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 IN BANKING SYSTEM BASEDON BLOCKCHAIN

[1]Satyabrata Behera, [2]Dr. Mir Aadil
[1]Masters Student, [2]Assistant Professor
[1]School of CS & IT,
[1]Jain Deemed To Be University, Bengaluru, India

Abstract: The aim of this project is to develop a decentralized and secure KYC (Know Your Customer) verification system based on blockchain technology. The system will use smart contracts to securely store and manage customer information, ensuring that it is only accessible by authorized parties. The decentralized architecture of the system will ensure that there is no central point of failure and that customer data is protected against unauthorized access and hacking attempts. This system will be designed to be user-friendly, allowing for efficient and seamless verification processes for both customers and organizations. The use of blockchain technology will provide a tamper-proof and auditable record of all KYC verification transactions, improving the overall security and trust in the system.

Index Terms **- KYC, Blockchain, Decentralize, Smart Contract, Ethereum**

1. INTRODUCTION

Banks gather details on the customers' names and addresses through a process known as KYC. Due diligence is a process that regulators oversee for confirming clients' identities. By following this procedure, banks' services are less likely to be abused. When opening new accounts, banks are in charge of completing the KYC process. The KYC information of banks' clients must also be updated on a regular basis. KYC may be laborious, tedious, and redundant between institutions. Financial institutions might achieve better compliance outcomes, boost productivity, and enhance customer experience by sharing KYC information on Blockchain.

The use of blockchain technology in KYC verification can provide several benefits. For example, it can increase the efficiency and security of the verification process by reducing the risk of fraud and data breaches. Additionally, since data is stored on a decentralized network, it is more difficult for unauthorized parties to access or alter the information. Another benefit of blockchain- based KYC verification is that it allows customers to have more control over their personal information. Customers can choose which information to share with different parties and can also revoke access to their information at any time.

Blockchain-based KYC (Know Your Customer) verification is a process of using blockchain technology to verify the identity of customers in a secure and decentralized manner. In this process, customer information is stored on a blockchain network, which is a digital ledger that is decentralized and distributed across a network of computers. This information can be accessed by aut horized parties, such as financial institutions, for verification purposes.

Overall, blockchain-based KYC verification is a promising new approach to identity verification that can enhance security, efficiency and customer empowerment.

2. APPLICATION OF KYC VERIFICATION SYSTEM

The application of a KYC verification system based on blockchain technology can be wide-ranging, including but not limited to the following industries:

- **Banking and finance:** To meet regulatory requirements and prevent money laundering and other financial crimes.
- **Cryptocurrency exchanges:** To comply with anti-money laundering (AML) and countering the financing of terrorism (CFT) regulations.
- **Healthcare:** To securely manage and store patients' personal and medical information.
- **Government services:** To securely manage and verify the identity of citizens for various services, such as passport issuance, voting, and tax filing.

- **Telecommunications:** To verify the identity of customers before providing services like mobile phone plans or internetaccess.

In all of these industries, the implementation of a KYC verification system based on blockchain can help improve security, increase efficiency, and reduce the risk of fraud and data breaches.

3. BLOCKCHAIN KYC VERIFICATION SYSTEM TECHNOLOGY IN BANKING SECTOR

In blockchain-based KYC verification systems used in the banking sector, various technologies can be employed, including:

3.1 Distributed Ledger Technology (DLT)

A type of technology called distributed ledger technology (DLT) makes it possible to store and transmit data and assets in a way that is secure, open, and decentralized. In the banking sector, DLT has the potential to revolutionize the way financial transactions are performed by providing a single source of truth for all parties involved, Consequently, there will be less need for middlemen, and financial transactions will be more secure and efficient.

One example of DLT in the banking sector is blockchain technology, which is a type of DLT that is often used in the creation of digital currencies like Bitcoin. In the banking sector, blockchain can be used to record and verify transactions, store customer information, and track the flow of funds between different financial institutions. Another example of DLT in the banking sector is distributed database technology, which is used to store and manage customer information and transaction data. This technology allows multiple institutions to have access to a shared database, allowing them to securely and transparently share information and collabo rate on financial transactions.

3.2 Smart Contracts

Smart contracts can automate the KYC verifying procedure, making sure the procedure is effective and secure. They can also enforce compliance with regulations, such as anti-money laundering (AML) and countering the financing of terrorism (CFT). The conditions of an agreement are immediately encoded into lines of code in a smart contract, which self-executes. When specific requirements are met, it is a computer software that automatically carries out a contract's provisions. A decentralized network of computers that validate transactions and uphold the terms of the contract maintains the blockchain network where the code and the agreements it contains are stored.

