JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

KYC VERIFICATION USING CIPHER TEXT POLICY ATTRIBUTE-BASED ENCRYPTION AND BLOCK CHAIN TECHNOLOGY

Mrs. S. Arunakumari[1], Dr. R. Gomathi[2], Mr. R. Arunkumar[3],
Assistant Professor[1], AI&DS, IFET College Engineering, Tamil Nadu, India.
Assistant Professor[2], EEE, MRK Institute of Technology, Tamil Nadu, India.
Assistant Professor[3], MECH, MRK Institute of Technology, Tamil Nadu, India.

ABSTRACT:

The Know Your Customer (KYC) process plays a vital role in the financial industry, especially for banks and other financial institutions. Its main objective is to verify the identities of customers, ensuring their legitimacy. This verification is essential to prevent illicit activities such as money laundering and terrorism financing, which can have severe repercussions for both the financial sector and society. Historically KYC procedures have heavily relied on manual methods that are now considered outdated and problematic. These methods entail the collection and validation of various identification documents from customers, often involving extensive paperwork and in-person visits to physical bank branches. The manual nature of these procedures results in time-consuming processes and a heightened risk of errors in contrast blockchain-based KYC verification presents an innovative solution. It offers decentralization, immutability, and heightened security. Blockchain technology makes use of advanced encryption algorithms like Ciphertext-Policy Attribute-Based Encryption (CPABE) to reinforce security measures. The immutability of blockchain ensures the integrity and accuracy of KYC data. Once customer information is recorded on the blockchain, it becomes impossible to alter or delete without proper authorization. This eliminates the risk of fraud and data tampering, addressing common issues in traditional KYC procedures. Financial institutions can rely on the precision of customer data and their adherence to regulatory requirements.

Keywords: KYC Procedure, Banks, Legitimacy Verification, Money Laundering, Drug Trafficking, Terrorism, Manual KYC Procedure, Dated, Time-consuming, Less Secure, Blockchain-based KYC Verification, Decentralized, Immutable, Secure Features, CPABE Algorithm, System Security, Financial Transactions, Sensitive Data, Organizations, Financial Institutions Validate KYC Documents.

INTRODUCTION:

In the ever-evolving landscape of the financial sector, ensuring customer legitimacy and preventing illicit activities is a top priority. Financial institutions, particularly banks, have a substantial role in the global economy, and they carry both a moral and regulatory responsibility to protect their services from exploitation by criminals engaged in activities such as money laundering, drug trafficking, and terrorism financing. To fulfil this obligation, banks implement the "Know Your Customer" (KYC) [1] procedure, serving as a critical defense to identify and verify their customers' authenticity The KYC procedure is a fundamental component of the financial industry, essential for maintaining the integrity of the banking system. Its primary objective is to establish a thorough understanding of each customer, ensuring their true identity and the legitimacy and transparency of their financial activities. This approach enables financial institutions to mitigate the risks associated with criminal activities and comply with regulatory requirements The traditional manual KYC procedure, which has long been the standard for customer verification, faces various challenges that impede its effectiveness. [2] This manual process relies on cumbersome paperwork, time-consuming administrative tasks, and limited security measures. As financial crimes become more sophisticated, the shortcomings of this outdated method become increasingly evident. Additionally, manual KYC procedures can be burdensome for customers, involving in-person visits to physical bank branches and extensive documentation Recognizing the limitations of the traditional KYC process, the financial industry is at a crossroads, seeking innovative and secure solutions to modernize customer verification. [3] In this pursuit, blockchain technology has emerged as a promising solution. Blockchain, a decentralized and immutable ledger, possesses features that align well with the evolving needs of KYC verification.

Our primary contributions can be summarised as follows:

- Blockchain's decentralized and immutable ledger ensures the highest level of security for KYC data. It guards against data breaches, tampering, and unauthorized access, contributing to a robust defense against financial crimes.
- The CPABE algorithm integrated into blockchain-based KYC systems ensures that sensitive customer information remains confidential. It provides privacy controls while allowing authorized access.
- The immutability of blockchain ensures the integrity and accuracy of KYC data, reducing the risk of fraud and manipulation.
- Blockchain-based KYC [5] offers customers a more seamless and convenient onboarding experience, promoting trust and satisfaction with financial institutions.

