The KYC Verification System Using Blockchain

G.BharathKumar Reddy
School of computer science engineering with blockchain technology
Sathyabama institute of science and technology
Chennai,Tamil Nadu-600119
bharathkumar96780@gmail.co m

J.Rupesh Kumar
School of computer science engineering with blockchain technology
Sathyabama institute of science and technology
Chennai,Tamil Nadu-600119
jrupeshkumar122003@gmail.co m

Dr.Geethanjali D
Assistant Professor
School of computer science engineering
Sathyabama institute of science and technology
Chennai, Tamil Nadu-600119
drgeethanjali81@gmail.com

N Umasankari,
Assistant Professor,
Department of Computer Science and Engineering,
Sathyabama Institute of Science and Technology,
Chennai, TamilNadu-600119
san_june18@yahoo.com

***Abstract-** Know your client or essentially KYC is the prepare of approving and confirming the personality of its clients and analyzing potential dangers of illicit eagerly for the commerce relationship. A few issues with the existing manual KYC prepare are that it is less secure, time devouring and expensive. With the appearance of Blockchain innovation, its properties such as unchanging nature, security, decentralization make them a great arrangement to such issues. Whereas commercial arrangements like "kyc-chain.com", "KYC.legal" right to empower blockchain-based KYC confirmation, it gives a strategy for archives to be approved by a trusted member in the arrange. In this work, Ethereum based Optimized KYC Blockchain framework utilizing symmetric AES encryption based compression instrument is proposed. This framework guarantees straightforwardness by conveyed record, secured by cryptography, productive by compression calculation and in general optimized by blockchain highlights.*

***Watchwords:** Blockchain, Ethereum, KYC, Compression, Encryption, DLT*

INTRODUCTION

Know your customer, alternatively known as know your client or simply KYC is the process in a business validating the identity of its users and measuring potential risks of illegal intentions for the business relationship as defined José Perra et al. The existing systems of data storage such as cloud storage, Direct Attached Storage (DAS) in Big data and Object Storage became more vulnerable to attacks from various malicious threats which includes privilege abuse attack, SQL injection attack, Storage media exposure attack, Targeting unpatched database vulnerability attack from all over the world. The Binance KYC data leak on 2008 costs 10000 user's data where KYC user information are stored in cloud result in storage media exposure attack. Information about customers such as Aadhar card details which contains highly sensitive data like biometric details are susceptible to attacks. One such example is Indian Bank recently faced attack on KYC worth 100 Crores on its business as stated Sujan Hajra in a blog about Indian Bank

The proposed systems require a trustworthy and extremely secure technology to protect such data. A few problems with the existing manual KYC process are that it is time consuming, redundant, costly, less secure for example in banking system if a customer holds multiple accounts which created at different time interval, the KYC process update is difficult in handling with existing manual entry process. Blockchain ledger is distributed and shared. When there is a official to operate an account. Therefore, there is a need for system information, safety, efficiency gains, cost advantages, enhanced customer experience, and increased transparency throughout the process of onboarding a customer. Blockchain technology, with its properties such as immutability, security, decentralization makes them a good solution to such problems. Blockchain is an emerging technology in cyber-security network. The distributed ledger can store transactions among participant efficiently and in a verifiable and permanent way. The most important nature of Blockchain is that it is extremely difficult to alter Change in the existing account then customer they can make update in KYC and get approval from a bank the logged data contained in a blockchain. This is ensured by having some sort of consensus within the decentralized blockchain system. It makes blockchain an efficient secure technology. One other reason why blockchain is intriguing to businesses is that this technology is completely open source. The aim of this proposed system is to effectively build an optimized KYC Blockchain system for managing KYC details of the customers. The system can be deployed in various organizations which require KYC verification of the customers. The result is analyzed with respect to the storage size in Blockchain and storage in the server, original data is compared with compressed data in percentage and it is shown that 20% reduction in size has been achieved. Next, data retrieval time is compared with respect to number of records retrieved from the ledger. In addition to this throughput and response time is also analyzed stakeholders. In sectors such as finance, healthcare, and supply chain management, where data sharing between multiple parties is common, blockchain's transparency and security can build confidence in the integrity of shared data. Partners and customers can be assured that their information is protected against unauthorized access and 10 tampering, which strengthens collaborative relationships and enhances overall data governance. The ability to provide transparent and tamper- proof records of data interactions builds trust and facilitates more secure and reliable data exchanges.In conclusion, blockchain hashing algorithms present a robust and innovative approach to data leakage prevention. By ensuring data integrity, enhancing security through decentralization, providing transparency and auditability.

