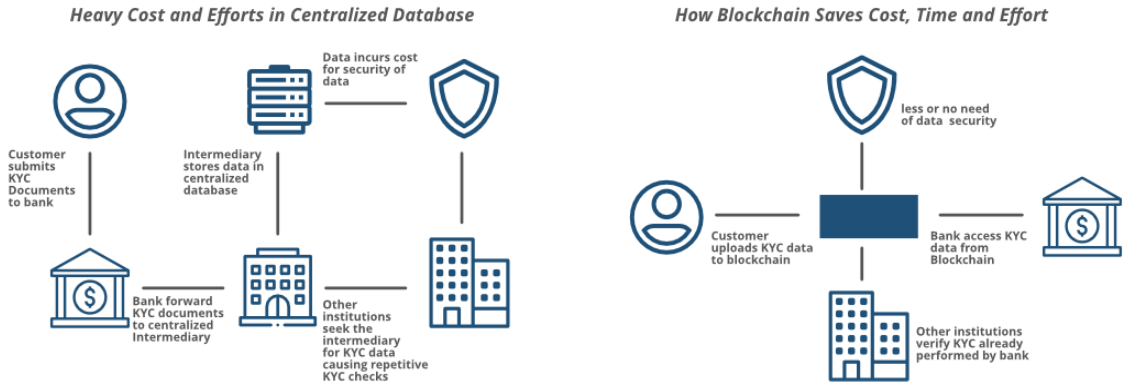

Fig 1:Existing vs the suggested system

A. Blockchain

Blockchain can be considered as one of the types of databases that stores records in blocks which are then connected to each other on the basis of various hashing techniques. At the arrival of a new record a fresh block is created and the record value is entered into it. Once the data is entered in the block, it is connected onto the preceding block, making the blocks chained jointly in sequential manner.. Each block is affixed with an component of date and time when it is connected to the chain

Blockchains can be used in a decentralized method along with proof of work which makes sure that no individual or a community has complete dominance, authority or control over the blockchain but rather, all of it's users maintain control inclusively or altogether. Decentralized blockchains are known to be immutable, which implies that the data that has been entered cannot be reversed i.e. it is irreversible. This means that transactions are not alterable thus transparent. In blockchain, each node has a reference to a complete chain which has been stored in the network, or blockchain created, since its initiation. If any node has an inaccuracy in its data it can be corrected by using the reference of the other nodes .

B. Know your customer

KYC is a shortened form of 'Know your customer'.It is an important process that every customer of the respective bank must endure to acquire any facilities offered by a particular organization.With the development in virtual cash exchange, many unethical cases have been consistently reported, thus each authority has designed a structure in which all the drawbacks of a client data is recognized and encrypted in such a way the client can be protected from any ill considered utilization of their data. .Customer acceptance policy, customer identification policy and transaction tracking are some of the policies that are measured within the structure.Blockchain technology can be used to optimize all of the above mentioned aspects.

II. Related Work

In the prevailing scenario, internet banking and online transactions along with digital information is seeing advancements day in and day out. This transformation(virtual) has led to the growth of the idea of digitized facts developing the angle of switch of facts, with effective reduction in time and fee. There is one extra idea of timestamping wherein a stamp is placed on every virtual file with TS (time of the advent of virtual file) earlier than transacting it over a community making sure that the receiver can't deny that it has now no longer acquired the transaction record . During the initial proposal of Bitcoin as an application of blockchain, there were many numerous

boundaries such as it being designed only to increase transaction of virtual currency and to eliminate the presence of a middleman to alternate the currency value responsible to each country .The blockchain has started expanding in various domains and found its application in most of the supply chain and financial and digital voting sectors .

III. Method Of Approach

Solidity is a high-level programming language It is object-oriented, and can be used for the implementation of Contracts i.e. Smart Contracts, which are programs to determine the behavior of data within the Ethereum state. Solidity is statically typed intending that the variables types are explicitly declared and determined at compile time. It supports inheritance, has rich libraries or module support and complex user-defined types among other features. Using Solidity one can build contracts for various purposes such as voting, crowdfunding, blind auctions, and multi-signature wallets.Hence it was very useful to authorize the KYC requests.It provides a platform to deploy the contracts.We use remix as an online browser solidity compiler using metamask.