RELATED WORK:

A. System Architecture:

Creating a working system for the blockchain-based KYC verification described in the statement is a complex and multifaceted task. Below is a high-level overview of the components and steps involved in building such a system.

1) Choose a Blockchain Platform:

Select a suitable blockchain platform that aligns with the requirements of KYC verification. Ethereum, Hyperledger Fabric, and Corda are popular options.

2) Smart Contracts:

Develop smart contracts to manage the KYC process. Smart contracts will handle data storage, access control, and validation rules. [7]

3) Decentralized Identity:

Implement decentralized identity solutions to give customers control over their KYC data. This may involve the use of Self-Sovereign Identity (SSI) principles.

4) CPABE Integration:

Incorporate the Ciphertext-Policy Attribute-Based Encryption (CPABE) algorithm into the system to enhance data security and attribute-based access control.

B. Data Management:

1) KYC Data Storage:

Define the data structure for storing KYC information on the blockchain. Ensure that sensitive data is encrypted and securely stored.

2) User Data Control:

Develop mechanisms for users to manage their KYC data, granting and revoking access to specific attributes as needed.

C. User Interaction:

1) User Interfaces:

Create user-friendly interfaces for both customers and bank personnel to interact with the system. This may include web and mobile applications.

2) On boarding Process:

Design an efficient on boarding process where customers can submit their KYC documents electronically. Implement document verification and validation procedures.

D. Identity Verification:

1) Identity Verification Providers:

Integrate with identity verification providers and government databases to verify customer identities.

2) Biometric Verification:

Implement biometric authentication methods for added security, such as facial recognition or fingerprint scanning.

E. Access Control:

1) Role-Based Access Control:

Define roles within the system (e.g., customer, bank employee, regulator) and implement role-based access control to ensure that only authorized individuals can access KYC data.

2) CPABE Attribute Policies:

Configure attribute-based access control policies using CPABE, allowing fine-grained control over data access.

F. Testing and Quality Assurance:

1) Testing:

Perform extensive testing, including functional, security, and performance testing, to ensure the system operates as intended.

G. Monitoring and Maintenance:

1) Continuous Monitoring:

Continuously monitor the system for performance, security, and compliance. Implement updates and improvements as needed.

H. Education and Awareness:

1) Industry Awareness:

Raise awareness within the industry about the benefits and potential of blockchain-based KYC verification through educational initiatives, conferences, and publications.

LITERATURE SURVEY:

Blockchain technology and smart contracts have found applications across various domains. In particular, there has been a significant focus on the use of blockchain for identification and authentication systems, showcasing their effectiveness in managing identity and authentication processes. However, electronic Know Your Customer (e-KYC) [9] procedures are considerably more intricate than simple authentication tasks. They encompass secure credential registration, KYC document management, secure verification between clients, multiple financial institutions (FIs), and a dedicated blockchain platform. Furthermore, the emergence of new forms of remote and spoofing attacks targeting KYC systems necessitates countermeasures.

Recent research in the realm of blockchain-based e-KYC places a strong emphasis on secure user identity management, credential verification, and the optimization of communication processes among FIs. For instance, one innovative approach employs the Inter Planetary File System (IPFS) [10] and blockchain for KYC document verification. Customers initiate identity registration with a bank, and their credentials are subsequently hashed and encrypted. However, it's worth noting that these solutions often overlook addressing privacy concerns and transaction traceability within blockchain networks.

Another proposal introduces a proof-of-concept (PoC) blockchain-based KYC system deployed within a private blockchain environment, concentrating on permissioned document sharing to streamline the KYC workflow.

