Decentralized KYC System Using Blockchain

Debabrat Parida
Information Technology Department
National Institute of Technology Karnataka
Surathkal, India
debabrataparida1247@gmail.com

Bhajan Kumar Barman
Information Technology Department
National Institute of Technology Karnataka
Surathkal, India
bhajankr328@gmail.com

Suraj Suthar
Information Technology Department
National Institute of Technology Karnataka
Surathkal, India
imssuthar@gmail.com

Abstract-Know your customer or simply KYC is the process of validating and verifying the identity of its users and examining potential risks of illegal intentions for the business relationship. A few problems with the existing manual KYC process are that it is less secure, time consuming and costly. With the advent of Blockchain technology, its properties such as immutability, security, decentralization make them a good solution to such problems. While commercial solutions like "kyc-chain.com", "KYC.legal" have the right to enable blockchain-based KYC verification, it provides a method for documents to be validated by a trusted participant in the network. In this work, an Ethereum based KYC Blockchain system using a symmetric SHA encryption mechanism is proposed. This system ensures transparency by a distributed ledger, secured by cryptography hashing.

KeyWord: Blockchain, KYC , Decentralized, SHA

I. Introduction

A bank or a financial institution typically caters to a large client base in both retail and corporate sectors. The 'Know Your Customer' process, better known as KYC, helps these institutions verify the identity of their clients. KYC is a regulatory and legal requirement that must be fulfilled by the companies or financial institutions for both new and existing clients. One of the prominent challenges the banking sector faces right now is the increased regulatory cost of the whole KYC process. This is supported by the global surveys conducted by Thomson Reuters (2016) which revealed a single clear message: the costs and complexity of KYC are rising and are having a negative impact on their businesses. The survey further cited that while financial firms' average costs to meet their obligations are $60 million, some of them have had to spend up to $500 million on compliance with KYC and Customer Due Diligence (CDD). The fines levied on financial institutions for their misconduct in various domains including KYC regulations further aggravate the situation. The fact that corporations can only grant KYC verification to their subsidiaries or customers post laborious background checks, etc, indicates that 89% of customers

do not have a good KYC experience. The aim of this paper is to propose a new approach to the traditional KYC verification process. In the light of the problems faced in the banking industry, regarding the lack of customer satisfaction and increased costs of the KYC process, we propose a Blockchain based solution. A decentralized KYC Decentralized application where banks come together and join the consortium blockchain network to ease the process of KYC.

II. Literature Survey

Several works carried out related to optimizing KYC processes in the blockchain were studied and are summarized as follows: across the industry, multinational companies implement their authentication software which is based on the OAuth protocol (open standard). However, it is understood that they serve as centralized trusted authorities and there is no widely accepted decentralized authority for storing private data and approving the identity of individuals with respect to security . The researchers have developed various techniques addressing privacy and security concerns on KYC data and few of them are discussed to understand the contribution of our proposed system.

1.Transforming the Know Your Customer (KYC) Process using Blockchain

Author: Piyush Yadav, Raj Chandak

In this paper, they proposed a new solution based on Distributed Ledger Technology or Blockchain technology, which will reduce the traditional KYC verification process cost for Institutions and cut short the general timeline of the completion of the process while making it smoother for the customers. Major enhancement in the solution over the conventional methods is that the whole verification process is conducted only once for each customer, irrespective of number of institutions he or she wishes to be linked to. Also, since they are using the DLT, verification results can be securely shared with the customers thereby increasing transparency. Following this approach, they developed a Proof of Concept (POC) with the Ethereum API, websites as endpoints and an android app as front office; realising the feasibility and effectiveness of this approach. All in all, this approach improves customer experience, reduces cost overheads, and increases transparency in the process of onboarding a customer.

2.Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology

Author: Abdullah Al Mamun,Sheikh Aias Hasan, Samim Kaiser

In this paper, they proposed a system that allows a customer to open an account at one Bank, complete the KYC process there and generate hash value using the IPFS network and share it using the blockchain technique.Upon receiving the private key , any Bank can retrieve , store customer data securely using IPFS network if the customer wish to open another account in that Bank organization . The system can save time, money and repetitive work during the KYC

process when someone tries to open an account at multiple banks.

3.Optimised KYC Blockchain System

Author: N. Sundareswaran , S.Sasirekha, I. Joe Louis Paul, S.Balakrishnan

In this work, an Ethereum based Optimized KYC Blockchain system using symmetric AES encryption and LZ based compression mechanism is proposed. This system ensures transparency by a distributed ledger, secured by cryptography, efficient by compression algorithms and optimized by blockchain features.

III. Methodology

In this paper we have designed and implemented a Decentralized application for KYC verification using blockchain.

We have done this in the following steps.

Step I: Designed a smart contract and implemented it in the solidity language.

Step II: Designed User Interface for the application and implemented using React framework.

Step III : Designed the backend to handle all the requests from the frontend and implemented using Nodejs.

Step IV : The Decentralized KYC application runs on an ethereum network.

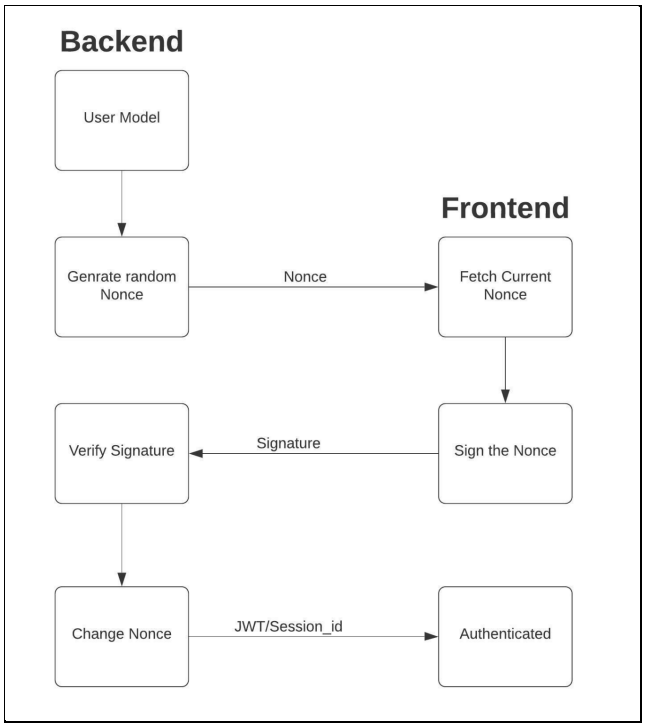

Fig 1. Authentication flow

- Login flow initiates by generating a one-time nonce from the backend and storing the public address to the nonce pair in the cache.
- User interacts with Metamask to sign this one time nonce. Metamask uses the user's public key and sings the nonce.
- The signature generated using metamask is then sent to the backend to verify the signature.
- Over the backend, given the signature from the front-end and the nonce stored in cache in the first step, the signature is verified using the elliptic curve digital signature algorithm giving back the public address of the user.
- The required authentication is done using the retrieved public address and a jwt token is being generated.
- Once the user is authenticated, the nonce for that user is updated for security reasons as it

should not be reused to sign the transaction again.

Steps to run the Application:

- Run the Ganache application. Create a new workspace with the standard configuration.
- Compile and deploy the smart contract. truffle deploy --reset
- Look out for the kyc contract address from the logs above. Update the following address in constants file available at this location ./app/constant.js
- In the same file update the admin address. Choose any one account and use its public address as the admin account.
- update the *userList* by the public addresses that you will be using as banks for testing.
- start the node js application located at ./app using command : npm run start
- Start the react client application located at ./client using command : npm run start
- The react application will run at http://localhost:3001/
- Connect to a new custom RPC in the Metamask plugin with the configurations same as that used for ganache.

IV. Results and Analysis

KYC DApp Features:

- One click authentication with Metamask.
- Role based authorization.
- Admin can verify banks and add them to the network.
- Banks can upvote other banks. Based on the votes, the bank rating is being calculated.
- Banks can add the customer KYC request and can process it further for verification by other banks if and only if the other rating of the bank is more than 50%.
- Banks can verify the data of the customer and up-vote the verification request raised by other banks.
- Customer's KYC request is considered valid if the customer request's rating is more than 50%.