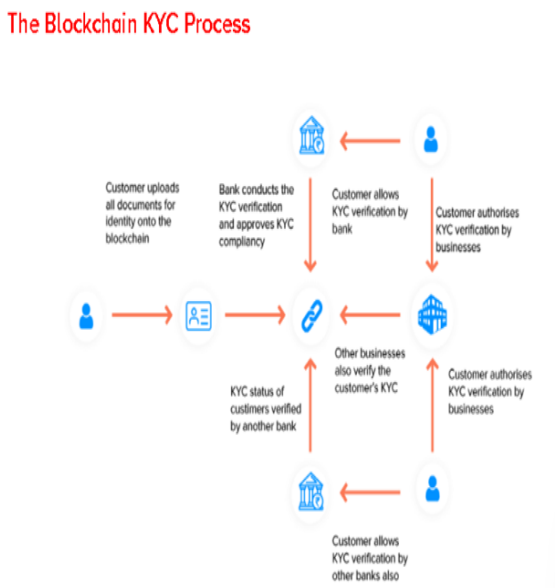

Fig 2.The KYC process[4]

The functions used for our smart contracts are described below:

IV. Approach to solve KYC verification

TABLE I

Smart contract functions.

(a) Function Name. (b) Description (c) Input (d) Response

Function-Name	Description	Input	Response
add_KYC_request()	This function adds a KYC request which is later on voted upon.	username of the kyc request and details of the customer	Integer success response
add_new_customer()	This function creates a new block containing the KYC information of a new customer.	username of the kyc request and details of the customer	Integer success response
elm_request()	This function is responsible for deleting a given kyc request	username of the kyc request	Integer success response
elm_customer()	This function is responsible for deleting a customer existing in the blockchain	username of the kyc request	Integer success response
update_customer()	This function is responsible for updating the pre-existing	username of the kyc request and details of the customer	Integer success response

	information of the customer stored in the blockchain.	to be updated	
display_customer()	This function displays the information of the customer which are sent through the other functions	username of the kyc request	details of the customer like username,data,upvotes and bank name
verify()	This function verifies a given kyc request by add_KYC_request() function	user name of the kyc request	Integer success response

V. Creating a smart contract using solidity

```
contract KYC {
    address admin;
    struct Customers {
        string username;
        string data;
        uint8 upvotes;
        address bank;
    }

    struct Bank {
        address Address;
        string bname;
        string reg_no;
    }

    struct KYC_request {
        string username;
        string data;
        address bank;
    }

    mapping(string => Customers) customers;
    string[] customer_name;

    mapping(address => Bank) banks;
    address[] bank_add;

    mapping(string => KYC_request) kyc_r;
    string[] customer_dl;

    mapping(string => mapping(address => uint256)) upvotes;

    constructor() public {
        admin = msg.sender;
    }
```

Fig. 3. Smart contract in remix.

VI. Conclusion

In this paper we showcase a system using DLT (distributed ledger technology) and blockchain for KYC verification . The additional technologies along with smart contracts and proof of work are aiding in the advancement of digital verification to the new era. We have discussed in detail the concepts this system is dependent on and the comparison of it to the existing system. This system reduces the total monetary cost, and administration expenses involved in the KYC process. These various expenses lead to major changes around the world. It minimizes the effort and time of the people by making it available real-time and online using the internet and in a very secure manner and it provides better customer experience, and is trustworthy among many financial organizations. It can facilitate more optimization by combining the blockchain methods with other complex technologies like Big data,machine learning ,IoT and AI enabling hassle-free and effortless implementation of a large population & inconsistent variations.

To summarize, this study introduces a system that permits automation and simplified and authorized information transactions between different banks. It is dedicated to minimize the constant repetition and lesser the burden required by the banks for the KYC process and provide a simpler and effective interphase for the users.

The paper provides information on how the system operates and shows the functionality of the system for the consumers and the financial institution.

In the future we would like to look into data breaches and try to come up with a solution for replication of data.[1]

VII. Acknowledgment

We would like to thank the ISFCR centre(PES University) for providing us with this opportunity and Ms. Vineetha B for guiding us through the project.

VIII. References

[1] Norvill, Robert, Mathis Steichen, Wazen M. Shbair, and Radu State. "Blockchain for the Simplification and Automation of KYC Result Sharing." In 2019 IEEE International Conference on

Blockchain and Cryptocurrency (ICBC), pp. 9-10. IEEE, 2019

[2] Moyano, José Parra, and Omri Ross. "KYC optimization using distributed ledger technology." Business & Information Systems Engineering 59, no. 6 (2017): 411- 423.

[3]Dika, Ardit, and Mariusz Nowostawski. "Security vulnerabilities in ethereum smart contracts." In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 955-962. IEEE, 2018.

[4] Bhardwaj, C., 2021. *Blockchain: The Solution to Inefficient KYC Process*. [online] Appinventiv. Available at: <https://appinventiv.com/wp-content/uploads/sites/1/2021/03/Blockchain-KYC-Process.png> [Accessed 2 January 2022].