Other initiatives involve the utilization of smart contracts in combination with IPFS for e-KYC processes. Smart contracts manage various KYC document operations, while KYC data is stored in IPFS. However, these methods frequently lack essential encryption mechanisms to safeguard KYC data.

To enhance privacy and security, some research efforts apply Ciphertext-Policy Attribute-Based Encryption (CP-ABE). [11] This approach allows for dynamic attribute management on the blockchain, aiding in efficient user attributes management. Some schemes combine CP-ABE with blockchain technology to enable traceable data sharing and data privacy protection.

To tackle computational costs, specific proposals introduce Zero-Knowledge Proof (ZKP) [12] authentication and encryption schemes tailored for lightweight encryption, particularly in Internet of Things (IoT) applications. These schemes incorporate ZKP for authentication while maintaining data security.

Lastly, smart contract implementations aim to facilitate consent-driven and double-blind data sharing on the Hyperledger Fabric blockchain platform. These smart contracts generate customer consent and enable public key sharing for document encryption, although they may lack digital signature binding for customer consent.

METHODOLOGY:

Leveraging Cloud Infrastructure: The e-KYC system is hosted on a cloud platform to optimize resource utilization and enhance accessibility for authorized users.

Ensuring Security and Privacy: The primary objective is to guarantee the security and privacy of e-KYC documents stored in the cloud. This involves the implementation of robust security measures, including strong authentication and encryption techniques.

Incorporating Blockchain Technology: The proposed system integrates blockchain technology to enhance trust and security. [14] By utilizing a blockchain, e-KYC data and transactions are securely stored, leveraging the decentralized and tamper-resistant properties of the technology to maintain data integrity and reliability.

Utilizing Ciphertext Policy Attribute-Based Encryption (CP-ABE): The methodology adopts CP-ABE, a cryptographic approach that facilitates fine-grained access control based on specific attributes or policies. This ensures that access to e-KYC data is limited to authorized entities, promoting privacy and data security.

Enforcing Client Consent: The system enforces client consent for access to their KYC data, ensuring that sensitive information can only be accessed with explicit permission from the user, thus enhancing privacy and data protection.

Validation Through Experiments: To assess the system's effectiveness, a series of experiments are conducted to evaluate its efficiency and scalability in practical scenarios. These experiments encompass various conditions and workloads to demonstrate the system's real-world viability. The methodology combines cloud infrastructure, blockchain technology, CP-ABE, [15] and client consent enforcement to develop a secure and privacy-compliant e-KYC system with a focus on fine-grained access control and operational efficiency. The system's practical viability is demonstrated through comprehensive experimentation.

Existing System

Challenges with Traditional: KYC The statement acknowledges that the conventional KYC approach used by banks is commonly regarded as unreliable and cost-intensive. This highlights the current issues within the industry, underscoring the demand for more streamlined and secure verification methods.

Role of Blockchain: The research investigates the potential of Blockchain technology in addressing these challenges. Blockchain's renown for reliability and security positions it as an attractive option for deployment in the banking sector.

Transforming Banking Practices: The primary goal of this study is to explore the transformative possibilities brought about by the integration of Blockchain technology in the banking sector, especially in the context of KYC document verification. The primary emphasis is on securely storing and vigilantly monitoring information.

Optimized KYC System: The research underscores the pressing need to implement an optimized KYC system that integrates Blockchain technology. This advanced system is expected to enhance security, reliability, and trustworthiness, while simultaneously resolving issues related to scalability and data privacy.

Analysis of Previous Research: The article conducts a thorough review and examination of earlier relevant research and studies in this field. These prior works are likely to provide valuable insights into the benefits and challenges associated with incorporating Blockchain into KYC processes. [16] Notably, it highlights how Blockchain has the potential to eliminate the reliance on intermediaries, thus reducing the likelihood of errors and malicious activities typically associated with manual tasks in the KYC process. the existing research is centered on recognizing the deficiencies of the traditional KYC approach in the banking sector, the promise offered by Blockchain technology, and the essentiality of a refined, secure KYC system. Moreover, it accentuates the role of Blockchain in reducing dependency on intermediaries and elevating the overall efficiency and security of the KYC procedure.