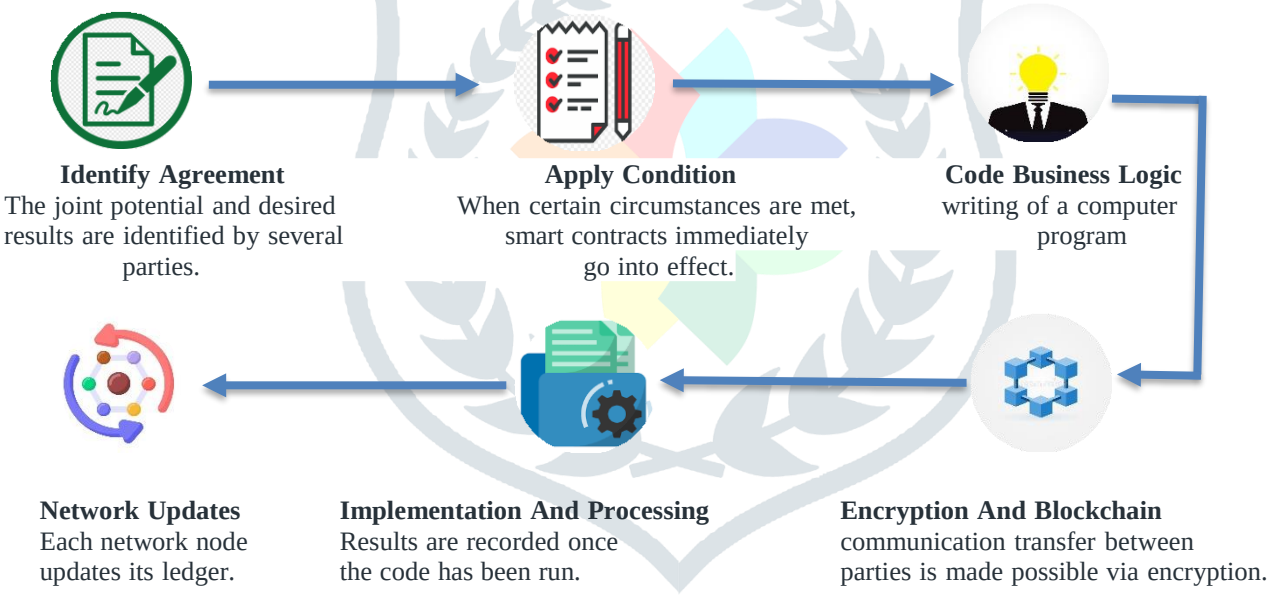

fig 3.2 architecture of smart contract

Smart contracts can automate the KYC verifying procedure, making sure the procedure is effective and secure. They can also enforce compliance with regulations, such as anti-money laundering (AML) and countering the financing of terrorism (CFT).

The conditions of an agreement are immediately encoded into lines of code in a smart contract, which self-executes. When specific requirements are met, it is a computer software that automatically carries out a contract's provisions. A decentralized network of computers that validate transactions and uphold the terms of the contract maintains the blockchain network where the code and the agreements it contains are stored.

One of the main benefits of using smart contracts is that they reduce the need for intermediaries and increase the security of transactions. This is because smart contracts are stored on a decentralized network, making them resistant to tampering, hack ing, and other forms of interference.

The execution of a smart contract is triggered by an event or a set of conditions being met. For example, a smart contract for the purchase of a house could be set up to automatically transfer ownership from the seller to the buyer when the buyer sends the agreed-upon amount of cryptocurrency to the contract's address. Smart contracts also facilitate the execution of complex financial transactions, such as derivatives and bonds, without the need for intermediaries like banks. This can lead to lower transacti on costs and faster settlement times. Another important aspect of smart contracts is their transparency. All parties involved in a transaction

can view the terms of the contract and the code that executes it, making it easier to verify that the terms are being followe d and the contract is being executed as intended.

3.3 Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a critical component of a Blockchain-based KYC (Know Your Customer) verification system. In a PKI, two keys are used for encryption and decryption of messages: a public key, which is used to encrypt the messages, and a private key, which is used to decrypt the messages. Digital certificates are issued, revoked, and distributed through a PKI system.