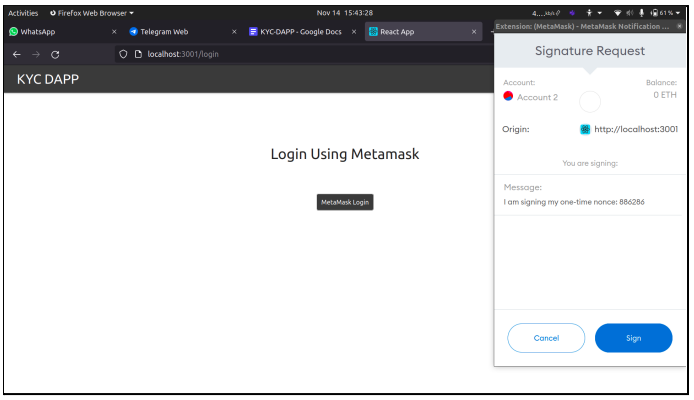

Fig 2. Login using Metamask

Fig 3. Admin: Add bank and Remove bank

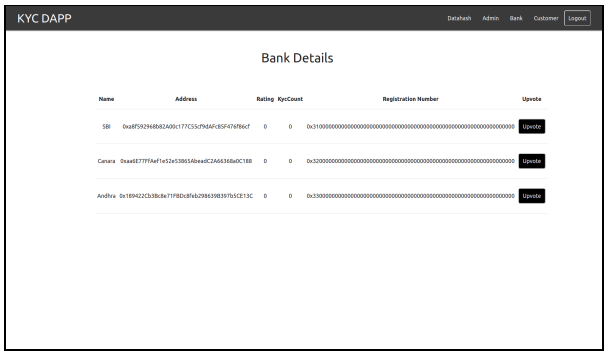

Fig 4.Showing Bank Details

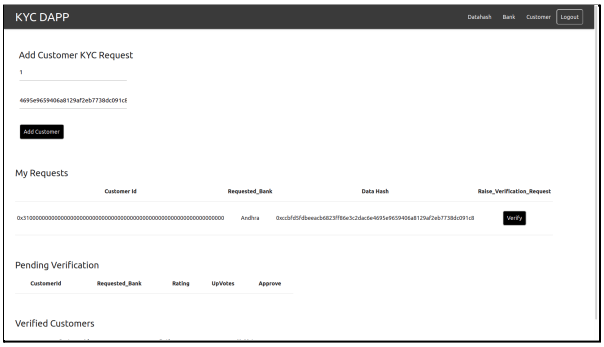

Fig 5. Customer KYC request

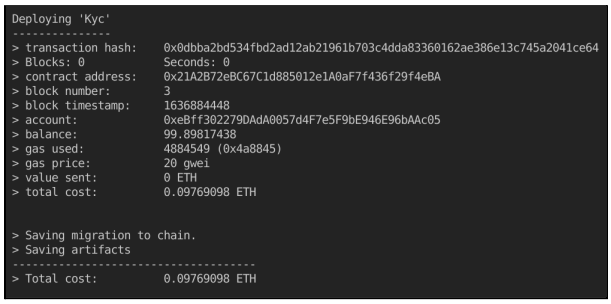

Fig 6. Showing the deployed smart contract

V. Conclusion

The proposed solution addresses the problem of redundant registration in the KYC process encountered in the existing situation. The KYC verification is done in a decentralized manner.The application will be useful for both banks and customers. A lot of time and paperwork can be saved using the Decentralized KYC application. User Details are permanently stored in a blockchain and can't be tampered by any user.

References

[1] José Parra Moyano and Omri Ross, "KYC Optimization using Distributed Ledger technology", Springer -Business & Information systems Engineering, , pp-411-423, vol.59,2018.

[2] G. Zyskind, O. Nathan and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", IEEE Security and Privacy Workshops, San Jose, CA, 2015.

[3] Mauro Isaja and John Soldatos, Distributed ledger technology for decentralization of manufacturing processes,IEEE Conference on Industrial Cyber-Physical Systems (ICPS) 2018 at, St. Petersburg, Russia, pp 696- 701,2018..

[4] Rui Yuan, Yu-Bin Xia, Hai-Bo Chen, Bin-Yu Zang, Jan Xie and ShadowEth: Private Smart Contract on Public Blockchain, Springer, Journal of Computer Science and Technology, Issue 3, pp 542–556. vol 33,2018.

[5] M. Harrop. "Know your Customer (KYC) Independent Survey." Thomson Reuters.

[6] "How Do Ethereum Smart Contracts Work?" CoinDesk.https://www.coindesk.com/information/ethereum-smart-contracts-work/

[7] "Learn About Ethereum." Ethereum. https://ethereum.org/learn/#ethereum-basics

[8] Petar Maymounkov and David Mazieres, "Kademlia: A peer-to- peer information system based on the xor metric", Business & Information Systems Engineering Journal, 2002

[9]S.Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", International Conference on Financial Cryptography and Data

Security, 2009

[10] Shbair, Wazen & Steichen, Mathis & François, Jérôme and State, Radu“Blockchain Orchestration and Experimentation Framework: A Case Study of KYC”, IEEE/IFIP Network Operations and Management Symposium,

[11] PaulJ.Taylor, TooskaDargahi, AliDehghantanha, Reza, M.Parizi, Kim Kwang and RaymondChoo, A systematic literature review of blockchain cyber security. DigitalCommunication and networks,", Elsevier Feb 2019

[12] Zhang F, Cecchetti E, Croman K, Juels A, Shi E. Town crier: An authenticated data feed for smart contracts. In Proc. the 23rd ACM SIGSAC Conf. Computer and Communications Security, ,pp.270-282, 2016