Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 46 No. 2 (2025)

Decentralised Know Your Customer (KYC) System Using Fetch.ai uAgents

[1]Dev Chauhan, [2]Punit Mittal, [3]Aryan Gupta, [4]Deepshikha Panwar

[1]Department of Computer Science & Information Technology, Meerut Institute of Engineering & Technology, Meerut, UP, India

[2]Department of Computer Science & Information Technology, Meerut Institute of Engineering & Technology, Meerut, UP, India

[3]Department of Computer Science & Information Technology, Meerut Institute of Engineering & Technology, Meerut, UP, India

[4]Department of Computer Science & Information Technology, Meerut Institute of Engineering & Technology, Meerut, UP, India

Abstract:- The standard Know Your Customer (KYC) procedures employed by banks are widely regarded as inefficient, costly, and prone to errors, leading to delays and dissatisfaction among customers. These challenges underscore the need for transformative technology to improve operational viability while ensuring compliance with stringent regulatory requirements. This study delves into how Fetch.ai's blockchain infrastructure and uAgent technology can revolutionize the KYC process by facilitating secure, decentralized data storage, real-time monitoring, and seamless data verification. By leveraging Fetch.ai's decentralized ledger and autonomous agents (uAgents), financial institutions can significantly reduce intermediary dependence, lower operational costs, and minimize human errors associated with manual data management. This innovative approach enhances scalability, privacy, and data security, while providing a robust framework to counter fraudulent activities in the banking sector. Additionally, the integration of Fetch.ai's ecosystem promotes a customer-centric KYC experience, fostering greater trust and transparency in financial transactions. The study demonstrates the potential for blockchain-driven KYC to streamline operations, optimize resource utilization, and redefine the standards of regulatory compliance in the modern banking industry.

Index Terms: Fetch.ai, blockchain, decentralisation, KYC, uAgents, distributed ledger technology, verification.

1. INTRODUCTION

This research delves into modernising the KYC process by examining centralised versus decentralised KYC systems and leveraging Fetch.ai's AI-driven, blockchain-based technology. Centralised systems, while traditional, often suffer from inefficiencies and security risks due to reliance on intermediaries and centralised data storage. In contrast, decentralised KYC, powered by Fetch.ai's autonomous agents (uAgents), offers a more secure, private, and efficient alternative, where verified data can be shared seamlessly across institutions.

The study also explores AI's role in enhancing decentralised KYC, focusing on real-time verification, data accuracy, and operational cost reduction. By integrating AI with Fetch.ai's autonomous agents, decentralised KYC provides a robust, adaptive, and scalable solution that addresses regulatory compliance and operational challenges across banking and financial services. This research ultimately aims to establish a comprehensive, resilient model for KYC, emphasising security, privacy, and efficiency through Fetch.ai's innovative technology.

Both individual experts and business experts believe that blockchain [1] holds great promise for many challenges faced by the banking sector. The device works as a decentralised database, which suggests a decentralised structure. More importantly, information is stored in a network of interconnected nodes, reducing the possibility of tampering with information. Blockchain technology brings many benefits to the banking sector, including the transfer of KYC information and the provision of accurate customer information [2]. Conduct a comprehensive review of the business and contribute to the advancement of knowledge on KYC certification. Provides valuable

information that can contribute to future improvements in the KYC process.

The main findings of this study highlight several novel contributions compared to previous research:

- T**horough Examination:** This investigation offers a comprehensive review of diverse KYC approaches adopted in the banking domain, exploring their specific attributes, benefits, and challenges.
- **Performance Evaluation:** Through indicator-based assessments, the research evaluates current KYC systems, identifying key performance areas, limitations, and areas for improvement.

By highlighting these gaps, the study offers insights into enhancing the efficiency, accuracy, and scalability of KYC practices, with implications for future research and development in decentralised KYC solutions.

In recent years, many meaningful and focused research articles have been published in the field of blockchain KYC. One article presents a case study focusing on blockchain and autonomous multi-agent electronic KYC systems in financial services [3]. This article explores the intersection of blockchain and electronic KYC by reviewing various research findings and implementation methods. The authors evaluate the effectiveness of Fetch.ai's autonomous agent system in terms of communication, technology stack, etc. Given the rapid adoption of blockchain technology in the banking sector, this article focuses on recommendations for future development of electronic KYC processes with blockchain technology using the PRISMA model.

Moreover, many scams as a result of the KYC system failure have been recorded over the past few decades. Examples include:

HSBC Money Laundering Scandal [4]

HSBC, one of the world's largest banks, faced allegations of facilitating money laundering for drug cartels and terrorist organisations. The scandal unfolded in the early 2010s and drew widespread attention due to the scale of illicit activities involved. Investigations revealed that HSBC's KYC processes were inadequate in detecting and preventing suspicious transactions. The bank failed to implement proper controls to monitor high-risk accounts and identify illicit activities. As a result, billions of dollars were laundered through HSBC accounts, with minimal oversight from the bank.HSBC faced significant regulatory fines and legal repercussions, including a record $1.9 billion settlement with U.S. authorities in 2012. The scandal tarnished the bank's reputation and led to changes in compliance practices. Additionally, several top executives resigned from their positions amidst public outcry and regulatory scrutiny.