Blockchain is playing a vital role in the field of cyber security applications. Distributed Ledger Technology (DLT) is one of the main parts of blockchain concept. DLT makes decentralized system in which replicas of data is available with multiple nodes connected within a network. These copies of data are always synchronized and are shared between the nodes. Any kind of data stored within blockchain is made available to everyone and will definitely be tamper proof. The consent of all the nodes in the DLT network is required before any data added within the blockchain. The nodes in the blockchain network must follow a 'consensus mechanism' which can be customized according to the application and Smart contract is the main application of blockchain technology. The significant idea in smart contract is that the terms of agreement between the nodes can be stored as contract inside the blockchain in the form of programs instead of data. This contract is made to execute automatically without the contribution of a third party. It could be able to mitigate several security threats. For example, the 51% Rule in blockchain to encounter security attack. Ethereum blockchain became the most standard blockchain platform as it is used for smart contract applications and Internet of Things (IoT). Ethereum makes smart contracts to be written in 'Solidity' which is an object oriented programming language developed only for writing smart contracts.

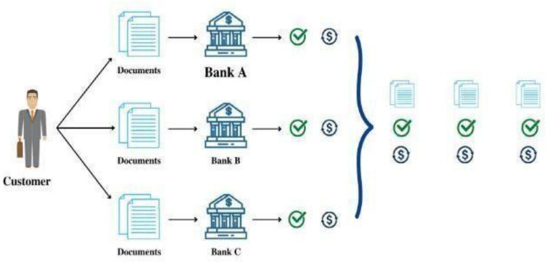


Fig No:-1 Traditional Kyc

There are malwares in circulation that can scan our KYC server for private key files of KYC users, so the challenge lies to protect the private key of the participants. Intruder may plant malicious code in the KYC server which gives the real time access to edit KYC data. Cyber attacks might change KYC file attributes, move files to a specified network by connecting network, executing KYC server commands to filter the contents of files or even delete the all KYC information. The following factors can be adopted to protect the KYC data. They are encryption, PIN, Location and Time factors which add more difficult for intrusion.

