IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303173|

Blockchain Powered Know Your Customer (KYC) Verification

D. Venkata Harshini[1], V. Keerthi Vardhani[2], V. Sasi Priya[3]

U.G. Student, Department of Computer Engineering (CIC), Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India[1]

U.G. Student, Department of Computer Engineering (CIC), Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India[2]

U.G. Student, Department of Computer Engineering(CIC), Vasireddy Venkatadri Institute of Technology , Nambur, Andhra Pradesh, India[3]

ABSTRACT: Know Your Customer (KYC) verification in banks refers to the process by which banks verify the identity of their customers before establishing a business relationship or conducting financial transactions. The Know Your Customer (KYC) process is now important but trivial problem in the financial sector. But the problem with this process is user has to do KYC every time whenever he goes to new institution for various purposes. Even in banks for different transactions he needs KYC. This project aims to provide a solution to this problem. We designed a blockchain-based solution that works unified KYC verification and maintains a unified security database, eliminating the need for multiple KYC checks. Only With the user's permission, there will be various financial institutions, to gain access to the user KYC information you must be present on the blockchain network. Since the user has control over the data, we even remove third-party interventions. It's up to the user to accept or decline the bank's request to view their KYC information. Financial institutions would be able to produce better compliance results, efficiency gains, and improvements in customer experience by sharing KYC information on blockchain. Later user will be able to access this information anywhere anytime for different purposes at different places.

KEYWORDS: Distributed Ledger Technology, Security, Transparency, Legitimacy, Digital Identity, Blockchain Technology.

I. INTRODUCTION

KYC is the process by which banks collect information about customers, identities and addresses. Due diligence is a process that is overseen by regulators and serves to confirm the legitimacy of clients. This process helps prevent misuse of bank services. KYC process must be completed by banks while opening new accounts. In addition, banks are expected to regularly update KYC information for their clients. The main disadvantages of traditional KYC are that it is manual, time-consuming, requires third-party involvement, and is redundant across institutions. We intend to overcome these drawbacks with our proposed blockchain-based approach. We intend to simplify the KYC verification process by enabling banks to perform a one-time KYC check that can be accessed by multiple financial institutions through the blockchain network. We even eliminate the need for redundant KYC checks, saving time. Any business can request data by presenting a service proof of identity using a consortium blockchain approach. Each organization will receive an identity to track their records. Storing data online on the blockchain will also eliminate maintenance costs associated with duplicate information and significantly reduce paperwork. The proposed KYC authentication approach optimizes data storage, update, sharing and access processes while enhancing security, transparency and privacy. It does this using Distributed Ledger Technology (DLT), cryptography and the blockchain consensus mechanism. Additionally, it increases customer ownership and enriches the customer experience. Each institution acting as a peer in the consortium network under the proposed approach is only able to verify the details, not edit them. Finally, while the internal operations inside each business are spread out, from the outside they appear as one cohesive unit. proposed a blockchain-based approach that reduces the cost of the standard KYC verification process. Regardless of the number of institutions each customer registers with, the entire verification process is performed only once for each, increasing transparency by securely communicating results via Distributed Ledger Technology (DLT). Here, the customer

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303173|

registers with only one financial institution, reducing the need to register with different financial institutions and eliminating duplication of effort. With this approach, ethereum is used for proof of concept (POC). This approach increases customer satisfaction, increases transparency and reduces overhead costs. With security concerns on the rise, the KYC process is complex and involves high completion costs for a single customer. In this work, we propose an economical, fast, secure, and transparent KYC document verification platform for the banking system through the Interplanetary File System (IPFS) and blockchain technology. The proposed system allows a customer to open an account with one bank, complete the KYC process there, generate a hash value using the IPFS network, and share it using blockchain technology.