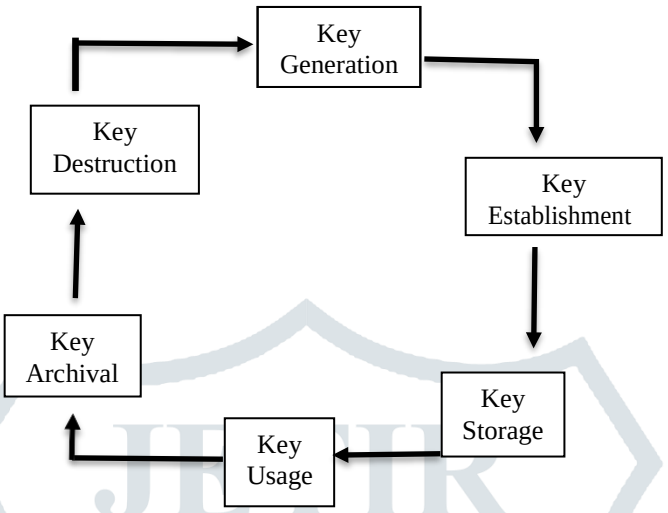

Fig 3.3 PKI Architecture

In the context of a Blockchain-based KYC verification system, PKI can be used to verify the identity of users in a secure and decentralized manner. When a user wants to get verified, they can provide their personal information, which is encrypted using their public key. The encrypted information is then stored on the Blockchain, making it tamper-proof and immutable. The verifier can then use the user's public key to verify the authenticity of the information. The verifier can also access the information st ored on the Blockchain to verify the user's identity. This ensures that the information provided by the user is secure and cannot be tampered with.

In summary, PKI provides a secure and decentralized way to verify the identity of users in a Blockchain-based KYC verification system. By using public and private keys for encryption and decryption, PKI helps to ensure the security and privacy of user information, making it an essential component of a robust KYC verification system.

3.4. Biometric authentication

Biometric authentication, such as facial recognition or fingerprint scanning, can be used to verify the identity of customers, making the process more secure and user-friendly. The technology used in blockchain-based KYC verification systems in the banking sector can vary depending on the specific requirements of the system and the needs of the organization. However, a combination of DLT, smart contracts, cryptography, biometric authentication, and AI/ML technologies can be used to create a secure and efficient system.

4. RESEARCH METHODOLOGY

The potential effects of adopting blockchain to store and track records on the current banking business, specifically the KYC document verification procedure. The KYC procedures used in banks today are very reliable, even when conducted on paper, which is an old procedure. The KYC process in the proposed system uses blockchain, which removes the need for middlemen. As a consequence, maximise productivity, cut expenses, enhance customer satisfaction, and maximise transparency throughout the integration of customer records into the bank database.[1]

The current “Know Your Customer” procedure is inconvenient and inefficient for both banks and customers. The procedure adds to running costs and is unneeded. Additionally, it provides users with scant to no privacy protection. In this paper, a blockchain-based approach is suggested. Verifying KYC documents for various financial sectors is a laborious and unsafe process because documents are maintained by a centralised organisation. The suggested KYC system is a decentralised, Blockchain-based system that may be used to establish a person's evidence of identification. The data saved on the decentralised application adds an extra layer of protection, and it is also a cost-effective way. [2]

Tushara Sasi et al. [3] explained where did the KYC came from, how it is working in the existing system. The Reserve Bank of India introduced the "Know Your Customer" (KYC) requirement as a mechanism for organisations to confirm and thereafter confirm the legitimacy of customers. They must provide their KYC documents, which serve as proof of their identity and residence, prior to investing in a variety of financial instruments. Know Your Customer (KYC) procedures are currently a significant but unimportant concern in the financial industry. Customers often find the process cumbersome because they must go through the identical steps no matter which bank or financial institution they choose to work with. It takes different amounts of time depending on how each person applies the technique, so a

quicker option is required. This paper seeks to address this problem with a solution. We propose a blockchain-based system that only needs to execute one KYC verification and maintain one safe database, doing away with the need for multiple KYC checks. The user's KYC information will only be accessible with the user's consent to the various financial institutions participating on the blockchain network. In fact, we even do away with third-party intervention because the user has ownership over the data. The user has the option of approving or declining the bank's request to examine their KYC data. By exchanging KYC data on Blockchain, financial institutions will be able to improve compliance outcomes, increase efficiency, and improve customer experience.

Blockchain help to secure our data. Data on the internet is not secure, as we have already heard from experts and scientists, and anyone with decent hacking abilities can simply into your system. But that's no longer the case, thanks to the recently developed blockchain technology, which has made it possible to protect the privacy and security of our data. Blockchain technology will be widely used by organisations in the near future to conduct financial transactions and protect sensitive data. In this article, we outline a blockchain-based system that financial institutions can utilise to verify KYC documents. Also covered in this essay are some of the key components of using blockchain. [4]