5.1 Draw backs of Existing System:

- Data privacy and security concerns
- Cost and Investment
- Resistance to change
- Scalability issues
- Regulatory compliance

5.2 Architecture of Existing System

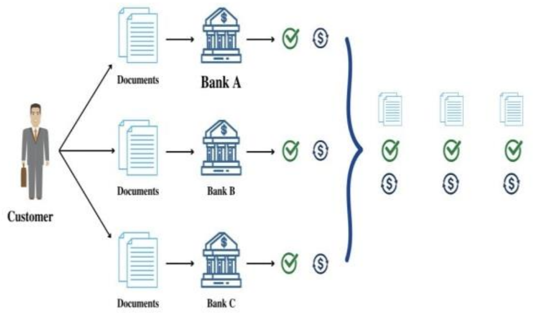


Fig 1. Architecture of the existing system

PROPSED SYSTEM:

The Know Your Customer (KYC) procedure is used by banks to verify the legitimacy of their customers and prevent criminal elements from using banks for money laundering schemes. The current manual KYC procedure is dated, time-consuming, and less secure. Blockchain-based KYC verification can be used to remove these restrictions because it has decentralized, immutable, and secure features. Blockchain also includes the CPABE algorithm to boost system security. [17] Organizations will frequently use blockchain technology to conduct financial transactions and safeguard sensitive data. Financial institutions can use the blockchain system and CPABE algorithm to validate KYC documents. The proposed initiative aims to revolutionize the KYC verification process in financial institutions by introducing a blockchain-based system. This system will address the shortcomings of the current manual KYC procedure and mitigate the risks associated with financial crimes like money laundering and terrorism financing. The key components and steps of this proposal include:

Blockchain Integration: Integrate blockchain technology into the existing KYC verification process to create a decentralized and distributed ledger for storing customer information and verification data.

Immutable Records: Exploit the immutability of blockchain to establish tamper-resistant records of KYC information, ensuring that once data is added, it cannot be altered or deleted.

Smart Contracts: Implement smart contracts to automate various aspects of the KYC process, allowing for the definition of rules and conditions for verifying customer information and triggering actions based on predefined criteria.

CPABE Algorithm: Enhance security by integrating the Ciphertext-Policy Attribute-Based Encryption (CPABE) [18] algorithm, which enables fine-grained access control and encryption of sensitive KYC documents.

Decentralization: Distribute the KYC verification process across the nodes of the blockchain network, reducing reliance on a central authority and enhancing overall security.

Data Privacy: Ensure that customer data remains confidential and is accessible only to authorized entities by utilizing encryption and access control mechanisms provided by CPABE.

Regulatory Compliance: Ensure compliance with relevant financial regulations and data protection laws, such as GDPR or local privacy regulations.

User-Friendly Interface: Develop an intuitive interface for customers and bank personnel to interact with the blockchain-based KYC system, making the process efficient and convenient.

Testing and Evaluation: Conduct comprehensive testing and evaluation to verify the system's effectiveness, security, and performance compared to the traditional manual KYC process.

Training and Adoption: Train bank staff and relevant stakeholders in using the new blockchain-based KYC system and promote its adoption within the organization.

This proposal aims to modernize the KYC verification process, enhancing its security, transparency, and efficiency while effectively combating financial crimes and improving customer data protection.

