Identity Secured Sharing Using Blockchain

M. Sneha, M. Vibin, T. Krishnaprabu, Aishwarya Mohan, R. Kanmani, S. Bhuvana

Abstract--- Frequent 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 personal identity for the authentication by different agencies. The KYC procedures which are used by the banks is completely dependent on the encryption which is slow and it can lead to the loss of customer details to other theirs party financial institutions. This system can be efficient by using the Blockchain technology, which has the potential to automate a lot of manual process and it is also resistant to hacks of any sort. The immutable blockchain block and its distributed ledger is the perfect complement to the opaque process of KYC. With the addition of the smart contacts fraud detection can be automated. For KYC identity details storage, 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.

I. INTRODUCTION

KYC (know your customer) is the common procedure which are used by the banks and the financial institutions to obtain customer information like Aadhar card, PAN card and the address proof .Current KYC procedures which are used by the leading banks and financial corporations around the world are completely dependent on the human beings. KYC rules is used for mandating every customer of the bank to prove the authenticity of their existence by submitting the proof of identity and the proof of address .As the result banks across the world spends a lot of resources on the KYC process which involves collecting, tracking and storing the huge amount of data, so that it may be reported to regulatory agencies in a timely fashion. the emergence of the digital wallets like patym means that the same KYC procedure has to be repeated several times by the various companies and stored in all of their separate databases. these databases are prone to hacks and also causes a lot of data redundancy and data theft. these KYC documents that are required to establish the customer's identity at the time of opening of savings bank account ,fixed deposit, mutual funds etc. KYC documents has been made mandatory along with the photograph of the customer because of fraud accounts and money laundering .thus to reduce as much fraud as possible and as an anti money laundering parameter .the blockchain is the best platform which enhances the security value of the information. Blockchain can enable us to storing the data on a decentralized network which makes use of the unused space on people's devices across the world to store files. this technology is effective that can help prevent data breaches in the financial sector. And it is a secure and reliable method which can be used for storing the sensitive data. the blockchain network can be public or private depending upon the use case which enhances the security of the application. the detailed description regarding the transaction is recorded and the main feature is that it is immutable. No hackers can change the data which has been recorded. this is pretty well suitable for financial applications .

II. LITERATURE SURVEY

The technology which was used before hand for storing the data is the encryption technique. Considering the openness and cross domains the identity is been stored by means of encryption. Identity based encryption is been used as the substitute to public key encryption .It is invoked by using the private key generator (PKG) throughout user revocation. the sender has access to the public parameters of the system and can encrypt a message using the value. the receiver obtains the decryption key having the trusted mechanism. the encryption schemes are currently based on the bilinear pairings. the advantage of this identity based encryption scheme is that it is better for finite numbers of users, after all users have been issued with keys the theirs party's secret can be destroyed. In the other method the efficient searching on encrypted data sent to the cloud with the equality test which has been identified as the better solution. the users can search on the outsourced data to determine the two ciphertexts are the encrypted version of the plaintext .Such techniques are inefficient particularly for deployment. the identity based encryption and the identity based signature are used along with the authentication protocol for the cloud computing for storing the user details which has the high scalability. the anonymous multi receiver encryption scheme can not only protect the privacy of the receiver but also ensures the security of the message. However the computational cost of this scheme is very larger. It is not suitable for the sender which has the limited source such as the mobile nodes. the sender can encrypt the message using the unique information of the user as its public key .the receiver obtains the information via the central authority.

The blockchain based techniques is been preferred nowadays for the secured sharing of the identity for the banks or the financial sectors. there are many platforms which can restrict the access for the network on public or private scale.

Manuscript received February 01, 2012. (Fill up the Details)

M. Sneha, Final Btech IT, Sri Krishna College of Technology. Coimbatore, Tamil Nadu.

M. Vibin, Final Btech IT, Sri Krishna College of Technology. Coimbatore, Tamil Nadu.

T. Krishnaprabu, Final Btech IT, Sri Krishna College of Technology. Coimbatore, Tamil Nadu.

Aishwarya Mohan, Final BE CSE, Sri Krishna College of Technology. Coimbatore, Tamil Nadu.

Dr.R. Kanmani, Associate Professor, Department of Information Technology, Sri Krishna College of Technology. Coimbatore, Tamil Nadu.

Dr.S. Bhuvana, Associate Professor, Department of Computer Science and Engineering, Sri Krishna College of Technology. Coimbatore, Tamil Nadu.

the consumer can become the owner for his information on board.

III. SYSTEM DESCRIPTION

The blockchain contains the details of the consumer that is the person's KYC documents such as aadhar card, pan card etc. And these details are being stored in the block along with the hash value. the hash value includes the previous hash and the next hash, more or less like a linked list fashion. the Ethereum is used as the platform for this application. By using the ethereum we can create an public or private network based on the need of the application .