The bank is doing KYC and the blockchain based verification system of the bank can do it. All banks rely heavily on the Know Your Customer (KYC) process to confirm the identification of their clients. KYC verification is essential to stop criminal elements from using banks for money laundering schemes like drug trafficking, terrorism, and other crimes. Currently, the widely used manual KYC method is out-of-date, time-consuming, and less safe. By implementing Blockchain-based KYC verification, these restrictions may be removed due to Blockchain's decentralization, immutability, and security properties. In this paper, we suggest an Ethereum Blockchain-based decentralized KYC verification mechanism. It would enable all of the banks connected to the Blockchain network to confirm and approve the accuracy of the information a customer has submitted. Depending on the number of votes, the blockchain stores the customer's KYC status. A significant improvement in our suggested approach is that banks can vote for other banks to be removed from the network if they are fiddling with KYC data. With its unique qualities, Blockchain can be utilized in this way to increase the effectiveness of the KYC process. [5]

Prof Maind A.L et al. [6] developed a blockchain-based strategy that permits one-time KYC for users and gets rid of middlemen. Users can access the data whenever they want, from anywhere, and for a variety of reasons. Blockchain technology's security is boosted by its decentralised ecosystem, user transparency, and absence of outside interference. Furthermore, quicker processing is promised.

In banks, hospitals, and other establishments, KYC (Know Your Customer) is used to confirm an individual's identification. The current state of affairs calls for a multi-location, independent third-party KYC system that may be used to verify an individual's identification. Blockchain technology underpins the decentralized KYC method that is being suggested. An individual's proof of identification may be established using the proposed approach. To ensure that the data recorded in the system remains impenetrable, the distributed ledger's immutability feature is essential. Comparable in functionality to the previous KYC system is the proposed system. Data is kept in a distributed database to provide data backup, replication, and lack of a single point of failure. The suggested system's totally decentralized architecture makes sure that it is not dependent on a centralized client-server architecture. There is no engagement of a third party to build confidence among the stakeholders. Regarding the amount of gas required to write a transaction to the blockchain, the suggested solution is inexpensive. To provide another level of security, the data stored in the decentralized database is encrypted. Since the data is encrypted, there is still no risk even if the decentralized database's data is compromised. [7]

This paper suggested activity used blockchain technology to enhance the current KYC system. A well-known DLT aspect is the elimination of third parties, and our logic for data mobility is built using smart contracts. To make transactions via a risky channel more secure, blockchain technology employs a number of cryptographic security mechanisms. The proposed KYC procedure might improve data storing, updating, sharing, and accessing operations while also boosting security, transparency, and privacy by applying DLT, cryptography, and the blockchain consensus mechanism. It also raises customer loyalty and improves customer happiness.[8]

A Blockchain-based fix to the traditional KYC verification process' high cost. The primary distinction is that, regardless of how many institutions a user registers, the entire verification process is only carried out once for each user, boosting transparency by safely communicating the results via DLT. This strategy makes use of Ethereum for proof of concept (POC). This process lowers costs, enhances client satisfaction, and fosters greater openness.[9]

Al Mamun et al. [10] approached an IPFS-based blockchain to Customers can use the suggested method to open an account at a single financial institution, complete their KYC there, and then use the IPFS network to generate a hash value and a unique decryption key that can be shared over blockchain. Customers can retrieve and securely save their personal information over the IPFS network in order to open a new account at any bank or financial institution. Before being sent via the IPFS network, the file is compressed and encrypted for added protection. Access to the contents requires knowledge of the hash values used by the IPFS network. The Cleopatra platform makes use of Gpg4win encryption software so that users can view encrypted KYC papers.

Know your customer, also referred to as know your client or just KYC, is the procedure that companies and financial institutions must use to identify their clients and assess any kind of risk that could arise from unethical motives and deceit for the commercial connection in accordance with a national regulatory agency. The word "KYC" is frequently used to refer to the anti-money laundering regulations and bank regulations that are in place to control such operations. Companies of all sizes are required to use KYC to ensure that their consultants, agents, or distributors abide by the regulations set by anti-bribery comply owing to bribery and other unethical behavior. With an estimated 1.3 billion people living in India, there is a huge demand for a secure and quick mechanism for exchanging sensitive information like KYC documents, which may contain personal documents. Although the idea of implementing such a system is not new, the current solutions have shortcomings. The functionality of the current KYC system will be duplicated by the proposed system. A tamper-proof system can be created by utilizing the immutable property of Distributed Ledger Technology (DLT) and Inter Planetary File System (IPFS). In order to create a more complete and safe system, this article proposes the installation of cutting-edge features to remedy some of the system's flaws.[11]

4.1 Review On Existing Application

Many new tactics and applications have been developed and a lot of study is being done to lower risk and reduce physical paperwork'sof KYC Verification System. The literature provides detailed descripting of such system and strategies.

The current KYC (Know Your Customer) verification system typically involves collecting personal information from an individual, such as their name, address, and government-issued ID, and then verifying that information against external sources. This is done to ensure that the individual is who they claim to be and to detect any potential fraudulent activity. The process can be done digitally or in-person and can include various forms of identification such as passport, ID card, Driver's license, and others.

One of the main criticisms of the current system is that it can be time-consuming and burdensome for individuals to provide all the necessary information. Additionally, there are privacy concerns as personal information is often collected and stored by companies.

Another issue with the current system is that it can be costly for companies to implement and maintain. There is also a risk that the information provided may not be accurate or up-to-date, which can lead to false positives or false negatives in the verification process.

Overall, the current KYC verification system aims to balance the need for security and fraud prevention with the need to protect individuals' privacy and minimize inconvenience. Some companies are starting to implement more advanced technologies such as biometrics and blockchain-based solutions to improve the process, but the current system is still widely used in most of the industry.

5. PROBLEM STATEMENT

One of the main problems with the current KYC verification system is that personal information is often collected and stored by multiple companies, increasing the risk of data breaches and identity theft. Additionally, the process can be time-consuming and burdensome for individuals, and it can be costly for companies to implement and maintain.

A blockchain-based KYC verification system aims to address these issues by creating a decentralized and secure platform for storing and verifying personal information. In this system, individuals would have control over their own personal information and could choose to share it with companies only when necessary. This could potentially reduce the risk of data breaches and identity theft, as well as the inconvenience and cost associated with the traditional KYC verification process.

However, there are also some challenges with implementing a blockchain-based KYC verification system. One of the main challenges is ensuring the accuracy and integrity of the personal information stored on the blockchain. This can be difficult to guarantee, as individuals may be able to provide false information or tamper with their own records. Additionally, there may be regulatory and compliance issuesto be addressed, as governments and financial institutions may have specific requirements for the verification and storage of personal information.

Overall, while a blockchain-based KYC verification system has the potential to improve the current system, it also poses some challenges that need to be addressed before it can be implemented on a large scale.

6. PROPOSED METHODOLOGY

Blockchain technology can be utilized to provide a secure, transparent and decentralized Know Your Customer (KYC) verification system.