II. LITERATURE SURVEY

In [1] we discovered that there are many unsolved issues with the existing KYC verification process. Hence, if we use the blockchain technology for the KYC verification, it will definitely help in decreasing the expenses.
In [2] we observe that to make an efficient KYC verification system using blockchain, we do not require any regulators, third parties or middlemen to interfere between the process. The KYC process will be distributed and won't be governed by any financial institutions. Further, the system can easily verify someone's identity and retrieve the documents from the blockchain.
In [3] we observed that the current KYC process is very inconvenient and inefficient. hence using a digital signature to verify the documents is a better way to avoid redundancy and fraudulent transactions.
In [4] we found out that a blockchain uses a peer to peer communication network where its nodes communicate with each other and keep the data secure. Moreover, a customer can encrypt their transactions using hashing algorithms. This makes sure the transactions and other data stays safe, also all the nodes in a blockchain reflect the same changes.

III. EXISTING SYSTEM

The KYC verification process is the backbone of any financial institution. If it's not done right, the institution can suffer huge losses through fraudulent transactions. It became mandatory for every financial institution to verify the KYC documents of their customers to prevent malpractices such as money laundering and illegal funding. The current KYC process works such that an individual who wants to work with any financial institution is required onboard with valid documents. The identity, address, and sometimes biometrics are verified during KYC verification. Further, these documents are authenticated by the banks and then only the customer is trusted. The customer needs to follow this procedure every time with a new financial institution. It is a lengthy and tiring process for both parties, especially for the customer as the middlemen extort money from them for passing the documents. In the diagram below, we can see that a customer needs to carry the same set of documents to bank A, bank B, and bank C for the KYC verification process. In India, a person can use documents such as an Aadhar card, Pan card, Voter ID, Driving license, and passport during the process of identity verification. Also, other than their own safety, banks follow the KYC process strictly because the Indian government has made it mandatory. Moreover, if the banks don’t follow the process, they are heavily fined.

Disadvantages of Existing System:

1. Centralized Architecture
2. Lot of fraud because of lack of transparency
3. Not trustworthy
4. Time consuming process for recruiters

IV. PROPOSED SYSTEM

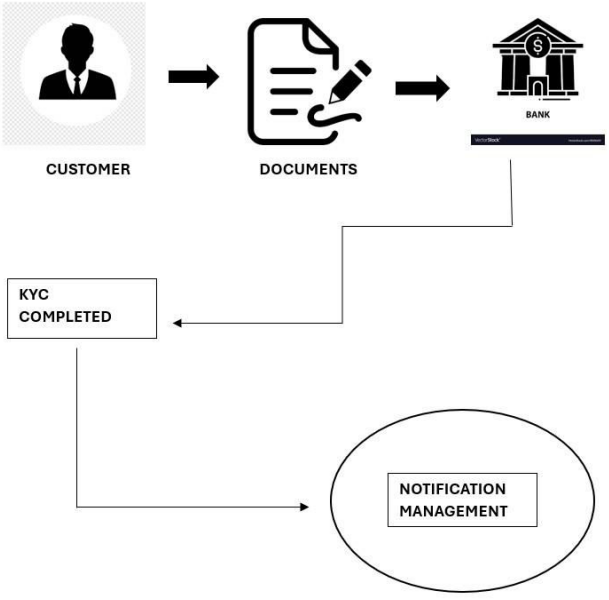
We are trying to create a blockchain-based KYC verification system that will create a block for each bank. After creating a block per bank, the client needs to enter the KYC data and it creates an account on the blockchain through the client account and stores it on the blockchain network. Then, when you ask your bank to open an account, the data is stored on the blockchain. Highlights stored on highly decentralized blockchains are often changed or modified solely by the client, which can be done with the client's permission first. When a read request is invoked on a customer profile, only the requested bank or administrator will read the customer's KYC document. When a request is submitted to the client profile, the client can choose to accept or deny it. If the client agrees to the read request, the blockchain can provide a complete read to the bank or administrator. To verify that the customer's KYC documents issued by the