CBA Money Laundering Scandal [5]

Commonwealth Bank of Australia (CBA), Australia's largest bank, faced allegations of widespread breaches of anti-money laundering laws. The scandal emerged in the late 2010s and shocked the Australian financial industry. The bank's KYC processes were criticised for failing to adequately monitor and report suspicious transactions. In particular, large cash deposits made through its intelligent deposit machines (IDMs) went unnoticed by the bank's compliance systems, allowing illicit funds to flow through CBA accounts unchecked. CBA agreed to pay a record $700 million fine in 2018 to settle the case with Australian authorities. The scandal resulted in executive resignations, regulatory scrutiny, and a loss of customer trust. The bank also faced ongoing legal challenges and had to implement significant reforms to strengthen its compliance controls and rebuild its reputation.

Deutsche Bank Money Laundering Scandal [6]

Deutsche Bank, Germany's largest bank, has faced multiple investigations and fines related to money laundering allegations. The scandals have rocked the bank's reputation and raised serious questions about its compliance practices. Investigations revealed deficiencies in Deutsche Bank's KYC processes, including inadequate customer due diligence and monitoring of high-risk accounts. The bank's lax controls allowed illicit funds to flow through its accounts, including money laundering for Russian clients and violating international sanctions. The bank has paid billions of dollars in fines to settle various cases, including allegations of laundering money for Russian clients and violating sanctions. The scandals have damaged Deutsche Bank's reputation and raised questions about its compliance controls. Several top executives have resigned, and the bank has faced increased regulatory scrutiny and legal challenges as a result. Some research papers highlight the importance of blockchain technology, especially in the banking sector. It contributes to its significance in the financial market by showing the critical

role of blockchain in Bitcoin and cryptocurrencies. The paper introduces blockchain as a reliable framework for data exchange, removing the dependency on intermediaries.

It categorizes blockchain into three types: public, private, and corporate (government), and explores various applications within the banking sector, such as KYC processes, settlement of transactions, financial dealings, digital payments, smart contracts, and collaborative loans. The main objective of this research is to reveal the benefits and impacts of blockchain technology adoption in banking.

For example, one review did not provide a comprehensive assessment of e- KYC solutions that would allow for comparison and understanding of blockchain's effectiveness, nor did it provide performance metrics for blockchain-based e-KYC systems.

Similarly, other reviews would benefit from a more comprehensive examination of the research as a framework for understanding its validity. In addition, one survey failed to address specific issues and limitations of using blockchain-based KYC systems, while another survey lacked understanding of issues and topics related to governance, collaboration, capacity building, and data analysis. Search and examine. The framework- based research was also divided into storage methods and encryption methods. The findings suggest that nonprofits will not benefit significantly from full KYC management, while academic and nonprofit organisations will view the system that way.

Another article provides a data-driven analysis focusing on the evolving landscape of blockchain technology in the financial domain. It emphasizes blockchain's capability to deliver a strategic edge and elaborates on various dimensions of its implementation in the financial industry, including its advantages and limitations. However, this review does not delve deeply into blockchain's applications in areas such as electronic KYC, data protection, and legal frameworks.

TABLE 1 : COMPARATIVE OVERVIEW OF DIFFERENT CURRENT WORKINGS

Papers / Studies	**Objectives**	**Platform / Technology proposed**	**Limitations**
Blockchain for KYC verification [8]	Enhancing kyc processes by improving security and efficiency using blockchain	Ethereum	Limited focus on regulatory compliance and integration challenges with existing systems
eKYC Solutions using AI [9]	Assessing the use of artificial intelligence in automating the kyc processes aiming to reduce manual errors and improve customer experience	Haar-cascade, DeepFace	High dependency on data quality potential biases in AI algorithms affecting accuracy
Privacy preserving techniques in eKYC [10]	Proposing privacy preserving techniques that enhance user confidentiality during the EKYC processes using cryptographic methods	CP-ABE Cryptography, Arbetiary Blockchain	Complexity of implementation :may require significant changes to existing infrastructure which could hinder adoption
Impact of Blockchain on financial services [11]	Analysing the broader impact of blockchain technology on financial services with a specific focus on its role in improving kyc processes	Arbetiary Blockchain	Generalisation across financial services may overlook specific challenges faced by different sectors within finance

Machine Learning Approaches for Fraud Detection in KYC [12]	Evaluating machine learning techniques for detecting fraudulent activities during kyc processes enhancing risk management strategies	Django, Bootstrap, Laravel, SQL	Requires large data set for training ; potential overfitting issues if not properly managed; reliance on historical data can limit adaptability to new fraud patterns
Comparative Study of Digital identity Solution for KYC [13]	Conducting a comparative analysis of various digital and identity solutions used for kyc purposes across different industries assessing their strengths and weakness	PADU Database System	May lack debt in analysing specific case studies or real world implementations which could provide practical insights
Togggle's Decentralised KYC Insights [14]	Exploring how distributed storage networks can enhance data security, privacy, and resilience compared to traditional, centralised KYC systems. By decentralising data storage, Togggle aims to address issues associated with central databases, such as single points of failure and vulnerability to large-scale data breaches. .	Arbetiary Blockchain	The challenge of regulatory compliance across jurisdictions. Decentralised storage requires coordination across a dispersed network, which may complicate adherence to strict data protection laws and operational consistency across countries
Decentralised vs Centralised: A Detailed Comparison [15]	Examine the benefits and challenges of centralised and decentralised systems and discuss use cases and potential applications for both approaches.	Arbetiary Blockchain	Focuses mainly on high-level comparisons, leaving out detailed technical analysis.Doesn't dive into specific use cases within the financial or regulatory sectors, which could provide more insight into the practical

The implementation of blockchain technology addresses numerous challenges associated with data verification while simultaneously enabling financial institutions and their clients to monitor their profits effectively. "Self-identification" is crucial in fostering trust between businesses and their customers, serving as the foundational step in initiating a business relationship. Initially, banks engage in the KYC (Know Your Customer) process to complete identity verification before progressing to subsequent stages. Although the specifics of the KYC process differ across jurisdictions, it remains a mandatory requirement in the investment sector [16]. This process involves the collection of personal information such as names, addresses, and utility bills as proof of residence. In the investment landscape, KYC ensures that financial entities possess accurate data regarding their clients' financial backgrounds and investment experiences. However, these essential procedures are frequently perceived as tedious and burdensome for both consumers and banks.