II. RELATED WORKS

Alex Biryukov et al. (2022).,[1],This research paper investigates privacy-preserving KYC solutions on the Ethereum blockchain. It employs advanced cryptographic techniques to ensure user data confidentiality while maintaining compliance with regulatory standards. The study highlights the potential of blockchain technology to create secure, transparent, and efficient identity verification systems, reducing reliance on centralized authorities and minimizing the risk of data breaches.Bharti Pralhad Rankhambe & Dr. Harmeet Kaur Khanuja (2021).,[2],The paper focuses on optimizing the KYC process in the banking sector using blockchain technology. It addresses the inefficiencies and redundancies in traditional KYC systems by proposing a decentralized approach. The study emphasizes blockchain's ability to streamline customer verification, enhance data sharing among institutions, and reduce operational costs, ultimately improving the overall efficiency of the banking sector. Hussain & Zeeshan-ul-hassan (2022).,[3], This research introduces a decentralized KYC system leveraging blockchain technology. The proposed system eliminates intermediaries, thereby reducing the risk of fraud and enhancing data security. The study highlights the benefits of blockchain in creating a transparent and trustworthy customer verification process, which can be adopted across various industries to improve identity management. Manoj Kumar & Nikhil Yadav (2020).,[4] The authors present a blockchain-based approach for an efficient and secure KYC process, emphasizing data sovereignty. The study addresses challenges such as data duplication and unauthorized access, proposing a robust solution that ensures data integrity and security. The paper highlights the potential of blockchain to revolutionize identity management by providing a decentralized and immutable ledger for customer data. Nikita Singhal et al. (2022).,[5], This research explores the integration of blockchain and IPFS for smart KYC systems. The proposed solution enables decentralized storage and secure data sharing, enhancing scalability and efficiency in handling customer data. The study highlights the benefits of combining blockchain's immutability with IPFS's distributed storage capabilities to create a robust and scalable KYC system. Steichen et al. (2018).,[6] The paper proposes a blockchain-based access control mechanism for IPFS, ensuring secure and decentralized data storage. The study emphasizes the integration of blockchain with distributed file systems to enhance data security and accessibility. The proposed solution addresses the challenges of data privacy and access control in decentralized storage systems, providing a secure framework for managing sensitive information. Sreelakshmi et al. (2022).,[7] This study investigates the implementation of KYC processes using blockchain technology. It focuses on the transparency and immutability provided by blockchain, which can significantly reduce verification time and costs. The paper highlights the potential of blockchain to create a more efficient and secure KYC system, benefiting various industries that require robust identity verification processes. S.NV (2022).,[8] The research discusses the use of blockchain for KYC verification, emphasizing its role in reducing fraud and improving data integrity. The proposed decentralized approach ensures secure identity management by leveraging blockchain's inherent properties of transparency and immutability. The study highlights the potential of blockchain to transform traditional KYC processes into more efficient and secure systems. Reddy et al. (2020).,[9],This work explores the application of blockchain technology in KYC processes, focusing on transparency and efficiency. The study highlights blockchain's potential to streamline customer verification and reduce operational costs. The proposed solution addresses the challenges of traditional KYC systems, offering a more secure and efficient approach to identity management. Wenger (2014).,[11] The article provides an in-depth analysis of blockchain's foundational innovation, particularly in the context of Bitcoin. It explores the potential of blockchain technology beyond cryptocurrencies, emphasizing its role in enabling decentralized systems. The study offers valuable insights into the transformative impact of blockchain on various industries, highlighting its potential to revolutionize traditional processes. Yadav & Chandak (2019).,[12], The authors propose transforming the KYC process using blockchain technology, focusing on data security and efficiency. The study highlights blockchain's ability to reduce redundancy and improve trust in verification processes. The proposed solution addresses the limitations of traditional KYC systems, offering a more secure and efficient approach to identity management. Zheng et al. (2023).,[13] This research introduces an innovative IPFS-based storage model for blockchain, enhancing data storage efficiency and security. The study emphasizes the integration of decentralized storage solutions with blockchain technology to address the challenges of data privacy and accessibility. The proposed model provides a secure and scalable framework for managing data in decentralized systems. solution.

III. OPTIMIZED KYC BLOCKCHAIN SYSTEM

The architecture of the proposed Optimized KYC Blockchain system. In the proposed solution, every single KYC Block information has been compressed and This monitoring function checks for anomalies in data access patterns and detects any attempts to breach security. If unauthorized access is detected, the system promptly raises an alarm, signaling a potential security breach and enabling rapid response actions. If no unauthorized access is detected, the system simply continues monitoring without triggering any alerts. This continuous monitoring process ensures that the data remains secure over time, with any access attempt recorded on the blockchain for auditability. By recording hash values and timestamps in a blockchain database, the system maintains an unalterable history of data access events, providing a robust, tamper-proof method for data integrity verification. Thus, the combination of hashing and blockchain technology in this workflow ensures that sensitive data is protected, any unauthorized access attempts are promptly deteled of all

transactions is maintained for transparency and audit purposes.