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303173|

government are valid. This client data stored on the blockchain is primarily for security reasons. Ganache is used to doing this business. A terminal window is opened on your system and the Smart Remix contract is running. It also uses the crypto wallet Metamask to create transactions in a highly secure way. The first step is to open a terminal and line up ganache-cli in the command line. Then change to the default directory in another terminal. After running the init.js command node, run the init.js file. The address of the assembled smart contract is generated in seconds as a 20-byte address. Open a text editor and navigate to the rootjscontractdetails.js file. Then, whenever you launch a text editor and enter the 20-byte address representing the address of the contract instance specified in the contract variable, visit ContractDetail.js. Here we want to edit the default string, which is the address of the contract instance provided by the contract variable. Set the addresses of 20 computer memory blocks after exhausting the previous 20. This program is currently available. Make sure your ganache works. An Ethereum network for locals. The system has two portals: Banking/Admin and Users. The most functional aspect of the bank/manager is that initially the bank/manager must register via a block with the bank/manager's name, password and registration number. Small text is left on the ganache. You will need to copy and paste this signature. When productive registration occurs, log in with the name of the bank or administrator and confirm it with your signature. 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 change your KYC. Click the "Add KYC" tab, enter "Non-Public Data" type and click the "Submit" button for bank/administrator declaration. When this notification appears with your current bank or manager account type, click the OK button. If the user profile is successfully created, a similar tab will appear and click the OK button. After uploading the documents an email is sent to the user. Then click the “Read KYC” tab. It will ask for your username. After entering the username, an "Access Denied" message is displayed and the user is asked for permission. After completing this procedure, users can use some basic functions. Users must log in to the Customer Portal using their customer username and password. When a productive registration occurs, the user logs into the newly created account and continues as needed. Once the action is entered, a page appears where the user reads the fine print on the KYC Details tab and the bank or administrator prompts the user on the Requests tab. Users decide whether to allow or deny access to user data. Because the user has given permission, the bank or administrator can access the fine print if the user chooses to allow it. There is a notification system to know the status of the KYC details of the client. After the successful verification of the documents an email is sent to the client’s mailing address.



V. METHODOLOGY

MODULE 1 : USER REGISTRATION

This module is responsible for registering new users on the platform. It collects basic user information such as name , address, contact information.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303173|

MODULE 2 : DOCUMENT VERIFICATION

This module is used to verify the authenticity of the user's identity documents. The module can use different technologies such as OCR (Optical Character Recognition) and facial recognition to match the user's information with the data on the identity documents.

MODULE 3 : BLOCKCHAIN

This module is responsible for storing the user's data in a secure and immutable way on the blockchain network.

MODULE 4 : KYC VERIFICATION

This module is responsible for verifying the user's identity based on the data collected by the User Registration and Document Verification modules.

MODULE 5 : ADMIN DASHBOARD

This module is used by the platform's admin to manage user accounts and to monitor the KYC verification process.

MODULE 6 : NOTIFICATION

This module is responsible for sending notifications to the user about their KYC verification status.

VI. IMPLEMENTATION

Smart Contract Development (Solidity):

Develop an Ethereum smart contract using Solidity that defines the KYC process.The smart contract should include functions for users to submit their KYC details, for bank admins to verify KYC, and for generating verification certificates.

IPFS Integration:

Integrate IPFS (InterPlanetary File System) with your application to store KYC documents securely off-chain.Use IPFS to store verification certificates generated by the smart contract.

Backend Development (Flask):

Create a Flask application to serve as the backend for your KYC verification system. Implement endpoints/routes for user registration, KYC submission, admin verification, certificate generation, etc.

Frontend Development (HTML/CSS/JS):

Develop a user-friendly frontend using HTML, CSS, and JavaScript to interact with the Flask backend and Ethereum smart contract.Create UI components for user registration, KYC submission, admin verification, and viewing certificates.

