International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

Security Management for Transaction and KYC using Blockchain Technology

S. B. Dhuttrgi[1], Trupti Banne[2], Arati Khopade[3], Anjali Kshirsagar[4], Isha Kulkarni[5]

[1]Professor, Department of Information Technology, [2]UG Student, [3]UG Student, [4]UG Student, [5]UG Student, Department of Information Technology, Bharati Vidyapeeth's College of Engineering for Women, Savitribai Phule Pune University, India

---

Abstract - Blockchain technology promises to be hugely trending and empowering in financial domain computing applications. The digital economy is becoming an integral part of modern life. So as the use of the digital world increases there are more chances of decrease is the security level. So more the use of digitization more the frauds and less the security. In some cases of personal data, leakage has brought back into the focus the security issues with the different identity sharing mechanisms. A customer is expected to provide his identity for authentication by different agencies. So, the KYC process deals with the identification of the user. And in turn, provides the required security. The KYC procedures which are used by the banks are completely dependent on the encryption which is slow and it can lead to the loss of customer details to other parties and financial institutions. This system can be efficient by using Blockchain technology, which has the potential to automate a lot of manual processes and it is also resistant to hacks of any sort. The immutable blockchain block and its distributed ledger is the perfect complement to the process of KYC. So, the banks can develop a shared private blockchain within the bank premise and the same can be used for verifying the documents. This allows the user to get control of their sensitive documents and also makes it easier for banks to obtain the documents they need for compliance.

Key Words: Blockchain, KYC verification, Security, Privacy

1. INTRODUCTION

Overview

A Blockchain-based security management system is for providing security to the bank transactions and to implement the KYC process in a simpler and secured way. Blockchain technology is a new technology which is based on mathematical, cryptographic and economic principles for maintaining a database between various participants without the necessity of any third party or central authority. It is a secured distributed database, tamper evident, wherein the validity of a transaction can be verified by parties in the transaction.

Know Your Customer (KYC) processes performed by banks on their customers are unmanageable and costly. Therefore, a system is proposed to automate unskilled tasks and allow sharing of data related to KYC. Blockchain technology, with its concept of distributed database, time-stamped ledgers, can effectively help banks improve their KYC process.

One of the main tasks of the bank is to ensure information security of data of the customers, confidentiality and the state of their account to guarantee their safety and integrity, in the process of exchange and processing of information. Thus, by using the capabilities of innovative information technology i.e., the Blockchain technology information security can be achieved.

Motivation

KYC processes are generally repetitive, incompatible, tedious and duplicated, leading to high administrative overheads and costs. A blockchain-based solution, with its immutable ledger, ease of integration, and considerably lower operational and infrastructure costs, is undeniably a better option as compared to existing KYC processes.

Banking information has always raised the interest of intruders to it, so each bank needs to organize the security of the data it stores i.e., the state of their accounts, their transaction history, etc. Blockchain is shared distributed ledger which stores transaction to a permanent chain which is unbreakable and can be viewed by the parties in a transaction. The vulnerabilities in cyber-attacks in transaction can be over-come by this technology.

2. LITERATURE SURVEY

Literature survey is the most important step in any kind of research. Before start developing, we need to study the previous papers of our domain which we are

working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers.

1. N. A. Popova and N. G. Butakova in this paper discuss the use of Blockchain technology without tokens to protect information about banking transactions, namely, transfer amounts, card details, names of participants, etc. The article analyzes the protection mechanisms of distributed databases, proposes a solution to the problem of maintaining the uniqueness of information in them based on Blockchain technology without tokens and gives recommendations on the introduction of Blockchain technology into modern banking systems.

2. J. Parra Moyano and O. Ross propose a new system, based on distributed ledger technology (DLT), that reduces the costs of the core KYC verification process for financial institutions and improves the customer experience.

3. Robert Norvill, Mathis Steichen, Wazen M. Shbair and Radu State proposed system to automate menial tasks and allow sharing of data related to KYC. A blockchain dictates the collaboration between different participants and several services are built around it to support the functionality of the system as a whole. An access control system is used to share data legitimately.

4. G. W. Peters and E. Panayi presents a work which give a diagram of the idea of block-chain innovation and its capacity to disturb the universe of managing an account through encouraging worldwide cash settlement, shrewd contracts, mechanized keeping money records and advanced resources. In such manner, they first give a concise outline of the center parts of this innovation, and in addition the second-age contract-based improvements.

5. M. Sneha, M. Vibin, R. Kanmani, S. Bhavna, A. Mohan, T. Krishnaprabhu this technology can be used for improving the KYC in many ways the feature moreover requires a fundamental reevaluating of specialized ways.

6. M. ZHANG and RUI XUE present a comprehensive overview of the security and privacy of blockchain. Firstly, they introduced the notion of blockchains and its utility in the context of Bitcoin like online transactions. Then we describe the basic security properties that are supported as the essential requirements and building blocks for Bitcoin. Finally, they reviewed the security and privacy techniques for achieving these security properties in blockchain-based systems, including representative consensus algorithms, hash chained storage, mixing protocols, anonymous signatures, non-interactive zero-knowledge proof, and so forth.

7. Eman T Alharbi, Daniyal Alghazzawi proposed framework based on the use of Blockchain technology, which add more security and better environment for authentication process. The proposed framework uses an encrypted OTP, which generated by smart contract and uses also its hash value to send it to the application/website to complete the authentication process.

3. EXISTING APPROACH

The KYC process consists of an exchange of documents between the customer and the financial institution that intend to work together. The process includes the collection of basic identity information from all beneficiaries to check for illicit activity and ‘‘politically exposed persons. The process also includes risk management with regard to onboarding new customers, the monitoring of transactions, and specific customer policies for banks. However, the KYC process is cumbersome and costly, and needs to be performed repeatedly by every bank for each of their customers. This includes redundant work that can be alleviated by trusted automation. Furthermore, the KYC process needs to be compliant with data protection regulations.