IV. PROPOSED SYSTEM

When a person requests, the requested transaction is broadcasted into a peer to peer network considering them as the nodes. then the validation of the records happens and the users is verified using the algorithms. A verified transaction is done by the miners who mine the ethers by setting the gas limit and the logic for the block is done by the writing the smart contracts in the solidity language. Once the details is verified it is been added as the block and each and every entity will be updated in the ledger. the details cannot be changed and hence it registers the trustworthy behaviour of the blockchain network. And finally, the block is added to the blockchain network. Ethereum platform is best suitable for the creating the business level applications ensuring the privacy between the nodes of the blockchain network.

V. METHODOLOGY

The KYC details of the consumer stored based on the particular venture tie up. the user who wishes that their details which can be shared to the other theirs party group of the financial organisation .the user will have his /her own privacy regarding their identity which when shared. the accumulation of the user has the rights when other theirs party group wanted the user's details ,the particular request will be first be displayed to the user's device .the user is the one who decides whether he /she can accept or reject the request. A decentralised infrastructure, the blockchain network will allow the accumulation of the data from the various multiple authoritative service establisher into a immutable secured storage entity. this technology allows for the creation of the e ledger which is distributed in nature and then it is shared to the all the nodes in the network. In this new infrastructure the data access will merely based on the user consent. the ownership of the data will always remains with the user. with this solution ,the identity management system will offer better data security by ensuring the data access is given only when the confirmation is received from the person concerned. this will eliminate the chance of the unauthorized access of other theirs parities.KYC work flow is been coded into smart contracts .with the help of the shared ledger ,the numerous financial organisations are maintaining the ledger ,the process of KYC could be easily adjusted and it can be monitored by all other nodes present in the blockchain network. this will help to improve the transparency in customer identification and thereby will improve the process and can prevent the fraud occurring .KYC can be managed by the decentralized applications that conduct KYC checks the entire system. the Ethereum is the platform for developing the decentralised application . Ethereum is without any chance of fraud, censorship, or theirs-party interference. the Evm (Ethereum Virtual Machine) is the runtime environment for the deployment of the smart contracts. the interaction with the application can be done in several ways such as web3js,metamask and mist. the difference is web3js mostly used by the developers whereas the mist and the metamask is used by the non technologist. the KYC application is deployed in metamask. To start with the metamask, the account creation is mandatory and the login credentials must be set. After logging into the metamask we will be provided with the different kinds of network such as main network, which is a public network and the other networks such as Ropsten, Rinkeby and localhost. In Ropsten Network, we can easily deploy our smart contracts with the free ethers. Gas is necessary for executing the contracts. Before the deployment, the specification of gas limit and the gas price is done by the user so this gas which used for the calculation of ether must be paid to the miner. When the gas exceeds the gas limit before the completion of the contract, the miner will automatically add the block into the network. thereby ending the gas flow error. So ethers are not refunded in case of gas flow error. In order to prevent the wastage of ether, it is recommended to deploy into the test network like Rinke by before deploying into the main network. this test network will automatically calculates the gas and thereby the deployment of the smart contract is done by using the fake ethers. these fake ethers can be obtained from many websites. After deploying into the Rinke by network, added blocks can be viewed through the Ether scan which provides the detailed information regarding the transactions. If the test is successful, the deployment can be done in the main network.

Ether = Tx Fees = Gas Limit * Gas Price

GAS LIMIT:

the gas is described as the gas limit ,Gas is a unit that is translated further into Ether and used as the cost for the work.

It is based on the rule of thumb which is stated as *If you want to pay less and are lowering the gas limit below the recommended gas limit, then this will not work.* Instead, try lowering the gas price.the minimum gas limit for transaction is twenty one thousand and more the amount to execute any fallback functions if it's sent to a contract, but the actual blocks also have a gas limit that specifies the maximum amount of gas all transactions in the block can consume. thereby by setting the gas limit and the gas price the working can be executed in the ethereum platform. the minning is done before the addition of the blocks into the blockchain network. Once when the ledger is connected to the metamask .these are the following steps which must be followed :

Once you connect your Ledger, you' all be able to

- Sign transactions
- Sign messages

- Check your Ledger account's Eth or token balance.

VI. FIGURES

The figures include the components of the decentralized network, the ether scan regarding the transaction details including the gas limit, gas price, value etc and the next is the blockchain network flow diagram.