User Registration and KYC Submission:

1. Users register on the platform by providing necessary details (name, email, etc.).
2. Users submit their KYC documents (ID proof, address proof, etc.) through the frontend interface.
3. KYC documents are securely uploaded to IPFS, and their IPFS hash is stored on-chain in the Ethereum smart contract along with user details.

Admin Verification:

1. Bank admins log in to the platform using their credentials.
2. Admins access a dashboard where they can view pending KYC requests.
3. Admins review the KYC documents submitted by users and either approve or reject them.
4. Upon approval, the admin updates the status in the smart contract, indicating successful verification.

Verification Certificate Generation:

1. Once a user's KYC is verified by the admin, the smart contract triggers the generation of a verification certificate.
2. The certificate is created using relevant details from the smart contract (user's name, KYC details, verification status, etc..
3. The certificate is stored on IPFS, and its IPFS hash is recorded on-chain in the smart contract.

User Interface:

1. Users can log in to their accounts to check the status of their KYC verification.
2. Upon successful verification, users can download their verification certificates from IPFS using the provided IPFS hash.

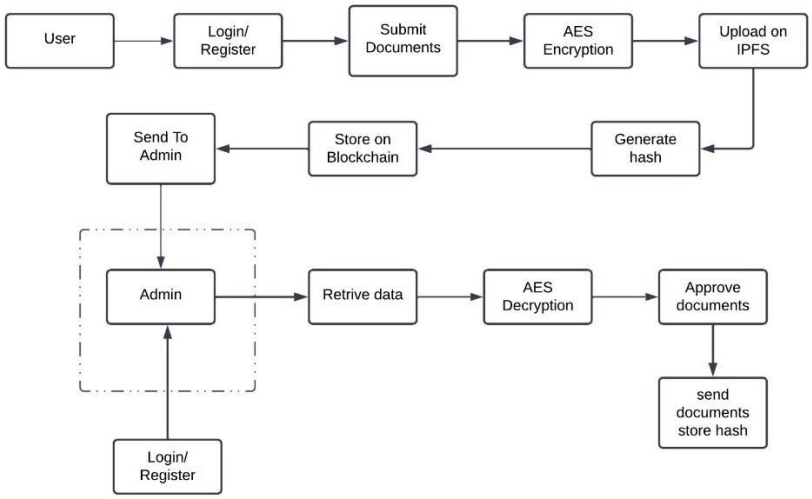
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303173|

3. The frontend should provide a seamless and intuitive experience for users, admins, and banks to interact with the KYC system.

Block Diagram :