A peer-to-peer network consisting of numerous participants replicates all data, while specific nodes conduct a linked key agreement to validate state transactions and synchronize copies. These elements are essential components of Distributed Ledger Technology (DLT). Distributed ledgers are designed to withstand crashes and prevent malicious actions from a small number of nodes, providing a highly accessible and decentralized digital framework. However, DLT does face challenges related to scalability and privacy. Blockchains, which are a type of DLT, are among the most widely used. The key characteristic of a blockchain is that transactions are grouped into blocks, with each block containing the hash value of the previous one. This structure forms a chain aimed at establishing a tamper-proof record. Given the Fig No-2 is the Architecture can explanation of Proposed System

SYSTEM ARCHITECTURE

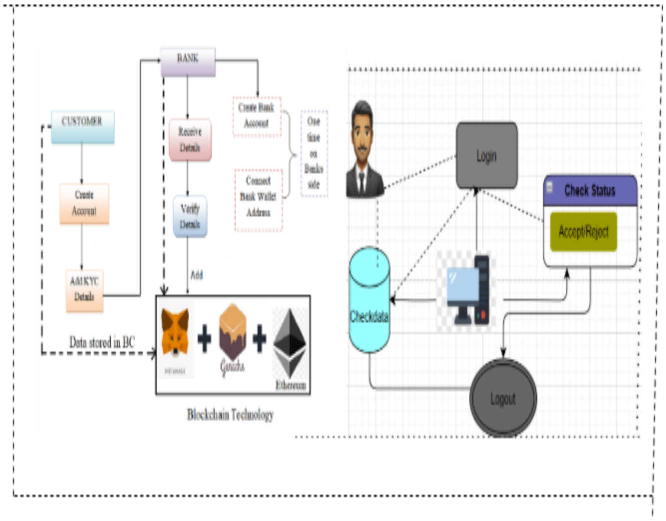


Fig No-2 System Architecture

Additionally, this workflow provides enhanced security due to blockchain’s decentralized nature, where each transaction is verified by a network of nodes, reducing the risk of single points of failure or manipulation. By storing data hashes rather than the actual data on the blockchain, the system ensures data privacy while still benefiting from blockchain's immutability and transparency. In case of any changes or tampering attempts, the altered hash will immediately reveal discrepancies, flagging any integrity issues. This system is especially useful in sectors that require strict data security, like finance, healthcare, or government, as it ensures real-time detection of unauthorized access and maintains a secure audit trail, promoting trustworthiness and regulatory compliance.

IV. IMPLEMENTATION

The proposed system is implemented and tested using the Geth, Gaanche-cli, solidity compile, Node JS softwares and Web3js, Geth is the Go language (golang) implementation of Ethereum blockchain.

Geth: Geth is the Go implementation of Ethereum, enabling node operation, mining, and smart contract deployment. It supports Ethereum's decentralized ecosystem and blockchain interactions.

Ganache-cli: Ganache-cli is a command-line tool for Ethereum development, allowing local blockchain simulation. It aids in testing smart contracts and dApps efficiently.

Solidity Compiler: The Solidity compiler converts Solidity code into Ethereum Virtual Machine (EVM) bytecode. It's essential for deploying smart contracts on the Ethereum blockchain.

Node.js: Node.js is a JavaScript runtime for building scalable server-side applications. It's used in Ethereum for backend development, APIs, and interacting with blockchain networks.

Web3.js: Web3.js is a JavaScript library for interacting with Ethereum nodes. It enables dApp development, smart contract interaction, and blockchain data retrieval via WebSocket.

Fig No-3 Home Page

The current KYC process is cumbersome, heavily dependent on manual documentation, and lacks a comprehensive monitoring system, which can lead to potential fraudulent activities. Banks must verify customer identities to combat illegal actions. While this process is essential, it faces significant challenges related to privacy, security, and efficiency.

Some researchers have proposed a KYC blockchain system that utilizes the IPFS protocol for peer-to-peer file sharing and Gpg4win for encryption. Verified customer documents are encrypted and uploaded to the IPFS network, allowing for document retrieval through hash keys. This method reduces the need for repetitive verification when opening accounts at different banks and addresses scalability concerns.