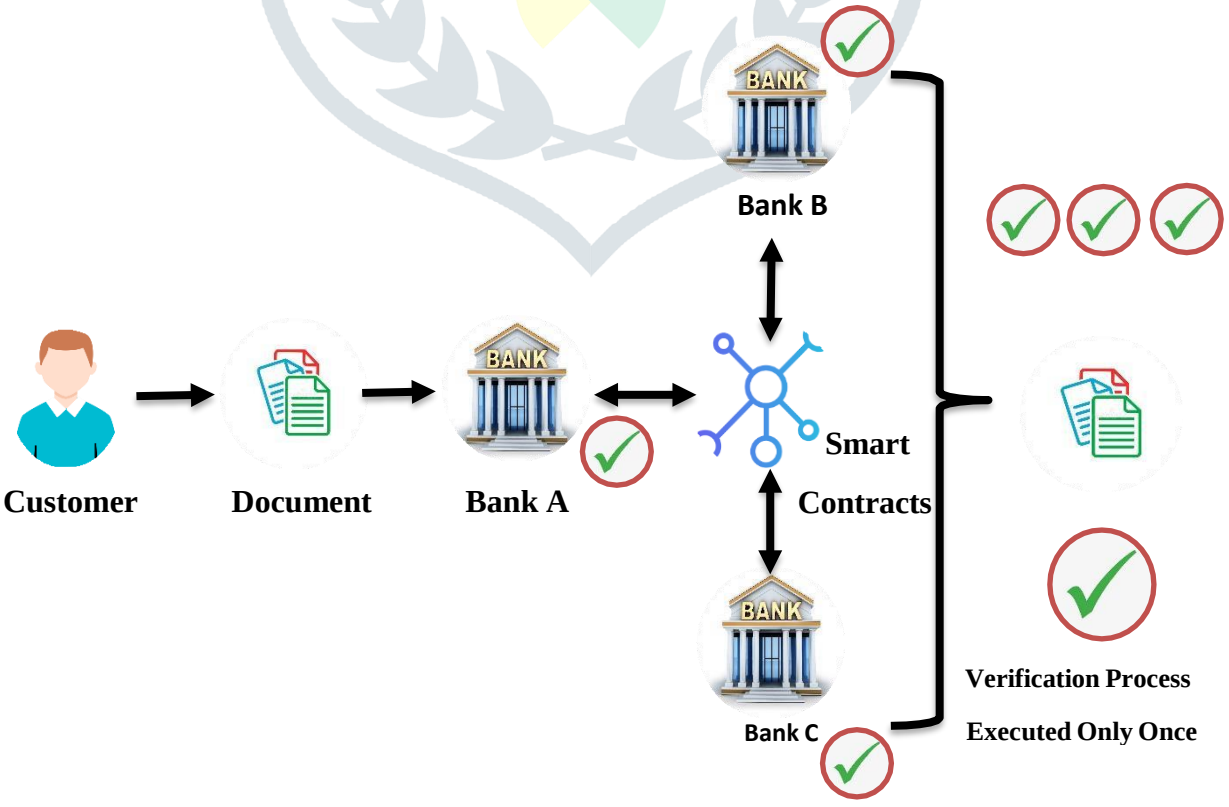

Fig. 7 process of using blockchain for KYC verification

A proposed methodology for a blockchain-based KYC (Know Your Customer) verification system in the banking sector could involve the following steps:

6.1 Customer on-boarding

Customer on-boarding in a blockchain-based KYC verification system in the banking sector refers to the process of collecting and storing a customer's personal information on the blockchain network. This process is initiated when a new customer opens an account with a bank or wants to avail of a financial service. During the customer on-boarding process, the Customer must submit personal data, including name, address, birthdate, government-issued ID, and other pertinent data. This information is then encrypted and stored on the blockchain network, creating a secure digital identity for the customer.

The customer's encrypted information is accessible only to authorized parties, such as the bank, with the customer's consent. The use of blockchain technology ensures that the customer's information is stored in a decentralized and tamper-proof manner, making it more secure compared to traditional methods of data storage. The customer on-boarding process is an essential step in the overall KYC verification process, as it forms the foundation for the rest of the verification process, including identity verification and KYC checks.

6.2 Identity verification

Identity verification in blockchain-based KYC (Know Your Customer) systems in the banking sector refers to the process of verifying the identity of a customer using blockchain technology. The aim is to establish the customer's identity and determine if they are who they claim to be. This is usually done to comply with regulatory requirements, such as anti-money laundering (AML) and counter-terrorism financing (CTF) laws. In a blockchain-based KYC verification system, the customer's personal information is encrypted and stored on a secure and decentralized blockchain network. This information can be securely accessed and verified by authorized parties, such as banks, without compromising the customer's privacy. The advantages of using blockchain technology in identity verification include improved security and transparency, as well as reduced costs and increased efficiency. The decentralized nature of the blockchain network ensures that data cannot be altered or deleted, and that the customer's identity information is secure and tamper-proof. This makes it an attractive option for banks and other financial institutions looking to comply with KYC requirements in a cost-effective and efficient manner.

6.3 KYC checks

KYC (Know Your Customer) checks are a key component of identity verification in a blockchain-based KYC verification system in the banking sector. These checks are designed to ensure that the customer's identity information is accurate and up-to-date, and that they are who they claim to be. The KYC checks in a blockchain-based KYC system typically involve the following steps:

- **Collection of personal information:** The customer provides personal information, such as their name, date of birth, address, and government-issued ID. This information is encrypted and stored on the blockchain network.
- **Identity verification:** The customer's identity information is verified using various methods, such as document verification, biometric authentication, or social media verification.
- **Risk assessment:** The customer's identity information and other relevant data is analyzed to determine any potential risk associated with the customer. This helps to ensure that the customer is not involved in any illegal or fraudulent activities.
- **Monitoring and updating:** The customer's identity information is continuously monitored and updated to ensure that it remains accurate and up-to-date.

These KYC checks are important for ensuring that the customer's identity information is secure and accurate, and that they are who they claim to be. They also help to prevent fraud, money laundering, and other financial crimes, making blockchain-based KYC systems an attractive option for banks and other financial institutions looking to comply with KYC requirements.

6.4 Smart Contract

Smart contract in a blockchain-based KYC (Know Your Customer) verification system in the banking sector refers to a self-executing contract with the agreement's terms are enshrined explicitly in lines of code. It is automatically carried out when a set of specified circumstances are satisfied and is kept on a decentralized blockchain network.

In a KYC verification system, a smart contract can be used to automate the process of identity verification and management. The contract can be programmed to automatically verify the customer's identity information, assess risk, and update the customer's information as needed.

Smart contracts can help to increase the efficiency and security of the KYC process by eliminating the need for manual intervention and reducing the risk of errors or fraud. They also ensure that the customer's identity information is securely stored and can only be accessed by authorized parties, such as banks and financial institutions. By using smart contracts, banks and other financial institutions can streamline their KYC processes and ensure compliance with regulatory requirements in a secure and efficient manner. This can help to reduce costs, improve customer experience, and enhance the overall security of the financial system.