VII. RESULT ANALYSIS

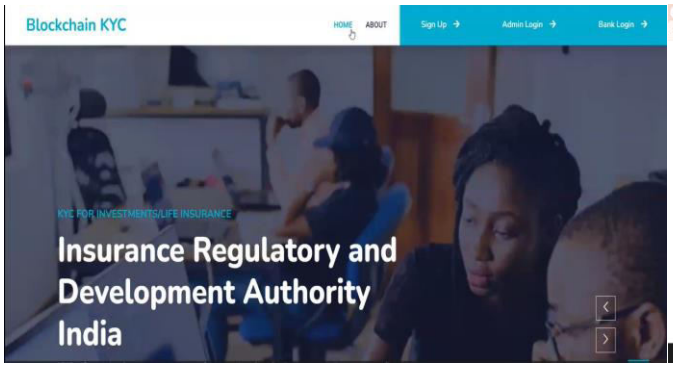


Fig 1 : Home page

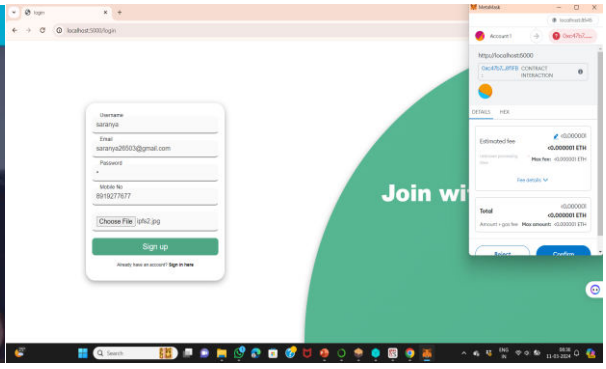


Fig 2 : Signup

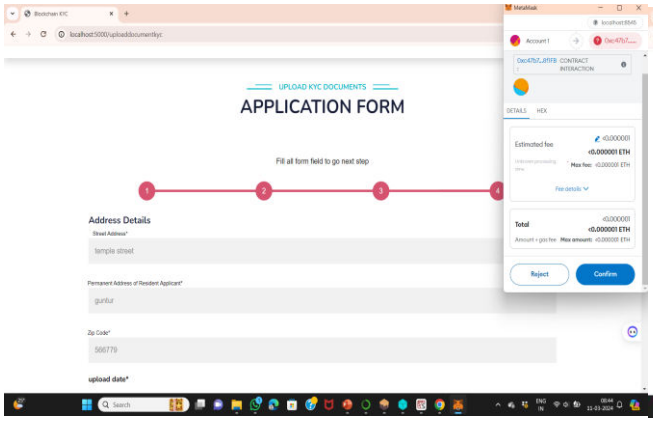


Fig 3 : Registration form for KYC process

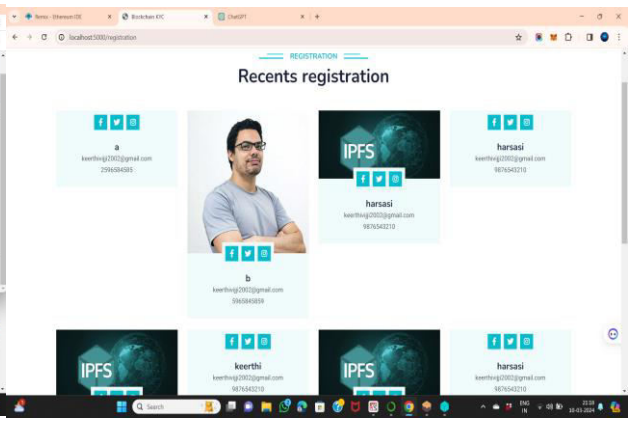


Fig 4 : Register Users Details

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303173|

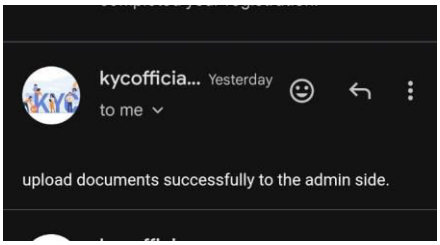


Fig 5 : Uploaded Documents mail

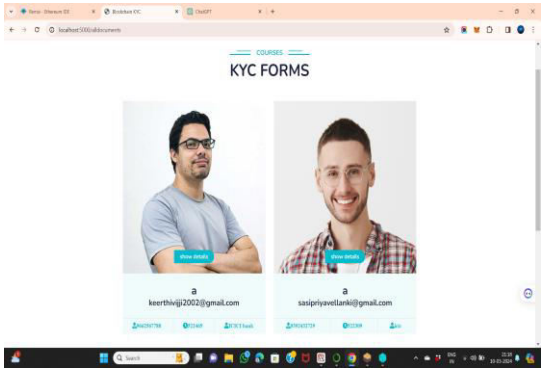


Fig 6 : KYC Form of User Details

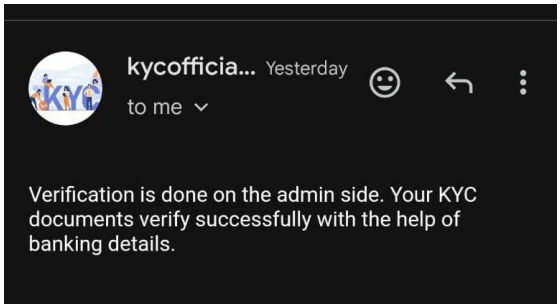


Fig 7 : Verification Acknowledgement

Fig 8 : KYC Completion Certificate

VIII. CONCLUSION

This project looks at the challenges that the customer has to face in the traditional KYC system and attempt to overcome its made KYC performs various operations regulator fi and customer verify the customer by any means organizations using blockchain and other technologies.