2. ASPECTS IN KYC USING BLOCKCHAIN

The primary goal of KYC regulations is to reduce financial fraud in financial institutions. Failure to comply with these requirements can result in additional costs associated with the KYC process. Instead, some organisations see KYC as an opportunity because it allows them to understand their customers, identify their needs and behaviours, offer customised products, and encourage customer loyalty, ultimately increasing profitability. There are two types of KYC procedures: traditional KYC procedures and electronic KYC (eKYC) procedures designed for digital platforms. While the steps for eKYC and KYC are similar, the KYC engagement process begins with potential customers applying for an account, then filling out a registration form, verifying personal information,

and logging in to financial services to set up the required number.

2.1. REGULAR KYC PROCESS

The traditional KYC process (Figure 1) involves an interview. This method is done without using technology, with paper branches. Customers must visit the nearest financial institution in person. First, they need to send copies of the required documents to the institution. After that, the customer fills the registration form and waits for the verification process to be completed. Manual work done with recycling has been transformed into digital services.

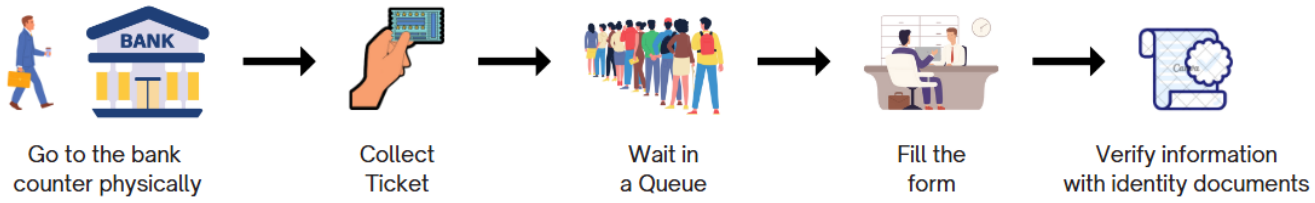


FIGURE 1 : REGULAR KYC PROCESS

2.2. INITIAL EKYC PROCESS

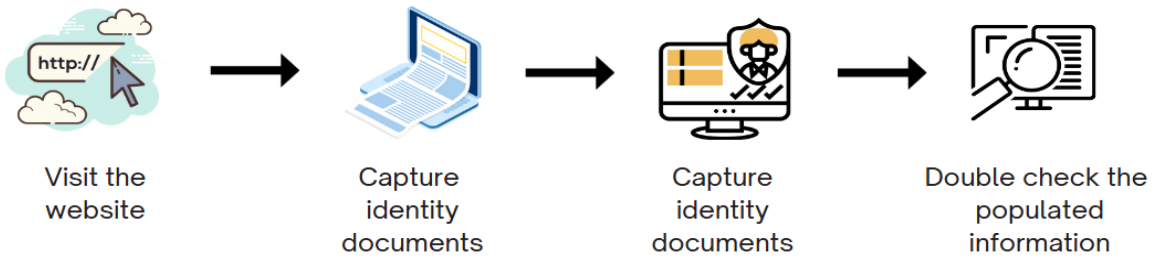


FIGURE 2. INITIAL EKYC PROCESS

The transition from manual processes to digital services in recycling has significantly transformed the landscape of eKYC (electronic Know Your Customer) solutions. This digitization empowers various financial service sectors, including digital banking, e-money, and fintech loans, to innovate and enhance their offerings. By facilitating scalability and improving user experience, eKYC enables immediate identity verification and efficient information management. However, the lengthy and repetitive registration procedures employed by many banks complicate the user experience for business clients. The limited reusability of customer KYC data across different banks is primarily hindered by the absence of standardized procedures and the reluctance of institutions to share customer data with competitors. In light of these challenges associated with centralized systems, banks are increasingly exploring decentralized ledger technology as a viable alternative