6.5 Sharing of verified information

Sharing of verified information in a blockchain-based KYC (Know Your Customer) verification system in the banking sector refers to the process of sharing the verified identity information of a customer between authorized parties. This information is encrypted and stored on a secure and decentralized blockchain network, making it possible to share the information with authorized parties in a secure and efficient manner. The sharing of verified information in a KYC verification system can help to increase efficiency and reduce costs by eliminating the need for multiple identity verification processes for the same customer. For example, if a customer opens a new bank account, their verified identity information can be shared with the new bank, saving the customer the time and effort of having to provide

the same information multiple times.

Sharing verified information in a blockchain-based KYC system can also help to reduce the risk of fraud and improve the overall security of the financial system. The decentralized nature of the blockchain network ensures that the customer's identity information is secure and cannot be altered or deleted, making it an attractive option for banks and other financial institutions looking to comply with KYC requirements in a secure and efficient manner.

However, it is important to ensure that the sharing of verified information is done in a way that complies with data protection laws and regulations, and that only authorized parties have access to the information.

6.6 Continuous monitoring

Continuous monitoring in a blockchain-based KYC (Know Your Customer) verification system in the banking sector refers to the ongoing process of monitoring the customer's identity information to ensure that it remains accurate and up-to-date. This is done to reduce the risk of fraud and ensure that the customer is who they claim to be. In a blockchain-based KYC system, the customer's identity information is stored on a secure and decentralized blockchain network. This information is continuously monitored and updated to ensure that it remains accurate and up-to-date. For example, if the customer's address changes, the information can be updated on the blockchain network to reflect this change.

Continuous monitoring helps to ensure that the customer's identity information is secure and accurate, and that they are who they claim to be. It also helps to reduce the risk of fraud, money laundering, and other financial crimes. The use of blockchain technology in continuous monitoring makes it possible to securely store and update the customer's identity information in real-time. This can help to improve the overall security of the financial system and ensure compliance with regulatory requirements, such as anti-money laundering (AML) and counter-terrorism financing (CTF) laws.

Overall, continuous monitoring is an important aspect of identity verification in a blockchain-based KYC system and helps to ensure that the customer's identity information remains secure and accurate over time.

6.8 Updating information

Updating information in a blockchain-based KYC (Know Your Customer) verification system in the banking sector refers to the process of updating the customer's identity information on the blockchain network to ensure that it remains accurate and up-to-date. In a blockchain-based KYC system, the customer's identity information is securely stored on a decentralized blockchain network, making it possible to update the information in real-time. The process of updating the information can be automated using smart contracts, which can be programmed to automatically verify the accuracy of the information and update it as needed.

For example, if the customer's address changes, the information can be updated on the blockchain network to reflect this change. The updated information is then immediately available to all authorized parties, such as banks and other financial institutions.

Updating information in a blockchain-based KYC system helps to reduce the risk of fraud and ensure that the customer is who they claim to be. It also helps to ensure that the customer's identity information remains accurate and up-to-date, making it easier for banks and other financial institutions to comply with regulatory requirements, such as anti-money laundering (AML) and counter-terrorism financing (CTF) laws.

Overall, updating information is an important aspect of identity verification in a blockchain-based KYC system and helps to ensure that the customer's identity information remains secure and accurate over time. This methodology provides a secure and efficient way for banks to perform KYC checks, while ensuring the privacy and security of the customer’s information.

7. IMPLEMENTATION

The implementation of a blockchain-based KYC verification system in the banking sector involves several steps:

- **Requirements gathering:** This involves defining the goals and requirements of the KYC system, as well as the types of data that need to be collected and verified.
- **Platform selection:** The next step is to choose a blockchain platform that meets the requirements of the bank, such as security, scalability, and interoperability.
- **Data integration:** This involves integrating the bank's existing systems and databases with the blockchain platform, so that customer information can be securely stored and verified.
- **Development of smart contracts:** Smart contracts are self-executing scripts that automate the KYC verification process on the blockchain. They can be used to verify customer information, manage access to customer data, and enforce compliance with regulations.
- **Deployment and testing:** When the blockchain-based KYC system has been developed to its full potential, it needs to be deployed and tested to ensure that it meets the requirements and is functioning as expected.
- **User training:** Finally, the bank's employees need to be trained on the use of the new system, and the bank's customers need to be informed of the benefits of using a blockchain-based KYC system.

The implementation of a blockchain-based KYC verification system can be a complex and time-consuming process, but it offers significant benefits in terms of security, efficiency, and customer experience.