6.1 Advantages:

- Enhanced security
- Privacy Compliance
- Efficiency and Scalability
- Reduced key Management
- Cloud Implementation

6.2 Architecture diagram for the proposed system:

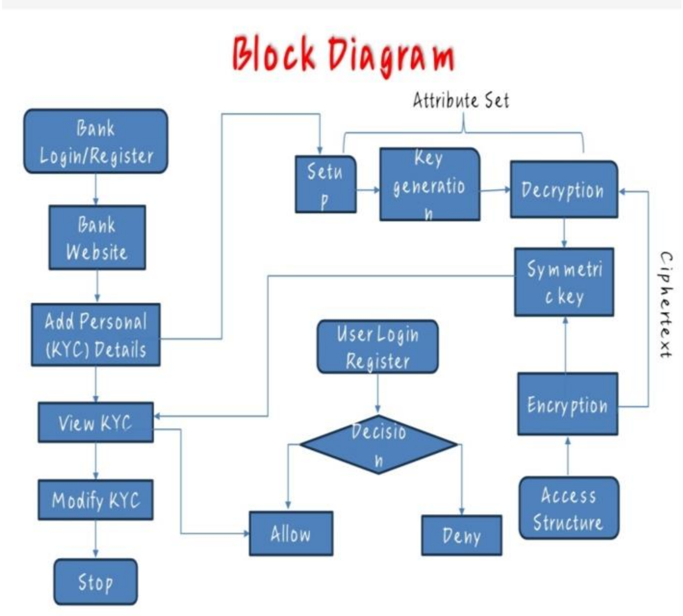
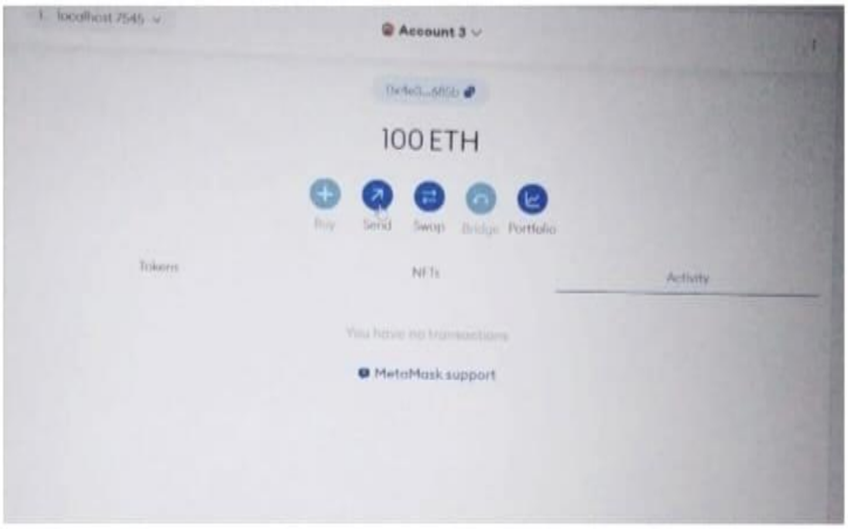


Fig 2. The Architecture of the proposed system

RESULT:

Banks heavily depend on the Know Your Customer (KYC) procedure to authenticate their customers and prevent criminal activities such as money laundering, drug trafficking, and terrorism. The traditional manual KYC process is antiquated, time-consuming, and lacks adequate security measures. Blockchain-based KYC verification provides a solution by introducing decentralization, immutability, and heightened security features. Additionally, the integration of the CPABE algorithm within blockchain technology enhances system security.[20] Many organizations are adopting blockchain for financial transactions and data protection, while financial institutions are using it for KYC document validation.