Centralized and Decentralized Blockchain Solutions Another study introduced a DLT-based KYC architecture designed to share processing costs among institutions. Feedback from banking executives emphasized the need for interbank collaboration and a gradual rollout in smaller countries. The initiative aimed to lower verification costs and enhance user experience, with a focus on proportionality and privacy. However, it did not tackle the issue of block data expansion over time.

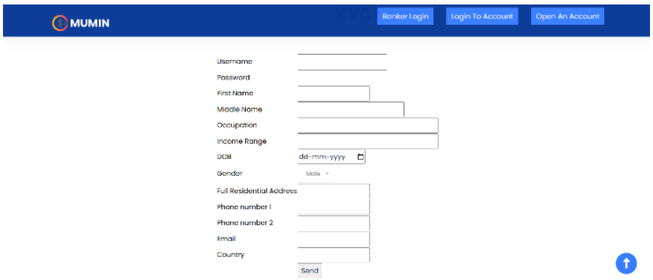
Regulatory Technology (Regtech) Researchers have recommended the integration of Regtech in banking to ease KYC challenges. Unlike Fintechs, Regtechs offer solutions specifically for financial institutions, including tax reporting based on clients' financial residency. While the concept is promising, the study fell short in detailing blockchain implementation and the associated costs.

create a virtual blockchain running in the current node (local). Along with this, the auto generated Ethereum accounts are used to simulate and test the working of Ethereum applications. Solidity Compiler was used to compile the smart contract written in solidity. Node JS was used to write serverside scripting for compression and interaction with the Ethereum blockchain. The following lists of Libraries are used in the implementation. Web3js was used for communicating with the Ethereum blockchain hosted locally in the computer. Crypto was used for implementing encryption and decryption of KYC data before feeding the data into the blockchain and while retrieving the data respectively. KYC data before encrypting the KYC data and after decrypting the data from KYC system respectively. Node mailer was used for sharing the generated secret key to the customer through email in the form of QR Code. QR Code Scanner This library/API was used to generate QR Codes corresponding to the secret key and for scanning the QR through the computer's camera. Ethereum wallet has been created for all the transaction, KYC data compression in the smart contract. The wallet is essential for validation because the Ether is used as a stake in the wallet to add the block in the blockchain.

USER PHASE

A. Open An Account

This module simplifies registration and account creation for new users or entities by gathering essential personal or entity-related details. Information collected during this process is securely stored on the Ethereum blockchain, ensuring its immutability and minimizing the likelihood of data tampering or unauthorized alterations. Utilizing the Ethereum blockchain enhances security measures, providing users with confidence in the integrity and permanence of their account information.

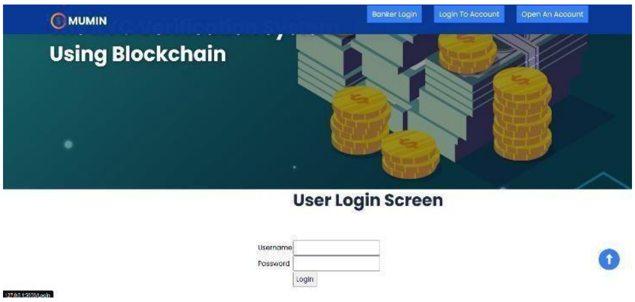


Username
Password
First Name
Middle Name
Occupation
Income Range
DOB dd-mm-yyyy
Gender Male
Full Residential Address
Phone number 1
Phone number 2
Email
Country

Fig No-4 Open Account

B. Login to Account

This module empowers registered users to securely access their accounts within the system. Users authenticate themselves using credentials managed by the blockchain, ensuring robust authentication and access control measures. Following successful authentication, users are granted access to various functionalities such as depositing funds, initiating transactions, or checking account balances.



User Login Screen

Fig No-5
Admin

C. Deposit Amount

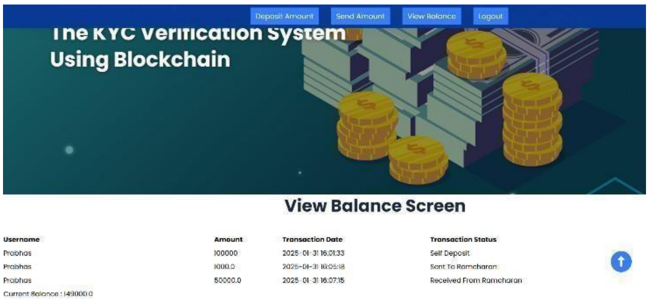
Users can securely add funds to their accounts through this feature, with blockchain technology managing the transactions to ensure accuracy and security.

D. Send Amount

Users can securely initiate transactions or transfers, transferring funds to other accounts or entities within the system through this feature.

E. View Balance

Users can conveniently check their account balances, facilitated by the blockchain, which guarantees the integrity of the information displayed. Accurate and up-to-date balances are provided, enhancing user trust and confidence in the system.



View Balance Screen

Username	Amount	Transaction Date	Transaction Status
Prabhas	100000	2025-01-31 16:01:33	Self Deposit
Prabhas	1000.0	2025-01-31 16:05:18	Sent To Ramcharan
Prabhas	50000.0	2025-01-31 16:07:15	Received From Ramcharan

Current Balance : 149000.0

Fig No-6
View Balance

BANK PHASE

F. Banker Login

This module offers a secure gateway for authorized bank personnel or administrators to enter the system. Bankers utilize their individual credentials to log in, granting them access to designated functionalities like user verification and transaction monitoring. The Ethereum blockchain safeguards the login procedure, guaranteeing that solely authorized personnel can access sensitive information and system management tools. This reinforces security measures, ensuring that confidential data remains protected within the system.In Fig No:-6 the banker can the login into admin portol for Checkstatus in G.

G.Check User Status

Authorized personnel, including bankers or compliance officers, utilize this feature to monitor user account statuses and verification processes. By querying the system, they can ascertain whether users have completed required Know Your Customer (KYC) procedures or if verifications are pending. The Ethereum blockchain securely records and stores user status updates, ensuring transparency and providing an auditable trail of verification progress. This enhances accountability and facilitates efficient management of user accounts within the system.

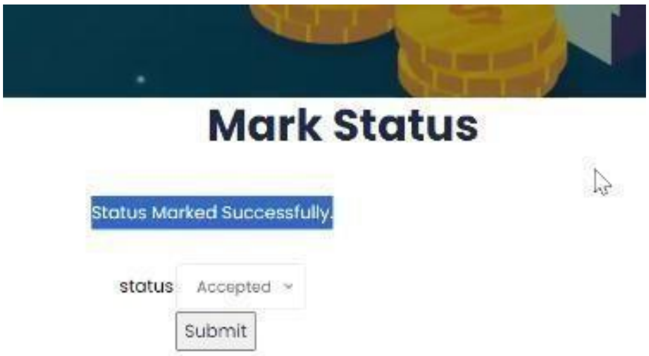
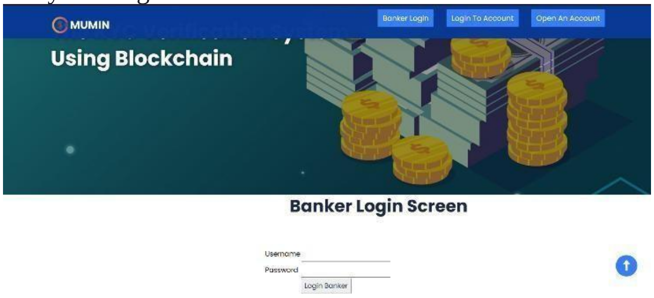


Fig No-8 Status Account

V. CONCLUSIONS AND FUTURE WORK

The proposed solution addresses the problem of redundant registration in the KYC process encountered in the existing situation. Additionally, encryption using AES algorithm is implemented and random key generation for providing the customer an access control of his/her KYC data and maintain their secrecy. The proposed system can reduce storage requirements approximately by about 20%. In future versions of this system, individual fields can be given separate access keys to provide better control over the private data of users. Extensive study of all encryption techniques and compression techniques can be done to analyze and get a more efficient solution in the realworld



Banker Login Screen

Fig No-7 Banker Login

decentralized environment manages and secure their data, both now and in the face of future threats, thereby maintaining the confidentiality and integrity of their critical data assets. Overall, the project underscores the benefits of blockchain technology in streamlining KYC procedures, reducing operational costs, and enhancing security within the financial sector. It emphasizes the potential for blockchain to revolutionize KYC practices, benefiting both institutions and customers with improved security, efficiency, and trust in identity verification processes.

REFERENCES

[1] Alex Biryukov, Dmitry Khovratovich, Sergei Tikhomi rov Privacy-preserving KYC on Ethereum Proceedings of the 1st ERCIM Blockchain Workshop Reports of the European Society for Socially Embedded Technologies (2022)

[2] Bharti Pralhad Rankhambe and Dr. Harmeet Kaur Khanuja,"Optimization of the KYC Process in the Banking Sector using Blockchain Technology",International Journal of Current Engineering and Technology, Special Issue-8 (Feb 2021) [3]Hussain,S.A., U. Zeeshan-ul-hassan.,"Blockchain- based DecentralizedKYC (Know-Your-Customer)", International Conference on Systems and Networks Communications, 2019.

[4] Manoj Kumar and Nikhil Yadav, "A Blockchain Based Approach For An Efficient Secure KYC Process With Data Sovereignty," International Journal for Research in Applied Science and Engineering Technology 9, no. 1 (2020): 3403-3407.

[5] Nikita Singhal, Mohit Kumar Sharma, Sandeep Singh Samant, Prajwal Goswami and Y.Abhilash Reddy, "Smart KYC Using Blockchain and IPFS", Springer Nature Singapore Pte Ltd. 2022

[6] Steichen, M., B. Fiz, R. Norvill, W. Shbair, and R. State,"Blockchain Based, Decentralized Access Control for IPFS", 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),July2018,Published, doi: 10.1109/cybermatics 2018.2018.00253.

[7] Sreelakshmi, V. G., Meera, P. M., Senna, M. P., Mathews, J., Swapna, B. S., "KYC using Blockchain", International Journal of Trend in Scientific Research and Development
(IJTSRD), vol. 4, no. 4, pp. 1600-1603, 2022.

[8]S.NV,"KYC Verification Using Blockchain", International Journal for Research in Applied Science and Engineering Technology, vol. 10, no. 7, pp. 861–
amples and case studies.
865, Jul.
2022, doi: 10.22214/ijraset.2022.45156

[9] Reddy, E. S. V., N. Suhag, and M. S., "Know Your Customer (KYC) Process through Blockchain." International Research Journal of Engi neering and Technology (IRJET) 7, no. 6 (2020): 2336-2339.

[10] Wenger, A. 2014, "Bitcoin: Clarifying the Foundational Innovation of the Blockchain." Continuations
[Online].
https://continuations.com/post/105272022635/bitcoin-clarifying the foundational-innovation-ofNakamoto Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System." October 2008

[11] Yadav, P., and R. Chandak, "Transforming the Know Your Customer (KYC) Process using Blockchain." 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), December 2019, doi: 10.1109/icac347590.2019.9036811.

[12] Zheng, Q., Li, Y., Chen, P., and Dong, X. "An Innovative IPFS-Based Storage Model for Blockchain", 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), December 2018, Published, doi: 10.1109/wi.2018.000-8.

[13] Consensys(2020).*Introduction to Smart Contracts and Solidity.*A practical guide to writing smart contracts in Solidity, with examples of how blockchain can be used for identity verification and KYC.

[14]HyperledgerFoundation(2021).*HyperledgerFabric: A Blockchain Platform for the Enterprise.*This resource explores Hyperledger Fabric, a blockchain framework that can be used for building KYC and identity management systems.

[15]IBMBlockchain(2020).*Blockchain for Identity Management:Comprehensive.*This guide discusses how blockchain can be used for identity management, including KYC, with practical ex