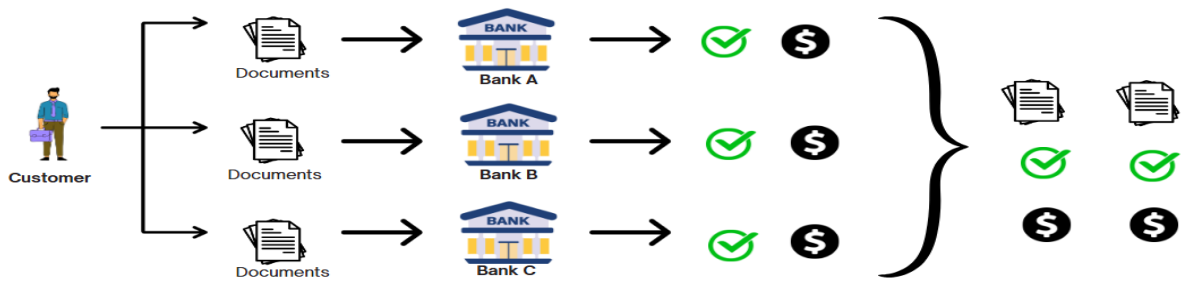
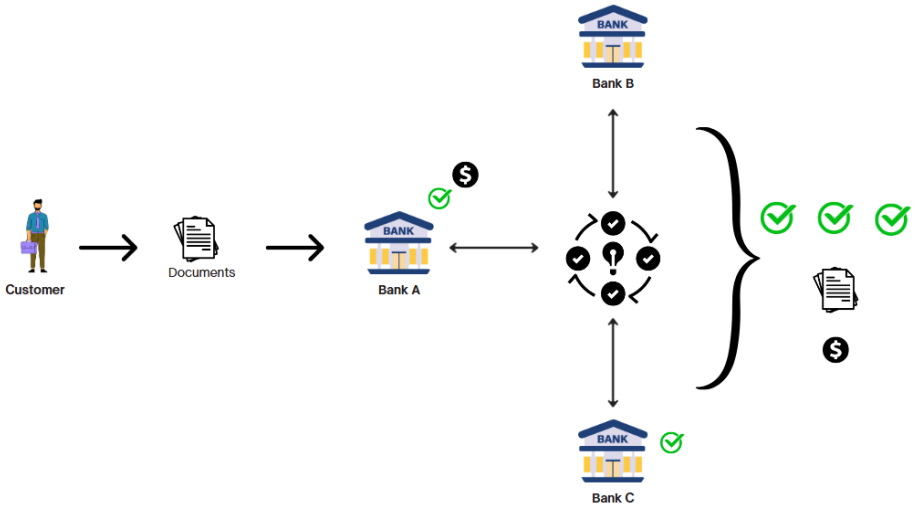


FIGURE 3: KYC PROCESS WITHOUT BLOCKCHAIN (TRADITIONAL)

The process depicted in Figure 3 outlines the current implementation of KYC systems across various financial sectors. In this framework, each financial institution independently verifies the identity of its users. For instance, when an individual seeks to open accounts at multiple banks, each institution conducts its own verification checks. A significant drawback of the existing KYC system is that all verifications must be performed from the ground up, resulting in considerable time and financial expenditure. This approach also raises security concerns, as personal information is transmitted from clients to servers during each verification, creating potential risks for data interception.

FIGURE 4: BLOCKCHAIN APPROACHES FOR KYC



In the banking example illustrated in Figure 4, the identity verification process operates as follows: business clients are required to engage with the KYC process to access the bank's services. Upon successful verification and approval, the bank records the user's data on a blockchain platform, enabling access for other banks. When a user seeks services from a different bank, that institution can connect to the system to authenticate the user's identity, thereby mitigating risks and simplifying the verification process. The architecture of blockchain allows for the integration of data from multiple financial institutions in a single, cryptographically secure, and immutable format, eliminating the necessity for third-party verification of information accuracy. This system facilitates a scenario where users need only complete the KYC process once to utilize the platform for identity verification. Importantly, access to user data is granted solely with the explicit consent of the user.

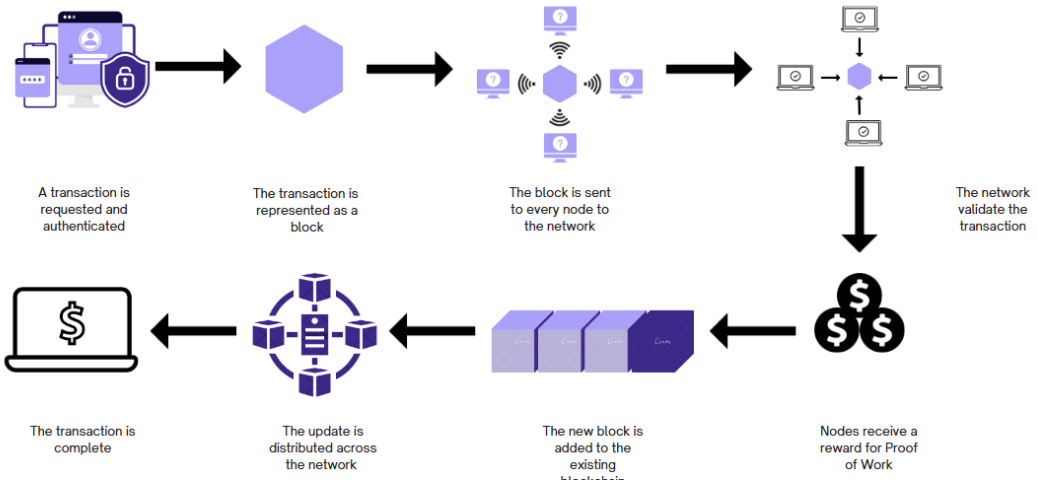


FIGURE 5 : THE BLOCKCHAIN PROCESS

Distributed Ledger Technology (DLT) encompasses a peer-to-peer network that replicates data across multiple nodes, with a dedicated node managing link key agreements to oversee transaction statuses and synchronize all copies. This decentralized ledger framework is designed to mitigate the risks of collisions and misconduct from a limited number of nodes, thereby facilitating easy access and a distributed digital infrastructure. However, DLT faces challenges related to scalability and privacy. Among the various business management systems, blockchain stands out as one of the most widely adopted technologies. A fundamental characteristic of blockchain is its method of organizing transactions into blocks, each containing the hash value of the preceding block, which contributes to the creation of tamper-proof records.