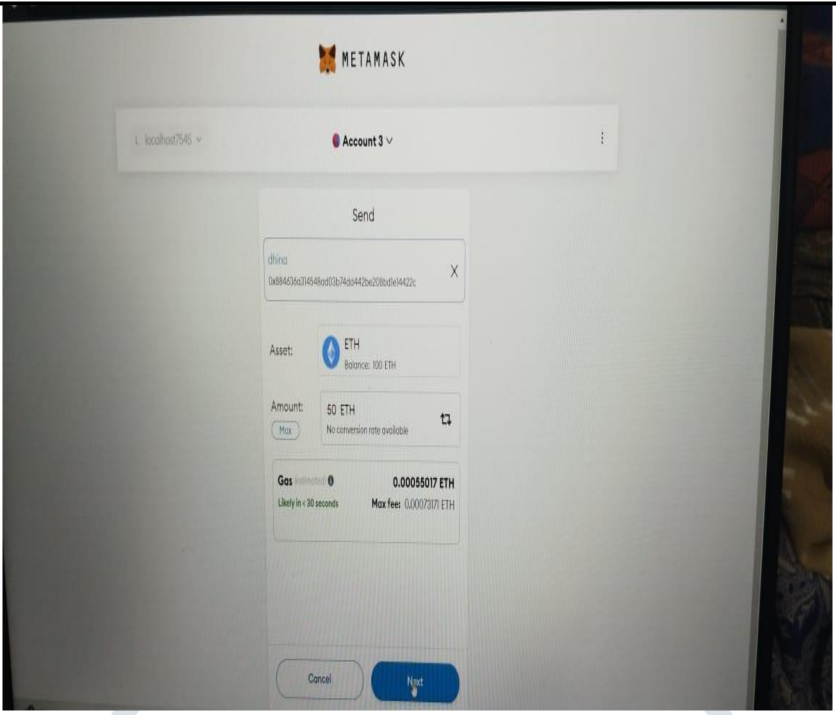
Know Your Customer (KYC) is a procedure employed by financial institutions, especially banks, to validate the authenticity of their customers and thwart criminal activities such as money laundering, drug trafficking, and terrorism. The conventional manual KYC process is outdated, time-consuming, and less secure. Implementing blockchain-based KYC verification can eliminate these drawbacks due to its decentralized, immutable, and secure characteristics. Furthermore, the incorporation of the CPABE algorithm in blockchain enhances system security. Financial institutions can harness this technology to validate KYC documents efficiently.



100 ETH

You have no transactions

Fig 3. Account was created.



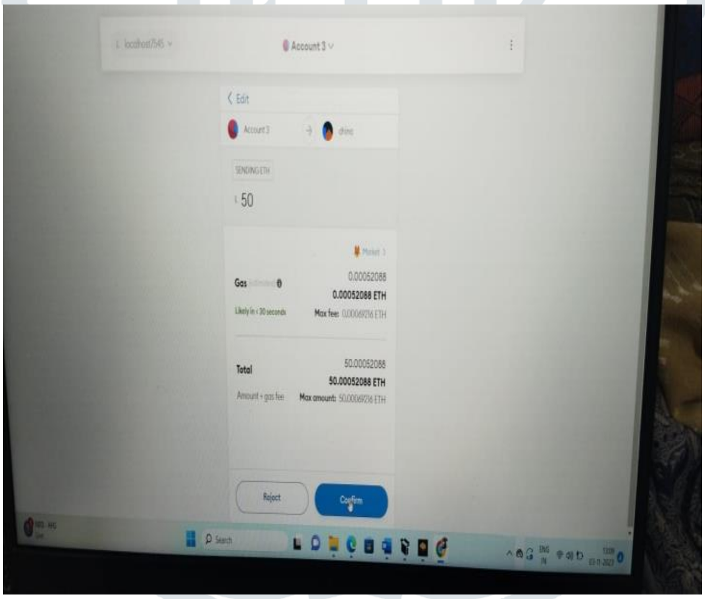
dhina
0x884636a314548ad03b74dd442be208bd1e14422c