The project utilizes blockchain technology to securely store and manage KYC data, ensuring that it remains tamper-proof and accessible only to authorized parties. By creating a separate block for each bank, the system enables decentralized verification while maintaining data integrity.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303173|

Our proposed approach performs KYC verification the process easier data is more secure and tamper-resistant by maintaining a single secure database via blockchain which will also get rid of redundant KYC checks performed financial institutions it even saves time even us away with third party interference because the user is given ownership over data.

REFERENCES

[1] https://www.researchgate.net/publication/350093013_KYC_Optimization_using_Blockchain_Smart_Contract_Technology
[2] https://www.academia.edu/39393562/Blockchain_as_the_Newest_Regtech_Application_the_Opportunity_to_Reduce_the_Burden_of_KYC_for_Financial_Institutions
[3] https://www.ijstr.org/final-print/jan2020/A-Blockchain-Based-Approach-For-An-Efficient-Secure-Kyc-Process-With-Data-Sovereignty.pdf
[4] https://www.researchgate.net/publication/328211101_Optimized_and_Dynamic_KYC_System_Based_on_Blockchain_Techn
[5] Vimalkumar Pachaiyappan and R. Kasturi. 2018. Block Chain Technology (DLT Technique) for KYC in FinTech Domain: A Survey. International Journal of Pure and Applied Mathematics Volume 119 No. 102108,259-265.https://acadpubl.eu/jsi/2018-119-10/articles/10c/36.pdf
[6] Sreelakshmi V G, Meera P M, Senna Mariya Pius, Mathews Jose, Swapna B Sasi "KYC using Blockchain" International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 4 Issue 4, June 2020 e-ISSN: 2456 – 6470.
[7] 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.
[8] Alex Biryukov, Dmitry Khovratovich, Sergei Tikhomirov, "Privacy preserving KYC on Ethereum ", 2018, W. Prinz & P. Hoschka (Eds.), Proceedings of the 1st ERCIM Blockchain Workshop 2018, (ISSN 2510- 2591), DOI: 10.18420/blockchain2018 09.
[9] José Parra-Moyano, Tryggvi Thoroddsen, Omri Ross "Optimized and Dynamic KYC System Based on Blockchain Technology", January 2019, International Journal of Blockchains and Cryptocurrencies, DOI: 10.1504/IJBC.2019.10021398.
[10] Vikrant Kulkarni, Awadhesh Pratap SINGH "Sustainable KYC through Blockchain Technology in Global Banks", July 2019, Annals of Dunarea de Jos University of Galati Fascicle I Economics and Applied Informatics, DOI: 10.35219/eai1584040929.
[11] Prof A. L. Maind, Pallavi Vijay Gedam, Snehal Kashinath Chavan, Chitrali Dnyaneshwar Shinde, "KYC USING BLOCKCHAIN " 2018,International Journal or Research in Engineering Application & Management (IJREAM), ISSN : 2454-9150 .
[12] Norvill R, Steichen M, Shbair WM, State R (2019) Blockchain for the Simplification and Automation of KYC Result Sharing. *In*: *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, pp 9–10
[13] SHARMA R Why a New "Know Your Customer" Project Is Crucial to Blockchain. https://www.investopedia.com/news/why-new-know-your-customer-project-crucial-blockchain/. Accessed 5 Dec 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details