A decentralized blockchain-enabled system for banks to collaborate on eKYC (electronic Know Your Customer) processes offers significant benefits by removing the need for intermediaries. This study presents an in- depth evaluation of the banking industry, specifically focusing on KYC processes, exploring how blockchain technology can be applied within this domain. It analyzes various recently developed blockchain-powered KYC frameworks and proposes a performance assessment methodology to evaluate the efficiency of blockchain-based KYC solutions in banking. Key evaluation criteria include data accuracy, privacy, security, and scalability.

Furthermore, this research advocates for an open approach to integrating blockchain into KYC processes, emphasizing aspects such as process approval, scalability, resolution strategies, decision-making frameworks, and the development of a robust blockchain platform. The aim of these studies is to address existing challenges within the banking sector, enhance security and efficiency, and contribute to the advancement of KYC procedures.

3. CURRENT FINDINGS

The existing KYC process is inefficient and overly dependent on manual paperwork, lacking an integrated monitoring framework, which creates opportunities for fraudulent activities. Banks must validate customer identities to prevent illegal activities, but this process often leads to concerns over privacy and security. Several contemporary systems have proposed methods to address these issues.

One solution leverages the IPFS protocol and Gpg4win through the Kleopatra platform to improve data privacy in KYC procedures. This approach enables banks to encrypt and store verified customer documents on the IPFS network, allowing customers to seamlessly open accounts at different banks without needing to resubmit documentation.[17]

Another study explored both centralised and decentralised blockchain KYC solutions, emphasising interbank cooperation and the need for pilot implementations in smaller countries. A DLT-based scheme was proposed to reduce KYC verification costs while enhancing user experience, although the growing data storage costs were not addressed. [18]

Implementing regulatory technology (Regtech) has also been suggested to alleviate the KYC burden on financial institutions. This approach highlights the differences between Regtech and Fintech, noting that Regtech provides solutions rather than competing with banks, although the full deployment of blockchain in this context was not fully explored. [19]

Trust issues in interbank transactions have been addressed by proposing a system to enhance anonymity and accountability using mathematical tools. A blockchain and smart contract-based approach was developed to improve anonymity for financial organisations, dividing the system into an application layer for user interaction and a code base for data processing.

Another examination of the integration of Blockchain in the banking sector identified challenges such as high energy consumption and hardware costs. The analysis focused on economic efficiency, operational efficiency, and service efficiency, highlighting the need for sustainable practices in mining operations.

A Hyperledger Composer-based system was tested, demonstrating its ability to expedite KYC processes, reduce inefficiencies, and enhance data sharing while ensuring cost-effectiveness and transparency. [20]

The advantages of integrating blockchain into KYC processes have been highlighted, showcasing how smart contracts can greatly reduce the costs associated with verification for organizations. The proposed blockchain framework focuses on the influence of KYC document authentication on financial entities and evaluates factors such as accreditation, validation, revocation, confidentiality, and accessibility. [3]

In another study, KYC risks in populous countries were investigated, opting for big data analysis to mitigate fraud risks instead of blockchain. This method compares customer identities and addresses using fuzzy matching and MapReduce techniques.

Lastly, a decentralised solution called CODE was introduced, utilising Corda for secure data exchange and proposing an address-search technique to expedite beneficiary identification without intermediaries. [21].

4. FETCH.AI TECHNOLOGY

Fetch.ai is a decentralised network powered by blockchain technology and artificial intelligence (AI). Its core objective is to enable autonomous agents—digital entities capable of performing tasks without human intervention—to interact with each other and the physical world in a decentralised economy. Fetch.ai creates a platform where machines, data, services, and people can seamlessly trade and collaborate autonomously in various sectors such as finance, supply chain, smart cities, and more. [22]

Fetch.ai combines key technologies such as autonomous economic agents (AEAs), decentralised machine learning, oracles, and a scalable blockchain to provide intelligent solutions for real-world problems, including decentralised Know Your Customer (dKYC) systems.

Using Fetch.ai's technology framework, a decentralised KYC (Know Your Customer) system can be implemented on the blockchain. Here's how the components of Fetch.ai’s tech stack can be leveraged for such an application:

a. Autonomous Economic Agents (AEAs) for KYC Verification:

In this context, AEAs can be deployed to act as KYC verifiers or users seeking verification. AEAs can autonomously handle tasks such as data collection, verification, and validation without human intervention. Here's how the process could unfold:uAgents (Autonomous Economic Agents) are modular, programmable digital entities that operate independently within the Fetch.ai ecosystem. Each uAgent is tailored for specific tasks and can autonomously interact with other agents, users, and services.

- KYC Request Handler Agents: These agents are responsible for processing and validating KYC requests, each focusing on a particular aspect of verification:
    - Document Validator Agent (DVA):
        - Role: Handles the preliminary validation of documents submitted by users, such as passports, utility bills, or national IDs
        - Tasks:
            - Scans documents for completeness and correctness.
            - Uses machine learning to verify authenticity, such as identifying watermarks or detecting signs of forgery
        - Output: Provides a validity score or approval flag for the submitted documents.
    - Identity Checker Agent (ICA):
        - Role: Cross-verifies the user’s identity against external data sources, such as government databases or credit bureaus.
        - Tasks:
            - Matches names, addresses, and photos with trusted off- chain sources.
            - Validates biometric data if provided.
        - Output: Confirms identity consistency and compliance with regulatory requirements.
    - Risk Assessment Agent (RAA):

- Role: Conducts a risk analysis of the individual based on their identity and historical behavior.
- Tasks:
  - Checks for red flags, such as associations with fraudulent activity or sanctions.
  - Employs predictive models to assess risk levels, such as creditworthiness or financial stability.
- Output: Assigns a risk score to the individual.