Asset: ETH
Balance: 100 ETH

Amount: 50 ETH
No conversion rate available

Gas (estimated) 0.00055017 ETH
Likely in < 30 seconds Max fee: 0.00073171 ETH

Fig 4. select the account for transaction



Account 3 → dhina

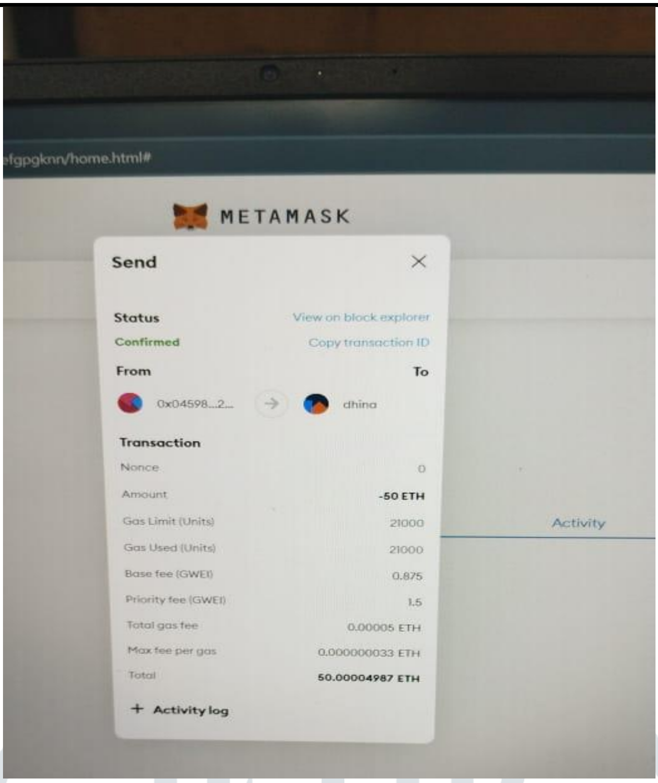
SENDING ETH

50

Gas (estimated) 0.00052088
0.00052088 ETH
Likely in < 30 seconds Max fee: 0.00069216 ETH

Total 50.00052088
50.00052088 ETH
Amount + gas fee Max amount: 50.00069216 ETH

Fig 5. Transaction account confirm



efgpgknn/home.html#

METAMASK

Send ×

Status — View on block explorer

Confirmed — Copy transaction ID

From → To

0x04598...2... → dhina

Transaction

Nonce	0
Amount	-50 ETH
Gas Limit (Units)	21000
Gas Used (Units)	21000
Base fee (GWEI)	0.875
Priority fee (GWEI)	1.5
Total gas fee	0.00005 ETH
Max fee per gas	0.000000033 ETH
Total	50.00004987 ETH

+ Activity log

Fig 6. After transaction completed

CONCLUSION:

To conclude, the Know Your Customer (KYC) process is a vital component for banks to verify their customers' authenticity and combat illegal activities such as money laundering, drug trafficking, and terrorism. The traditional manual KYC procedure has become outdated, cumbersome, and less secure. However, the integration of blockchain-based KYC verification offers a promising solution, featuring decentralization, immutability, and enhanced security attributes. The inclusion of the CPABE algorithm within blockchain further reinforces system security. As a result, we can expect a broad adoption of blockchain technology by various organizations for secure financial transactions and data protection. Financial institutions are poised to benefit from this technology, utilizing the blockchain system and CPABE algorithm for efficient KYC document validation, leading to a more secure and streamlined KYC process.

The Know Your Customer (KYC) process is a critical procedure employed by banks to confirm the authenticity of their customers and to deter the use of banks for illicit activities such as money laundering, drug trafficking, and terrorism. The current manual KYC process is outdated, time-consuming, and lacks robust security measures. Blockchain-based KYC verification presents a solution to address these issues by offering decentralization, immutability, and enhanced security features. Furthermore, blockchain incorporates the CPABE algorithm, enhancing system security. Many organizations are increasingly adopting blockchain technology for financial transactions and safeguarding sensitive data. Financial institutions can utilize the blockchain system and CPABE algorithm for efficient KYC document validation.

Blockchain technology is capable of addressing the challenges and inefficiencies inherent in traditional KYC processes. Its ability to provide secure, transparent, and immutable record-keeping is highly valuable. Through blockchain, companies can establish a decentralized identity verification system to securely store and share customer data in an unalterable manner. Moreover, blockchain significantly enhances the security level of KYC processes. While traditional KYC processes store customer data in centralized databases vulnerable to cyberattacks and data breaches, blockchain employs advanced cryptographic techniques to ensure the security and privacy of customer data. Its decentralized structure makes it significantly more challenging for hackers to access and manipulate data.