In case of bank transactions, currently, all information about cards and transactions is stored on banking servers in their centralized databases. They provide stability, ease of implementation, flexibility, scalability, performance. Due to the fact that in the modern world more and more applications are working under heavy loads, special requirements for network servers are required. From this it follows that distributed databases (DDB) are increasingly finding their use. Distributed database - a set of copied, shared and synchronized digital data, geographically distributed in different places by country and / or institution. Computers of a distributed database are called “nodes”; they are full-fledged and passive participants. In order to update the database, it is necessary to validate the full nodes. But, DDB also has disadvantages like data

compatibility, storing the system catalog, ensuring data integrity, competitive access, etc. One possible solution to these problems may be Blockchain technology.

4. PROPOSED SYSTEM

In proposed system, we implement a block chain Based KYC system, in which each customer uploads data files and encrypts these data with corresponding key. To implement both security preservation and relevant searches, we propose an effective search scheme. In this framework, the server is permitted to viably combine various encrypted records, and safely play out the pursuit without uncovering the user sensitive data, neither information documents nor the questions.

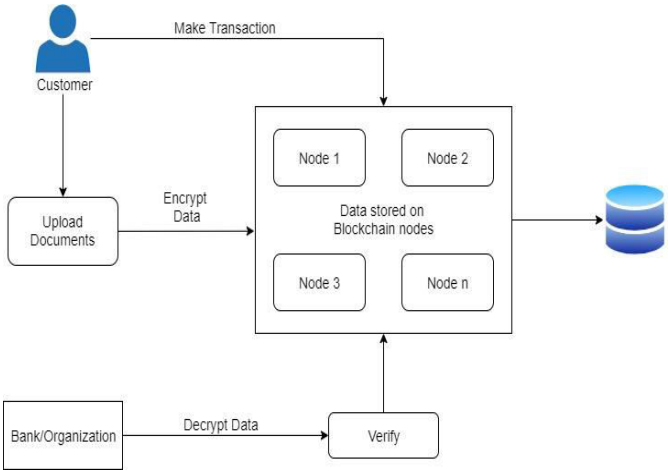

Fig. System Architecture

- If the user is going to use the application for the first time, then the user first has to register into the application to create an account. User has to enter his/her credentials like name, email address, username and password. On successful registration of the user, an account will be created.
- Once the user has successfully activated his/her account, he/she has to login into the application using the login credentials i.e., username and password.
- Once the user has logged into the application, he/she can upload all the KYC documents i.e identity proof and address proof. Documents for identity proof can be Aadhar card/PAN card and for address proof can be a driving license/passport/electricity bill. All the uploaded documents get encrypted because of which no one is able to view them except for the user. These documents can only be referred by the banks and accredited organizations. Thus, the customer has to go through the KYC verification process only once.
- After the user's KYC documents are successfully uploaded into the application, he/she can make a bank transaction easily from any bank.

5. CONCLUSIONS

In many ways, Blockchain today is comparable to where the Internet was in early 20s. The development of information technology and electronic business every day has an increasingly significant impact on all spheres of the modern life. Blockchain technology is designed to change the traditional perception of how people interact through a network. The main advantage of the Blockchain technology is the complete synchronization of processes, integrity and uniqueness of all processed information, regardless of mining and tokens. Blockchain technology helps to improve distributed databases in terms of storage, synchronization, loss and integrity of data.

Its early days, but industry leaders are sponsoring a wide range of blockchain use cases supported by industry consortiums. Having seen the potential of this technology and the challenges, we think the opportunity is clear but the blue sky is too far off and companies need to validate use cases implementing blockchain.

ACKNOWLEDGEMENT

Express my true sense of gratitude to my project guide Prof. S. B. Dhuttargi for her precious collaboration and guidance that she gave me during my research, to inspire me and provide me with all the laboratory facilities. It allowed me to carry out this research work in a very simple and practical way. I would also like to express my thanks to our HOD. Prof. Dr. D. A. Godse and Principal Dr. S. R. Patil and all my friends who,

knowingly or unknowingly, helped me during my hard work.

REFERENCES

1. N. A. Popova and N. G. Butakova, "Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transactions," 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Saint Petersburg and Moscow, Russia, 2019, pp. 1764- 1768.
2. J. Parra Moyano, O. Ross: "KYC Optimization Using Distributed Ledger Technology", Business & Information Systems Engineering59(6):411–423 (2017).
3. Norvill R., Steichen, MD., Shabbir, W. M., Radu State, R. (2019). Demo: "Blockchain for the Simplification and Automation of KYC Result Sharing", 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). doi:10.1109/bloc.2019.8751480.
4. G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in Banking Beyond Banks and Money. New York, NY, USA: Springer-Verlag, 2016, pp. 239–278.
5. M. Sneha, M. Vibin, R. Kanmani, S. Bhavna, A. Mohan, T. Krishnaprabhu, Feb.2019, "Identity Secured Sharing Using Blockchain","IJRTE" Vol.7, Issue-5S3, Feb-2019.
6. M. ZHANG and RUI XUE, "Security and privacy on Blockchain", ACM Computing Surveys, Vol.1, No.1, Page no.-1,2,3, Jan.2019.
7. T. Alharbi, DaniyalAlghazzawi; "Two Factor Authentication Framework Using OTP-SMS Based on Blockchain", Transactions on Machine Learning and Artificial Intelligence, Volume 7, 3 June (2019); pp: 17-27.