- Unique Identity Generator Agent (UIGA):
  - Role: Ensures that each user is uniquely identifiable within the network while preserving anonymity where required.
  - Tasks:
    - Generates cryptographic identifiers for users (e.g., hashed IDs).
    - Prevents duplicate identities by comparing hashed records against existing identifiers.
  - Output: Issues a unique, reusable identity for the user on the blockchain.

- Service Provider Agent (SPA):
  - Role: Represents the organisation or platform (e.g., banks, DeFi platforms) requesting the KYC verification.
  - Tasks:
    - Initiates KYC requests and communicates specific requirements to the network.
    - Receives and interprets verification results from the KYC Request Handler Agents.
    - Uses selective disclosure to access only the information needed for compliance.
  - Output: Provides services (e.g., account creation, transaction approval) upon successful KYC completion.

This ensures real-time, tamper-proof KYC processes, reducing the need for centralised KYC systems where user data is held by multiple entities.

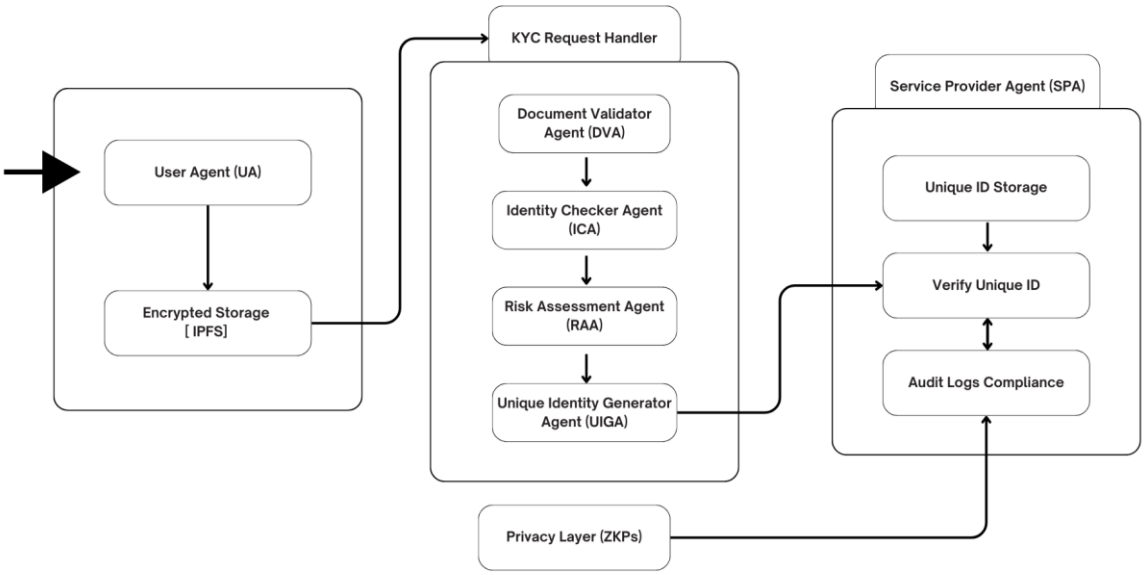


FIGURE 6: PROPOSED ARCHITECTURE

b. Fetch.ai Blockchain for Secure Data Storage and Transparency:

The blockchain provides a decentralised ledger that securely stores verified KYC information and audit trails without exposing private details. Instead of storing the sensitive data directly on-chain, hashed versions of the KYC data can be stored to ensure security and privacy. Some key features:

- **Immutable Records**: Once KYC is verified and recorded, it becomes immutable, preventing tampering and fraud.
- **Selective Disclosure**: The user can give selective access to their KYC information to different institutions or services without revealing unnecessary data. For example, they could prove their identity to one service without disclosing the full documentation.
- **Auditability**: Every KYC request and verification can be audited easily on the blockchain, ensuring transparency and compliance with regulations.

c. Decentralised Machine Learning for KYC Data Processing: Decentralised machine learning models on Fetch.ai can be used to enhance the KYC process by automating the verification of documents. Machine learning models can:

- **Analyse Documents**: Automatically scan and validate identification documents, recognizing patterns, matching signatures, and detecting anomalies such as forged documents.
- **Fraud Detection**: Predictive algorithms could be used to identify potential fraud based on historical data, flags, and behavioural patterns in the submissions.
- **Ongoing Monitoring**: Post-verification, machine learning can continually monitor transactions and activities associated with the verified individuals to detect suspicious or non-compliant activities. Since the machine learning models are decentralised, no single entity owns or controls the data, making the system more secure and trustworthy.

d. Oracles for Off-Chain Data Integration:

In the KYC process, it's often necessary to integrate external, off-chain data sources such as government databases, credit agencies, or financial institutions. Fetch.ai's decentralised oracles can securely pull in off-chain data to the blockchain for use by AEAs during verification.

- **Data Integration:** An oracle could fetch real-time data from trusted third-party identity providers (e.g., government IDs, biometrics) for KYC validation.
- **Trustless Verification:** By using decentralised oracles, you ensure that the KYC system remains tamper-resistant, as no single centralised provider controls the data flow.

e. Interoperability via Cosmos SDK:

Fetch.ai's interoperability through Cosmos SDK can facilitate cross-chain KYC solutions. For example, if an individual has already undergone KYC on another blockchain (e.g., Ethereum or Binance Smart Chain), Fetch.ai's system can pull in this verified KYC information via cross-chain communication, ensuring no redundancy.