REFERENCES

[1] Rajput, Venkatesh U. "Research on know your customer (KYC)." International Journal of Scientific and Research Publications 3, no. 7 (2013): 541-546.

[2] Kapsoulis, Nikolaos, Alexandros Psychas, Georgios Palaiokrassas, Achilleas Marinakis, Antonios Litke, and Theodora Varvarigou. "Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture." Future Internet 12, no. 2 (2020): 41.

[3] Yadav, Piyush, and Raj Chandak. "Transforming the know your customer (KYC) process using blockchain." In 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), pp. 1-5. IEEE, 2019.

[4] Mondal, Prakash Chandra, Rupam Deb, and Mohammad Nurul Huda. "Know your customer (KYC) based authentication method for financial services through the internet." In 2016 19th International Conference on Computer and Information Technology (ICCIT), pp. 535-540. IEEE, 2016.

[5] Mondal, Prakash Chandra, Rupam Deb, and Mohammad Nurul Huda. "Transaction authorization from Know Your Customer (KYC) information in online banking." In 2016 9th international conference on electrical and computer engineering (ICECE), pp. 523-526. IEEE, 2016.

[6] Soni, Anuraj, and Reena Duggal. "Reducing risk in KYC (know your customer) for large Indian banks using big data analytics." International Journal of Computer Applications 97, no. 9 (2014).

[7] George, Denson, Anand Wani, and Ashutosh Bhatia. "A blockchain based solution to know your customer (kyc) dilemma." In 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6. IEEE, 2019.

[8] Yadav, Piyush, and Raj Chandak. "Transforming the know your customer (KYC) process using blockchain." In 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), pp. 1-5. IEEE, 2019.

[9] Eduardo Demarco, André. "Analysing blockchain/distributed ledger technology in capital markets and know your customer process." Journal of Securities Operations & Custody 12, no. 1 (2020): 58-71.

[10] Drgon, Matus. "Know Your Customer using Distributed Ledger Technology."

[11] Ratnawat, Niraj, Saujanya Pandey, Rudresh Paradkar, and Soumi Banerjee. "Optimizing the KYC Process using a Blockchain based approach." In ITM Web of Conferences, vol. 44, p. 03039. EDP Sciences, 2022.

[12] Schlatt, Vincent, Johannes Sedlmeir, Simon Feulner, and Nils Urbach. "Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity." Information & Management 59, no. 7 (2022): 103553.

[13] Malhotra, Diksha, Poonam Saini, and Awadhesh Kumar Singh. "How blockchain can automate KYC: systematic review." Wireless Personal Communications 122, no. 2 (2022): 1987-2021.

[14] Thavanathan, Jenitha. "Process Innovation with Blockchain in Banking-A case study of how Blockchain can change the KYC process in banks." Master's thesis, NTNU, 2017.

[15] Choi, Nakhoon, and Heeyoul Kim. "A Blockchain-based user authentication model using MetaMask." Journal of Internet Computing and Services 20, no. 6 (2019): 119-127.

[16] Choi, Nakhoon, and Heeyoul Kim. "A Blockchain-based user authentication model using MetaMask." Journal of Internet Computing and Services 20, no. 6 (2019): 119-127.

[17] Nagendra, Chandini. "A decentralized service for personal data privacy protection." PhD diss., California State University, Sacramento, 2020.

[18] Sundareswaran, N., S. Sasirekha, I. Joe Louis Paul, S. Balakrishnan, and G. Swaminathan. "Optimised KYC blockchain system." In 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), pp. 1-6. IEEE, 2020.

[19] Zhang, Yichen, Jiguo Li, and Hao Yan. "Constant size ciphertext distributed CP-ABE scheme with privacy protection and fully hiding access structure." IEEE Access 7 (2019): 47982-47990.

[20] Li, Chunhua, Jinbiao He, Cheng Lei, Chan Guo, and Ke Zhou. "Achieving privacy-preserving CP-ABE access control with multi-cloud." In 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), pp. 801-808. IEEE, 2018.