8. ADVANTAGES

- **Increased security:** The decentralized and encrypted nature of blockchain technology makes it more secure than traditional KYC verification methods, reducing the risk of data breaches and fraud.
- **Improved efficiency:** Blockchain-based KYC eliminates the need for manual data entry and reduces the time and resources required to complete KYC verification.
- **Enhanced transparency:** Blockchain provides a tamper-proof and transparent record of KYC information, enabling easy access and sharing of customer information between different banks and financial institutions.
- **Better customer experience:** With a blockchain-based KYC system, customers only need to undergo the KYC process once, and the verified information can be securely and easily shared between institutions.
- **Cost savings:** By automating the KYC process and reducing the need for manual intervention, blockchain-based KYC can result in significant cost savings for banks and financial institutions.

9. DISVANTAGES

- **Technical barriers:** Implementing a blockchain-based KYC system requires a significant amount of technical expertise, as well as investment in infrastructure and technology.
- **Limited adoption:** The implementing of blockchain technology in the banking sector is still in its early stages, and many banks may be reluctant to adopt it due to lack of familiarity and understanding.
- **Interoperability issues:** There may be compatibility issues between different blockchain platforms, which can make it difficult to share customer information between institutions.
- **Regulation:** The regulatory environment surrounding the use of blockchain technology in finance is still evolving, and there may be legal and compliance challenges that need to be addressed.
- **Data privacy:** Despite the security benefits of blockchain, there are still concerns about data privacy, especially when it comes to sensitive customer information. It's important for blockchain-based KYC systems to be designed with strong privacy protections inplace.

10. CONCLUSION

Implementing blockchain technology for Know Your Customer (KYC) verification in the banking sector has the potential to revolutionize the way banks perform identity verification and compliance. With blockchain, the process of KYC verification becomes secure, efficient, and cost-effective. The decentralized database where customer data is kept renders it unchangeable and impenetrable. This lowers the possibility of financial fraud and identity steal. Additionally, with blockchain, customers only need to undergo KYC verification once, as their information can be shared with all banks in the network, saving time and effort for both the customer and the bank. In today's fast-paced world, where customers demand instant gratification, incorporating blockchain into the KYC process is a step in the right direction for the banking sector.

REFERENCES

[1] Rankhambe, B. P., & Khanuja, H. K. (2021). Hassle-Free and Secure e-KYC System Using Distributed Ledger Technology. *International Journal of Next-Generation Computing*, *12*(2).

[2] V. N. Sunitha, Ashwini P., S., Bhat S., (2022) KYC Verification Using Blockchain *International Journal for Research in Applied Science & Engineering Technology (IJRASET),* ISSN: 2321-9653; DOI: https://www.ijraset.com/best-journal/kyc-verification-using-blockchain

[3] Sasi T., V. N. Sunitha, Bhat S., N. H. Sandhya, Ashwini P., (2022) KYC Verification Using Blockchain. *International Research Journal of Engineering and Technology (IRJET),* e-ISSN: 2395-0056 p-ISSN: 2395- 0072.

[4] Prof. Kazi A., Salgaonkar S., Parab S., Tamhanekar (2022) KYC Verification Using Blockchain. *International Journal ofcreative Research Thought (IJCRT),* ISSN: 2320-2882.

[5] Patil, P., & Sangeetha, M. (2022). Blockchain-based Decentralized KYC Verification Framework for Banks. *Procedia Computer Science*, *215*, 529-536.

[6] Maind L. A., Gedam V. P., Chavan K. S., Shinde D. C., (2020) KYC USING BLOCKCHAIN. *International Journal for Research in Engineering Application & Management (IJREAM), ISSN: 2454-9150.*

[7] Sinha, P., & Kaul, A. (2018). Decentralized KYC system. *International Research Journal of Engineering and Technology(IRJET)*, *5*(8), 1209-1210.

[8] Yadav, A. K., & Bajpai, R. K. (2020). KYC optimization using blockchain smart contract technology. *Int J Innov Res Appl Sci Eng (IJIRASE)*, *4*(3), 669-674.

[9] Reddy, Suhag, S., (2020). Know Your Customer (KYC) Process through Blockchain. *International Reasearch Journal of Engineering and Technology (IRJET) , p-ISSN:2395-0072, e-ISSN: 2395-0056*

[10] Al Mamun, A., Hasan, S. R., Bhuiyan, M. S., Kaiser, M. S., & Yousuf, M. A. (2020, June). Secure and transparent KYC for banking system using IPFS and blockchain technology. In *2020 IEEE region 10 symposium (TENSYMP)* (pp. 348-351).

IEEE.

[11] Singhal, N., Sharma, M. K., Samant, S. S., Goswami, P., & Reddy, Y. A. (2020). Smart KYC using blockchain and IPFS. *Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies*, 77-84.