- **Cross-Chain Identity Management**: Individuals won't need to repeat the KYC process on every blockchain or platform they use; instead, verified credentials can be shared across different chains through interoperability.

f. Open Economic Framework (OEF) for KYC Marketplace:

The OEF could support a decentralised KYC marketplace where identity providers (banks, government agencies, etc.) and verifiers (e.g., financial institutions, exchanges) interact in a trustless manner:

- **Discovery of Providers**: Service providers needing KYC verification (such as a crypto exchange) can automatically discover KYC verification agents available on the network.
- **Decentralised Marketplace**: The OEF ensures that multiple KYC service providers compete, ensuring better pricing and faster services for users and businesses.

4.1. USE CASE EXAMPLE FOR KYC IN FETCH.AI'S FRAMEWORK

Imagine a decentralised finance (DeFi) platform or crypto exchange using a KYC process. A user wants to join the platform:

- **The user's agent** submits identification details.
- **KYC verification agents** (banks, certified identity verifiers, or government agencies) assess the documents and confirm validity.
- Upon successful verification, a hashed record of this KYC is stored on the blockchain.
- The user can now prove their identity to any other platform or service by giving selective access to this verified KYC record without redoing the process.

4.2. PROPOSED ADVANTAGES USING FETCH.AI'S DECENTRALIZED SYSTEM

- **Enhanced Security and Privacy:** By decentralising data and allowing users to control access, Fetch.ai minimises the risk of data breaches and misuse.
- **Efficient and Scalable:** AEAs and machine learning models can quickly verify identities, making the system faster and more scalable than traditional KYC processes.
- **Interoperability:** Fetch.ai's blockchain can work across different chains, allowing verified KYC credentials to be reused across platforms.
- **Cost-Effective:** By decentralising the KYC process, intermediaries are reduced, leading to lower costs for businesses and users.

This approach is especially relevant for applications in decentralised finance (DeFi), online financial services, and blockchain-based platforms where user verification is necessary for compliance or trust-building.

4.3. FETCH.AI TECHNOLOGY TO ADDRESS CHALLENGES IN KYC SYSTEMS

Fetch.ai's decentralised artificial intelligence framework, built on blockchain technology, presents innovative solutions to the challenges identified in current research regarding Know Your Customer (KYC) processes and financial services:

- **Regulatory Compliance and Integration Difficulties:** The decentralised structure of Fetch.ai facilitates secure data sharing among various entities, thereby ensuring adherence to regulatory standards such as the General Data Protection Regulation (GDPR). Its consensus mechanism promotes coordination across different jurisdictions, supporting regulatory compliance while maintaining user privacy.
- **Data Quality and Algorithmic Bias in AI:** By utilising decentralised data sources and enabling real-time validation, Fetch.ai effectively addresses the risks associated with biassed datasets in AI training.

This approach leads to the development of more precise and adaptable models for fraud detection.

- **Implementation Complexity:** Fetch.ai adopts a modular strategy for integrating AI agents and blockchain technology into existing infrastructures, which simplifies the implementation process.This reduces the burden on financial institutions, allowing for easier adoption without necessitating extensive infrastructure changes.
- **Cross-Sector Applicability in Financial Services:** The customizable nature of Fetch.ai's framework allows for adjustments to meet the specific needs of various sectors, ensuring that its solutions are versatile and applicable across different financial domains, including retail banking, insurance, and asset management.
- **Handling Large Datasets and Overfitting Issues:** Through the use of federated learning, Fetch.ai enables machine learning on distributed datasets without the need to centralise sensitive information. This approach diminishes the risks of overfitting and enhances the system's ability to adapt to changing fraud patterns.
- **Absence of Practical Case Studies:** Fetch.ai has successfully implemented its technology in sectors such as supply chain and energy, offering valuable insights that can be leveraged within the financial industry. By analysing these case studies, Fetch.ai can improve the understanding of practical

applications in finance, leading to more tailored solutions.

5. CONCLUSION

This article provides an in-depth evaluation of applying blockchain technology in the banking industry, specifically focusing on Know Your Customer processes. It examines the integration of IPFS-based distributed storage and Fetch.ai's multi-agent technology to improve the efficiency and decentralization of KYC solutions. The study also reviews several modern implementations of blockchain-enabled KYC frameworks. Additionally, the article introduces a performance evaluation framework to assess the effectiveness of these solutions, emphasizing key aspects such as data accuracy, privacy, robustness, and scalability.

Furthermore, this article advocates for an open research approach to integrating blockchain into KYC processes, concentrating on aspects such as process validation, scalability, resolution strategies, decision-making frameworks, and the development of a robust blockchain platform. The objective of these studies is to address existing challenges within the banking sector, enhance security and efficiency, and contribute to the advancement of KYC procedures.

REFERENCES

[1] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). "An overview of blockchain technology: Architecture, consensus, and future trends." Proceedings - 2017 IEEE 6th International Congress on Big Data (BigData Congress). This paper provides an in-depth understanding of blockchain architecture and its potential applications in various sectors, including KYC.

[2] Lee, J. H., & Pilkington, M. (2017). "How the blockchain revolution will reshape the consumer electronics industry." IEEE Consumer Electronics Magazine, 6(3), 19-23. While the focus is on the electronics industry, the insights on how blockchain transforms identity verification and data handling are highly relevant for KYC.

[3] Nguyen, Q. K. (2016). "Blockchain - A Financial Technology for Future Sustainable Development." 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD). This paper highlights the sustainable and secure nature of blockchain, with discussions on its use for identity verification in financial services.

[4] HSBC Money Laundering Scandal

- U.S. Department of Justice. (2012). "HSBC Bank USA, N.A. to Forfeit $1.256 Billion and Enter into Deferred Prosecution Agreement."
- BBC News. (2012). "HSBC fined $1.9bn over money laundering."
- The Guardian. (2012). "HSBC admits failure to prevent money laundering."

[5] CBA Money Laundering Scandal

- AUSTRAC. (2017). "Commonwealth Bank of Australia - Statement of Claim."
- The Sydney Morning Herald. (2018). "Commonwealth Bank to pay $700 million in AUSTRAC settlement."
- Reuters. (2018). "Commonwealth Bank agrees to pay A$700 million in money-laundering case."

[6] Deutsche Bank Money Laundering Scandal

- The New York Times. (2017). "Deutsche Bank to Pay $630 Million to Resolve Money Laundering Case."
- The Guardian. (2020). "Deutsche Bank fined $150m for Epstein ties and money laundering breaches."
- Bloomberg. (2021). "Deutsche Bank's Compliance Crisis: A Timeline"

[7] Alharby, M., & van Moorsel, A. (2017). "Blockchain-based smart contracts: A systematic mapping study." Proceedings of the International Conference on Cloud Computing (CLOUD 2017). This paper explores smart contracts on blockchain, including how they can be utilised in automating KYC processes in a decentralised manner.

[8] Blockchain for KYC Verification. "Patil, P., & Sangeetha, M. (2022). Blockchain-based decentralised KYC verification framework for Banks. Procedia Computer Science, 215, 529-536."

[9] Transforming KYC with AI: A Comprehensive Review of Artificial Intelligence-Based Identity Verification. “Khare, P., & Srivastava, S. (2023). Transforming KYC with AI: A Comprehensive Review of Artificial Intelligence-Based Identity Verification. J. Emerg. Technol. Innov. Res, 10(12), 525-530.”

[10] Privacy preserving techniques in eKYC. “Fugkeaw, S. (2022). Enabling trust and privacy-preserving e-KYC systems using blockchain. IEEE Access, 10, 49028-49039.”

[11] Impact of Blockchain on financial services. “Fairoh, A. A. M., Hussin, N. N., Jamali, N. A. A., & Ali, M. M. (2024). The Impact of Blockchain in Financial Industry: A Concept Paper. Information Management and Business Review, 16(1 (I)), 190-196.”

[12] Machine Learning Approaches for Fraud Detection in KYC. “Njoku, D. O., Iwuchukwu, V. C., Jibiri, J. E., Ikwuazom, C. T., Ofoegbu, C. I., & Nwokoma, F. O. (2024). Machine learning approach for fraud detection system in financial institution: a web base application. Machine Learning, 20(4), 01-12”

[13] Comparative Study of Digital identity Solution for KYC. “Subri, N. I., Hanafi, A. G., & Pozin, M. A. A. (2024). Comparative Analysis of eKYC and 2FA in Implementing PADU Database System to Strengthen Digital Identity Security.”

[14] Togggle’s Decentralised KYC Insights. “Togggle’s Decentralised KYC Insights, Togggle” (https://www.togggle.io/blog/kyc-data-storage-centralized-decentralized)

[15] Decentralised vs. Centralised: A Detailed Comparison. “Decentralised vs. Centralised: A Detailed Comparison, 101 Blockchains” (https://101blockchains.com/decentralized-vs-centralized/)

[16] Lemieux, V. L. (2016). "Trusting records: is Blockchain technology the answer?" Records Management Journal, 26(2), 110-139. This article examines blockchain as a technology for securing and verifying records, relevant to KYC where trust and verification are key.

[17] Al Mamun, A., Hasan, S., Bhuiyan, M., Kaiser, M. & Yousuf, M. Secure and transparent KYC for banking system using IPFS and blockchain technology. 2020 IEEE Region 10 Symposium (TENSYMP). pp. 348-351 (2020). DOI: 10.1109/TENSYMP50017.2020.9230987.

[18] Moyano, J. & Ross, O. KYC Optimization Using Distributed Ledger Technology. Business & Information Systems Engineering. 59, 411-423 (2017,11). DOI: 10.1007/s12599-017-0504-2.

[19] Lootsma, Y. Blockchain as the newest regtech application—the opportunity to reduce the burden of kyc for financial institutions. Banking & Financial Services Policy Report. 36, 16-21 (2017).

[20] Ullah, N., Al-Dhlan, K. & Al-Rahmi, W. KYC optimization by blockchain based hyperledger fabric network. 2021 4th International Conference On Advanced Electronic Materials, Computers And Software Engineering (AEMCSE). pp. 1294-1299 (2021). DOI: 10.1109/AEMCSE51986.2021.00264.

[21] Lee, C., Kang, C., Choi, W., Cha, M., Woo, J. & Hong, J. CODE: Blockchain-based Travel Rule Compliance System. 2022 IEEE International Conference On Blockchain (Blockchain). pp. 222-229 (2022). DOI: 10.1109/Blockchain55522.2022.00038.

[22] Fetch.ai, Decentralized economy and autonomous agents: https://fetch.ai/ .