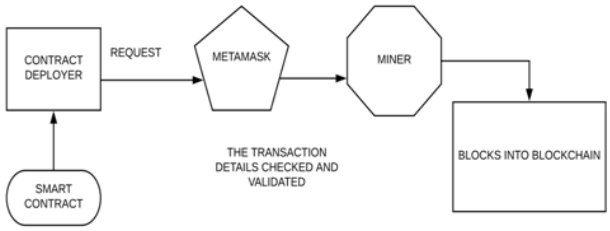


Figure 1: Workflow Model

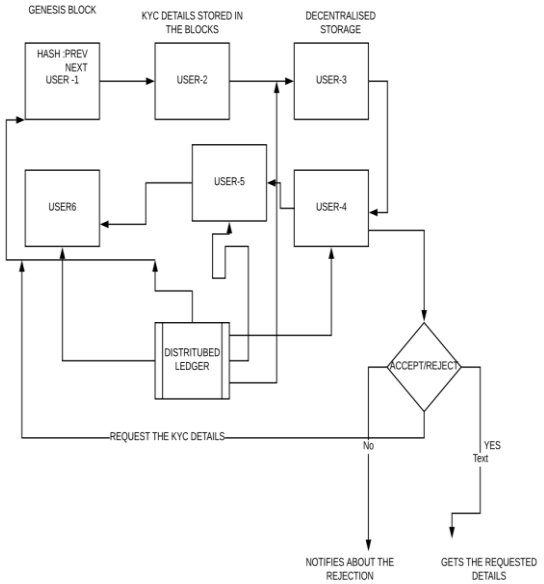
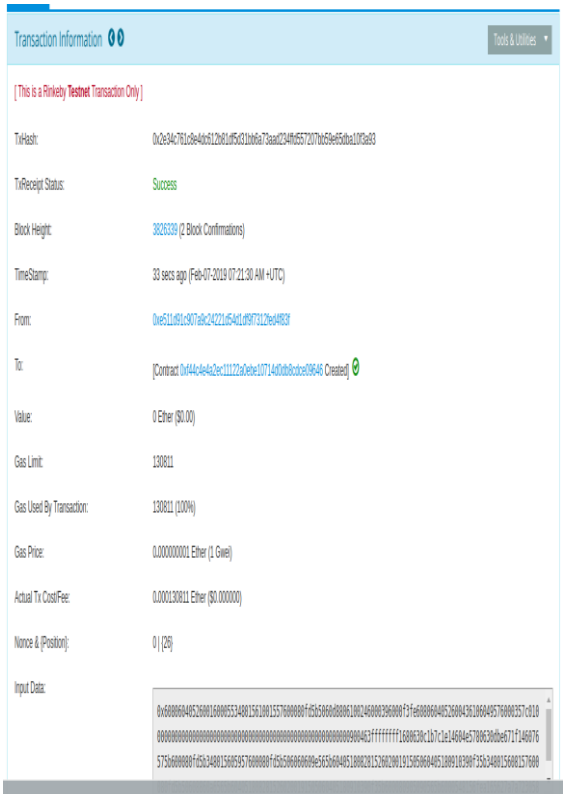


Figure 2: Blockchain Network

VII. CONCLUSION

The blockchain technology offers the best platform for the financial applications .And this technology can be used for improving the KYC in many ways .the feature underlying immutability is used for enhancement of the transparency and the identification of the details of the customer. there is a wider scope of the application among the industries that require authenticated user identification .the security which is offered by this technology makes the chance of reducing the fraud .the increasing demand demand for the banks and other financial institutions to create application which allows the user for conducting online banking .Having the direct access to a shared ledger would help the institutions save the time . the future enhancement of this technique can be made digitalised by using the other platform of blockchain technology which is made featured ahead of ethereum platform. this application can be made public which can include multiple number of nodes .Since all data is stored in a homogeneous blockchain, resulting better governance and use of data would help banks detect fraud at an earlier stage. Manual error while performing the KYC initiation can be avoided. the trust factor in the veracity of blockchain is built on the fact that the verifying parties are doing their job with due diligence. To this end, the authenticity of data depends on the integrity of the 'Trusted Parties' to ensure the data is valid.

VIII. RESULTS



Etherscan Screenshot

REFERENCES

1. Identity-Based Encryption - Applied Cryptography Group https://crypto.stanford.edu/ibe/
2. Identity Based Encryption - Applied Cryptography Group – Stanford crypto.stanford.edu/~dabo/cs355/lectures/IBE.pdf by D Boneh
3. Identity-Based Encryption | Computerworldhttps://www.computerworld.com/article/2551479/.../identity-based-encryption.html
4. Identity Based Encryption: An Overview - CSE@IIT Delhi www.cse.iitd.ernet.in/~ssen/csl863/ibeIntro.pdf
5. Githeub - decrypto-org/blockchain-papers: A curated list of academic https://githeub.com/decrypto-org/blockchain-papers
6. Applications of Blockchain Technology beyond Cryptocurrency – arXiv https://arxiv.org/pdf/1801.03528
7. Public Blockchain White Paper - OneLedger https://oneledger.io/whitepaper/oneledger-whitepaper.en.pdf
8. Introduction to Solidity Programming and Smart Contracts (For ... https://medium.com/.../introduction-to-solidity-programming-and-smart-contracts-for-...
9. Solidity Documentation - Read the Docs https://media.readthedocs.org/pdf/solidity/develop/solidity.pdf
10. What is Ethereum? the Most Comprehensive Beginners Guide https://blockgeeks.com/guides/ethereum/

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication