# AUTHENTICITY OF CREDENTIALS USING BLOCKCHAIN

**Sakshi M[1], Manashri M[2], Tithi N[3], Ayesha P[4], Sayali Karmode[5]**

[1,2,3,4]Student, Department of Information Technology MGM's College of Engineering and Technology Kamothe, Navi Mumbai, India

[5]Assistant Professor, Department of Information Technology MGM's College of Engineering and Technology Kamothe, Navi Mumbai, India

## ABSTRACT

As experts and scientists have already taught us, data on the internet is not secure, and anyone with strong hacking abilities can quickly access your system. Nevertheless, this is no longer the case because of the recently developed blockchain technology, which has made it feasible to protect and maintain the privacy of our data. Blockchain technology will be used in the near future by a large number of companies and organizations to protect private data and conduct financial transactions. In this work, we suggest a blockchain system that financial institutions can use for KYC document verification. Additionally, this paper will clarify some of the key elements of blockchain use.

**Keywords-** Blockchain, Smart Contracts, Transparency, KYC process, Digital Identity, Ethereum, Metamask, Know your customer**.**

## 1. INTRODUCTION

**1.1** Since its creation in 2008, the Blockchain system has experienced strong growth due to the emergence of cryptocurrency exchanges and data sharing.

A blockchain, to put it simply, is a system that aids in the recording and security of information. Blockchain technology has been used to safeguard data such that it is difficult for hackers or other unauthorized parties to alter the system. For the time being, blockchain-based transactions are the safest. It is ideal for the financial industry due to its features including consensus, improved security, and immutability. The standard KYC verification procedure for any bank is, as we all know, exhausting for both sides.

Therefore, it would be a huge accomplishment if we could use blockchain technology to instantly validate important papers. Therefore, the ideal approach to maintain the system's adaptability and integrity is to use blockchain technology for both the verification and storage of the KYC papers. Given its wide range of applications across other industries, blockchain technology has the potential to significantly alter the financial sector.

In today's computerized age, Know Your Client (KYC) confirmation stands as a significant handle for businesses around the world, guaranteeing compliance with administrative measures whereas relieving dangers related with extortion and character burglary. Conventional KYC strategies, in any case, are regularly tormented with wasteful aspects, driving to long preparing times, expanded costs, and vulnerabilities to information breaches. Enter blockchain innovation, a troublesome drive balanced to revolutionize KYC confirmation, advertising improved security, straightforwardness, and efficiency.At the bleeding edge of this change is the integration of blockchain with Metamask Ethereum, a broadly received cryptocurrency wallet and door to decentralized applications (dApps).

Leveraging the permanent nature of blockchain and the user-friendly interface of Metamask, businesses can streamline their KYC forms whereas giving clients with more noteworthy control over their individual data.With blockchain, KYC information is safely put away in a decentralized record, disposing of the require for middle people and decreasing the chance of unauthorized get to or altering. Each KYC passage is cryptographically hashed and timestamped, guaranteeing its astuteness and realness.

Besides, the dispersed nature of blockchain guarantees repetition and strength against framework disappointments or assaults, upgrading the in general unwavering quality of KYC verification.Metamask Ethereum serves as the bridge between clients and blockchain-powered KYC arrangements, advertising a consistent and natural involvement. Through Metamask's browser expansion or versatile app, clients can safely connected with KYC dApps, giving consent to get to their KYC information as required.

The integration of Metamask Ethereum too encourages moment confirmation forms, dispensing with the require for manual report entries and decreasing hold up times for users.Furthermore, the decentralized nature of Metamask Ethereum guarantees that clients hold full control over their individual information. Instep of entrusting delicate data to centralized substances, clients can give transitory get to to their KYC information, with the confirmation that their information remains scrambled and blocked off without their unequivocal consent.

## 1.2 ETHEREUM AND ETHEREUM WALLET

Ethereum is a decentralized, open-source blockchain platform that enables the development of smart contracts and decentralized applications (DApps). It was proposed by Vitalik Buterin in late 2013 and development began in early 2014, with the network officially launching on July 30, 2015. Ethereum's native cryptocurrency is called Ether (ETH), which serves as both a means of value transfer and a "fuel" for executing smart contracts and transactions on the network.

Here are some key features and concepts related to Ethereum:

**1. Smart Contracts**: Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They automatically execute and enforce the terms of the agreement when predefined conditions are met. Ethereum's blockchain enables the deployment and execution of smart contracts, opening up possibilities for a wide range of applications, including decentralized finance (DeFi), supply chain management, decentralized autonomous organizations (DAOs), and more.

**2. Decentralized Applications (DApps):** Ethereum allows developers to build decentralized applications (DApps) on top of its blockchain. These applications can offer various functionalities, such as financial services, games, social networks, and decentralized exchanges. DApps interact with smart contracts to perform transactions and execute logic in a trustless and decentralized manner.

**3. Ethereum Virtual Machine (EVM):** The Ethereum Virtual Machine is a runtime environment that executes smart contracts on the Ethereum network. It is a Turing-complete virtual machine, meaning it can run any arbitrary code, making it highly flexible for developers.

**4. Consensus Mechanism**: Ethereum currently uses a Proof of Work (PoW) consensus mechanism similar to Bitcoin, where miners compete to solve complex mathematical puzzles to validate and add new blocks to the blockchain. However, Ethereum is in the process of transitioning to Ethereum 2.0, which will implement a Proof of Stake (PoS) consensus mechanism. PoS relies on validators who lock up a certain amount of Ether as stake to validate transactions and create new blocks.

**5. Ethereum Wallet:** An Ethereum wallet is a software application or service that allows users to store, send, and receive Ether (ETH) and other Ethereum-based tokens. It consists of a public address (used for receiving funds) and a private key (used for accessing and controlling funds). Ethereum wallets come in various forms, including desktop wallets, mobile wallets, web wallets, and hardware wallets.

**6. Ethereum Improvement Proposals (EIPs):** EIPs are proposals for improvements or new features to be added to the Ethereum protocol. They are discussed and implemented through Ethereum's community-driven governance process, allowing for continuous innovation and upgrades to the platform.

## 1.3 METAMASK

MetaMask is a popular cryptocurrency portmanteau and cybersurfer extension that allows druggies to interact with the Ethereum blockchain. It serves as a ground between the traditional web and blockchain technology, enabling druggies to manage their Ethereum- grounded means and access decentralized operations( DApps) directly from their web cybersurfers. Then is a breakdown of its crucial features and functionalities

1. Wallet MetaMask functions as a digital portmanteau where druggies can securely store, shoot, and admit Ethereum( ETH) and other ERC- 20 commemoratives. It generates and manages Ethereum addresses, which are used for deals on the Ethereum network.

2. Cybersurfer Extension MetaMask is primarily available as a cybersurfer extension for popular web cybersurfers like Chrome, Firefox, Brave, and Edge. formerly installed, it integrates seamlessly with the cybersurfer, allowing druggies to interact with Ethereum- grounded operations directly from their cybersurfers.

3. stoner Interface MetaMask provides a stoner-friendly interface that allows druggies to manage their cryptocurrency effects and interact with DApps. It displays account balances, sale history, and other applicable information.

4. Decentralized operations( DApps) MetaMask enables druggies to pierce and interact with colorful DApps erected on the Ethereum blockchain. These DApps cover a wide range of use cases, including decentralized finance( DeFi), gaming, social networks, and more. druggies can connect their MetaMask portmanteau to these DApps to perform colorful conduct, similar as trading commemoratives, advancing and adopting means, sharing in token deals, and playing games.

5. Security MetaMask emphasizes security by furnishing features similar as translated vaults, word protection, and seed expression backups. druggies are needed to produce a strong word and coagulate their seed expression( a series

of words used to recover the portmanteau) during the setup process. also, MetaMask warns druggies about potentially vicious websites and phishing attempts.

6. Network Support MetaMask supports multiple Ethereum networks, including the Ethereum mainnet, testnets( Ropsten, Rinkeby, Kovan), and custom networks. This inflexibility allows inventors to test their DApps on different networks before planting them to the mainnet.

7. Interoperability MetaMask can be integrated with other blockchain services and operations, allowing for flawless interoperability between different platforms and services.

### 1.4 OBJECTIVES

The objectives of this research paper are as follows:

**1.** To explain how a blockchain-based system can be used in the KYC document verification and storage process by any financial institutions and individuals.

**2.** To check whether the blockchain technology can be fully trusted by any financial institution for KYC verification

### 1.5 BLOCKCHAIN CHARACTERISTICS

Numerous exceptional features of blockchain technology can aid in the KYC document verification procedure. The following are a blockchain's salient features:

- Secure document verification using Blockchain and IPFS technologies
- Decentralized system, with no central authority or single point of failure
- Fast and easy verification process, with no need for intermediaries or third-party services
- User-friendly interface for document upload and verification
- Support for multiple document types and formats

## 2. LITERATURE SURVEY

1. "Blockchain for Identity and Access Management: A Literature Review" by Al-Turjman, Fadi M., et al. (2019) This article provides a comprehensive overview of blockchain-based identity and access systems, including their applications in KYC processes. It discusses various blockchain platforms, consensus mechanisms, and privacy-enhancing techniques used for identity verification.

2. "Blockchain-Based KYC for Anti-Money Laundering" by Azzopardi, Simon, et al. (2018) This study explores the potential of blockchain technology in improving KYC procedures to prevent money laundering. It explores the use of distributed ledger technology, smart contracts and cryptographic techniques to improve the security and efficiency of KYC verification.

3. "A Survey on Blockchain Identity Management: Requirements, Challenges, and Opportunities" by Nguyen, Khoa, et al. (2020) This research paper provides an overview of blockchain-based identity management systems, focusing on their applicability in KYC processes. It discusses the requirements, challenges and opportunities associated with incorporating blockchain technology into identity verification workflows.

4. "Blockchain-Based KYC Verification: A Systematic Review" by Singh, Jaskirat, et al. (2021) This systematic review analyzes the existing literature on blockchain-based KYC verification systems. It identifies the main features, implementation challenges and potential benefits of using blockchain technology for identity verification in various industries.

5. "Blockchain and KYC: A Game Changer in Identity Verification" by Kshetri, Nir (2018) This article examines the impact of blockchain technology on KYC processes and identity verification. It discusses the potential benefits of distributed identity systems, such as better privacy, security and management of users' personal information.

6. "Blockchain-Based Identity Management Systems: A Literature Review and Research Agenda" by Makhdoom, Irfan, et al. (2020) This literature review examines the development of blockchain-based identity management systems and their potential applications in KYC authentication. It identifies research gaps and suggests future research directions for the development of blockchain-based identity solutions.

7. "Decentralized Identity Management and Verification Using Blockchain Technology" by Azaria, Asaf, et al. (2016) This paper presents a decentralized identity management framework that uses blockchain technology. It discusses the role of smart contracts and cryptographic technologies in enabling secure and efficient KYC verification processes.

8. "Blockchain-Based KYC Compliance: Opportunities and Challenges" by Huh, Sangmin, et al. (2018) This study explores the opportunities and challenges of implementing blockchain-based KYC compliance solutions. It explores

regulatory considerations, interoperability and scalability issues related to blockchain-enabled identity verification systems.

9. "Identity Management Systems: A Blockchain-Based Survey" by Biswas, Kshirasindhu, et al. (2020) This survey paper provides an overview of blockchain-based identity management systems with a focus on their relevance for KYC verification processes. It discusses the role of distributed identifiers, zero-knowledge certificates and autonomous identity principles in improving the security and privacy of identity verification.

10. "Blockchain-Based KYC Verification Systems: A Review of Current Trends and Future Directions" by Patel, Dhruvit, et al. (2021) This review analyzes current and future trends in blockchain-based KYC verification systems. It covers emerging technologies, regulatory developments and industry initiatives aimed at improving the efficiency and reliability of KYC processes using blockchain technology.

## 3. 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.

## 4. PROPOSED SYSTEM

The blockchain system is controlled by its nodes, there is no central authority required. All the nodes have the same information with them, thus the data in a blockchain cannot be changed. We can add new documents, but only when they match the previous documents. In this paper, we have proposed a way we can utilize blockchain for KYC document verification using smart contracts. It will save a lot of effort, paperwork, and time for both parties. The smart contract makes the process even easier and better as it works as per the specified conditions. If a set of documents are not valid according to its conditions, it will reject them. Whereas the current KYC system will take a long time to determine whether a document is valid or not.

### 4.1 Flowchart 1

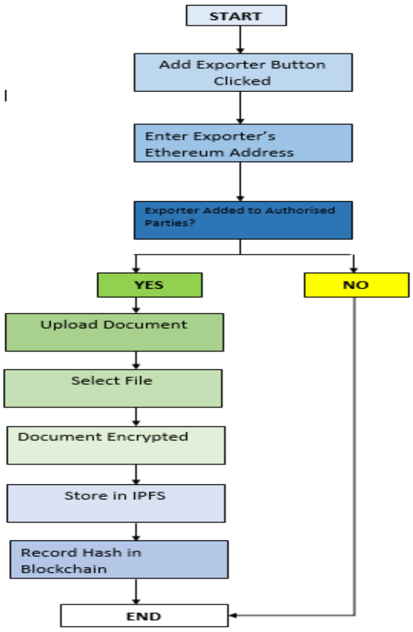
START
Add Exporter Button Clicked
Enter Exporter's Ethereum Address
Exporter Added to Authorised Parties?
YES
NO
Upload Document
Select File
Document Encrypted
Store in IPFS
Record Hash in Blockchain
END

**Fig. 1**Document Uploading For Verification

### 4.2 Flowchart 2

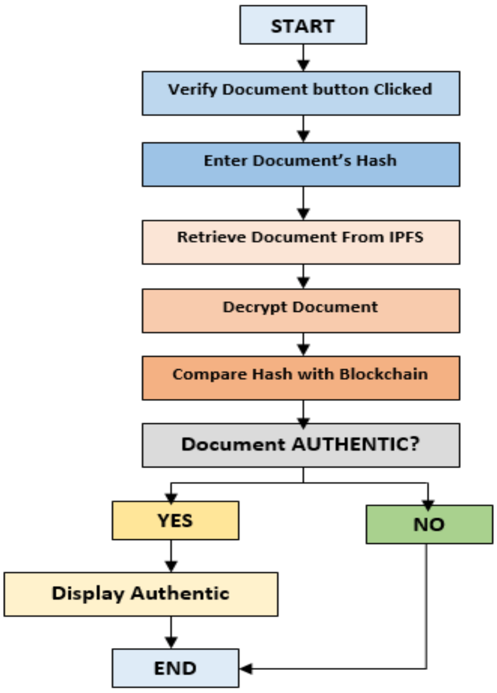

**Fig. 2** Verification of Document

## 5. METHODOLOGY

1. The  proprietor of the system must first add an exporter to the list of authorized parties. This is done by clicking on the" Add Exporter" button and entering the exporter's Ethereum address.

2. Upload a document to the system by clicking on the" Upload Document" button and  opting  a  train from your computer. The document will be translated and stored in the IPFS network, and its hash will be recorded in the Blockchain.

3. corroborate a document by clicking on the" corroborate Document" button and entering its unique identifier( hash) in the input field. The system will  recoup the document from the IPFS network,  decipher it, and compare its hash with the one recorded in the Blockchain.

4. The system will display a communication indicating whether the document is authentic or not.

## 6. ADVANTAGES

Using blockchain, Ethereum, and MetaMask for Know Your client( KYC) verification offers several advantages

1. **Security**: Blockchain technology ensures the security of data through cryptographic principles. Each KYC record can be securely stored on the blockchain, and access can be  confined using encryption  ways. This reduces the  threat of data breaches and unauthorized access.

2. **Invariability**: Once data is recorded on the blockchain, it can not be altered or deleted. This  point ensures the integrity of KYC records,  furnishing a tamper-  evidence  inspection trail of all verification conditioning.

3. **Decentralization**: Ethereum is a decentralized platform, meaning there's no central authority controlling the network. This eliminates the need for a trusted  conciliator in the KYC process, reducing the  threat of manipulation or bias.

4. **Translucency**: Blockchain technology enables transparent and auditable deals. All KYC conditioning, including verification requests and  blessings, can be recorded on the blockchain,  furnishing  translucency to controllers and stakeholders.

5. **Efficiency**: By  using smart contracts on the Ethereum blockchain, KYC processes can be automated, reducing homemade intervention and processing times. Smart contracts can execute predefined rules and conditions, streamlining the verification process.

4. **Cost Savings**: Using blockchain for KYC verification can lead to cost savings by  barring the need for  interposers, reducing paperwork, and streamlining processes. This is particularly  salutary for associations that handle a large volume of KYC checks.

**5. Global Availability**: Blockchain- grounded KYC results are accessible from anywhere in the world with an internet connection. This enables flawless verification for druggies across different geographical locales, fostering fiscal addition and availability.

6. **Interoperability**: Ethereum's open- source nature allows for interoperability with other blockchain platforms and operations. This means that KYC verification processes erected on Ethereum can fluently integrate with other systems and services, enhancing interoperability and scalability.

7. **Compliance Blockchain**: grounded KYC results can help associations misbehave with nonsupervisory conditions more efficiently. By using transparent and auditable processes, associations can demonstrate compliance with KYC regulations to controllers and adjudicators.

## 7. CONCLUSION

In this paper, we've suggested a KYC verification using blockchain technology and its armature which might help in cutting down the costs of KYC verification and make the process easier for guests. The current fiscal system might see good growth if only valid druggies can pierce it and for that, this KYC verification system can surely bring some changes. This design aims to produce a secure and decentralized system for document verification using Blockchain and InterPlanetary train System( IPFS) technologies. The system stores the hash of the documents in the Blockchain network and the documents themselves in the IPFS network. This ensures that the documents can not be tampered with or altered, and they can be fluently recaptured and vindicated by sanctioned parties.

## ACKNOWLEDGMENT

We amplify sincere much appreciated to Prof. Sayali Karmode, our committed direct, for important back, direction, and support. Their conviction in our capacities, coupled with adaptability in work plans, was instrumental in completing this paper. Our appreciation too amplifies to all who straightforwardly or by implication contributed to our research.

## 8. REFERENCES

[1] "Blockchain for Identity and Access Management: A Literature Review" by Al-Turjman, Fadi M., et al. (2019)

[2] "Blockchain-Based KYC for Anti-Money Laundering" by Azzopardi, Simon, et al. (2018)

[3] "A Survey on Blockchain Identity Management: Requirements, Challenges, and Opportunities" by Nguyen, Khoa, et al. (2020)

[4] "Blockchain-Based KYC Verification: A Systematic Review" by Singh, Jaskirat, et al. (2021)

[5] "Blockchain and KYC: A Game Changer in Identity Verification" by Kshetri, Nir (2018)

[6] "Blockchain-Based Identity Management Systems: A Literature Review and Research Agenda" by Makhdoom, Irfan, et al. (2020)

[7] "Decentralized Identity Management and Verification Using Blockchain Technology" by Azaria, Asaf, et al. (2016)

[8] "Blockchain-Based KYC Compliance: Opportunities and Challenges" by Huh, Sangmin, et al. (2018)

[9] "Identity Management Systems: A Blockchain-Based Survey" by Biswas, Kshirasindhu, et al. (2020)

[10] "Blockchain-Based KYC Verification Systems: A Review of Current Trends and Future Directions" by Patel, Dhruvit, et al. (2021)

[11] S. Gore, S. Hamsa, S. Roychowdhury, G. Patil, S. Gore and S. Karmode, "Augmented Intelligence in Machine Learning for Cybersecurity: Enhancing Threat Detection and Human-Machine Collaboration," 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2023, pp. 638-644, doi: 10.1109/ICAISS58487.2023.10250514.

[12] Layth Almahadeen, Renzon Daniel Cosme Pecho, Murugananth Gopal Raj, Nichenametla Rajesh, Zainab Mohammed Imneef, Sayali Karmode Yelpale, “Digital Investigation Forensic Model with P2P Timestamp Blockchain for Monitoring and Analysis” , Journal of Electrical System, Vol. 1, No 1, (2024): 09-17 ( DOI : https://doi.org/10.52783/jes.656)

[13] Sayali Karmode, Security Challenges for IoT Based Applications & Solutions Using Fog Computing: A Survey, Journal of Journal of Cybersecurity and Information Management, Vol. 3 , No. 1 , (2020) : 21-28 (Doi : https://doi.org/10.54216/JCIM.030103)

[14] M. S. K. Yelpale, “Security and privacy challenges in cloud computing: a review,” Journal of Cybersecurity and Information Management, vol. 4, no. 1, pp. 36–45, 2020.

[15] Sayali Karmode Yelpale, "IOT Technology for Pandemic Situation", NJITM, vol. 4, no. 2, pp. 25–27, Jan. 2022 https://mbajournals.in/index.php/JoITM/article/view/806.

[16] Karmode, S. S., & Bhagat, V. B. (2017). DETECTION AND BLOCKING SOCIAL MEDIA MALICIOUS POSTS. International journal of modern trends in engineering and research, 4(5).

[17] Kermode, S. S., & Bhagat, V. B. (2016). A Review: Detection and Blocking Social Media Malicious Posts. Int. J. Mod. Trends Eng. Res, 3(11), 130-136. doi: 10.21884/IJMTER.2016.3133.Q4M8O .

[18] Prof. Bhushan B. Thakare, Prof. Sayali Karmode Yelpale, "Smart Home with Edge Computing", International Journal of Interdisciplinary Innovative Research & Development (IJIIRD), Vol 6, 2021 https://ijiird.com/wp-content/uploads/CSE016-1.pdf

[19] Sayali Karmode, "Blockchain Technology Security Issues and Concerns : A Review", International Research Journal of Modernization in Engineering Technology and Science, Vol 6, Issue 03, March 2024 https://www.doi.org/10.56726/IRJMETS50249

[20] Pranav Chavan, Harshraj Deshmukh, Aakash Dhotre, Aditya Gharat, Sayali Karmode, "Blockchain Democracy : Evaluating a Secure Voting System", International Research Journal of Modernization in Engineering Technology and Science, Vol 6, Issue 03, March 2024, https://www.doi.org/10.56726/IRJMETS50478

[21] B. J. Dange, Kaustubh Manikrao Gaikwad, H. E. Khodke, Santosh Gore, S. N. Gunjal, Kalyani Kadam, Sayali Karmode, "Machine Learning for Quantum Computing Bridging the Gap between AI and Quantum Algorithms", Int J Intell Syst Appl Eng, vol. 12, no. 21s, pp. 600–605, Mar. 2024.

[22] N Kumar, E Howard, S Karmode, "Reinforcement Learning for Optimal Treatment Planning in Radiation Therapy", NATURALISTA CAMPANO, Vol 28, Issue 1, 2024, https://museonaturalistico.it/index.php/journal/article/view/355