CogNexus Volume: 1 Issue: 2 4/2025/pp.206-224

A Multidisciplinary, International, Peer-Reviewed, Open Access Journal

Federated and Privacy-Preserving MLOps Frameworks: Blockchain-Enabled Compliance for KYC in Financial Systems

[1] Emmanuel Ahaiwe
[2]Joseph Oduro-Gyan
[3]Damilare Samson Ogunsesan
[4]Abdul-Lateef Arotayo
[5]Ahmed Bello
[6]Godliver Alangyam Awonlie
Corresponding Author Email: ***emmanuelahaiwe27@gmail.com***
[1]University of Portsmouth
Orcid ID: https://orcid.org/0009-0009-1446-9698
[2]College of Professional Studies, Northeastern University
Orcid ID: https://orcid.org/0009-0002-7890-5312
[3]Department of Computer science, Kutztown University of Pennsylvania
Orcid ID: https://orcid.org/0009-0002-9138-8006
[4]Department of Management Science, University Of Bradford, England
Orcid ID: https://orcid.org/0009-0009-7158-8108
[5]Illinois State University, Normal, Illinois
Orcid ID: https://orcid.org/0009-0005-1692-4413
[6]College of Professional Studies, Northeastern University
Orcid ID: https://orcid.org/0009-0000-6091-4136

.

Abstract

Federated learning (FL), privacy-preserving machine learning (PPML), and blockchain technologies present an opportunity to improve Know Your Customer (KYC) compliance in the financial systems and ensure that the privacy of the user is protected. Regardless of this growing interest, the current frameworks usually do not meet the complex regulatory demands, scalability issues and identity attestation demands of real-world financial systems. Based on an integrative review approach, articles and the latest frameworks of the credible data sources are examined to pinpoint the architectural patterns, privacy strategies, governing models, and compliance characteristics are examined. Study found out that there are enduring privacy and auditability tradeoffs, a bottleneck in large-scale deployments, and gaps in full regulatory alignment, especially in the areas of credential revocation and lawful deanonymization. Review emphasises the recent practical models like REGKYC and DPFedBank, which show the progress of policy implementation and privacy-utility ratios. Considering these insights, we will make our recommendations based on the following provisions: modular architecture, flexible identity credential systems, the clarity of governance, adjustable regulatory provisions, and user-friendly privacy mechanisms. This paper highlights the necessity of field pilot applications and cross-functional cooperation to move federated privacy-preserving MLOps out of the prototype into a working application in financial KYC. This review can be seen as a contribution to the further development of blockchain-based compliance tools that will provide safe and transparent, and privacy-sensitive identity management in the changing financial industry.

Keywords: *Federated Learning, Privacy-Preserving Machine Learning, Blockchain, KYC Compliance, Financial Systems, Data Privacy, MLOps*

INTRODUCTION

Know Your Customer (KYC) rules are the mainstay of anti-money laundering (AML) and counter-terrorism financing (CTF) compliance in the global banking system, which requires any financial institution to ensure the authenticity of its clients to spot and prevent fraud and other illicit financial flows. A growing digitisation of the financial services sector, alongside the complications of human interaction, has rendered previously resource-intensive, error-prone, and generally ineffective at scale, traditional KYC operations (Bello et al., 2025).

Machine Learning (ML) brings a paradigm shift towards streamlining the KYC business, as it allows automated identity verification, fraud detection, monitoring transactions, and profiling risks (Abdulrauf et al., 2025a; Adebowale & Akinnagbe, 2023). Nonetheless, ML utility mainly relies on access to large amounts of quality data. Concentration of such sensitive financial and identity information creates significant issues of privacy, security and regulatory compliance, especially with the tough data protection rules, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and industry-specific financial rules (Zhuk, 2025; Umakor et al., 2025).

As a way of mitigating these problems, Federated Learning (FL) has become one of the privacy-friendly distributed ML frameworks that allow multiple parties to train models collectively without transferring raw data. Rather, the participants use model parameters or gradients to exchange data, maintaining locality (Baabdullah et al., 2024). Privacy-Preserving Machine Learning (PPML) techniques like Differential Privacy (DP), Secure Multi-Party Computation (SMPC), Homomorphic Encryption (HE), and Zero-Knowledge Proofs (ZKPs) are frequently used together with FL to further reduce the risks associated with privacy when one is training or using their models to infer information (Sameera et al., 2024; Zhou et al., 2024; Umakor et al., 2025).

Nonetheless, the technical merits of FL and PPML are sometimes incapable of meeting the entire financial regulatory requirements, especially as regards auditing, policy implementation, identity testimonies, and identifiable decision-making. Regulators not only need to ensure data protection but also expect to see demonstrable signs of behavioural compliance and open systems of oversight throughout financial AI systems (Xiong et al., 2025; James et al., 2025).

It is in this area that blockchain technologies can provide important complements. Blockchain offers a decentralised record keeping, cryptographic assurances of data integrity, verifiable credentials and Decentralised Identifier (DID) systems--all of which are necessary in regulated identity and access management (Suzuki et al., 2024; Aidoo & Dip, 2025). Additionally, the compliance policies can be coded and enforced by smart contracts, and the auditability and accountability of distributed ML activities are preserved (Chen et al., 2025; Ahmed & Alabi, 2024).

With Federated Learning, Privacy-Preserving ML, and Blockchain converging, it is now possible to construct powerful and regulation-vaulting MLOps designs that fit financial institutions. Such combined systems allow joint, privacy-conscious AI development and deployment, as well as provide the necessary transparency in operations and legal responsibility, which is essential in the KYC, AML, and fraud detection applications (Abuzied et al., 2024; Chhetri et al., 2023; Brahmandam, 2025).

This paper conducts an integrative systematic review to explore this emerging intersection and to answer the following research questions:

1. What recent frameworks combine federated learning, privacy-preserving ML, and blockchain for KYC or related identity verification and fraud prevention in financial services?
2. What are the architectural designs, privacy and security techniques, blockchain usage patterns, and regulatory compliance features in those frameworks?
3. What are the gaps, trade-offs, and challenges observed in current research?
4. What are directions and recommendations for future research and real-world implementation?

By synthesising the latest developments in federated, privacy-preserving, and blockchain-enhanced ML frameworks, this paper aims to provide foundational insights and actionable recommendations for designing next-generation, regulation-aware MLOps systems that align with both business goals and compliance mandates in the financial sector.

Methodology

The method of the study is an integrative review, which is most appropriate in synthesising a wide scope of research findings, both empirical and theoretical, in order to bring a comprehensive picture of complex topics. Since federated learning is an interdisciplinary method, privacy-sensitive solutions, blockchain, and KYC compliance in financial systems, the integrative review method enables the incorporation of different views into a shared framework.

A systematic search of several well-known academic databases, such as IEEE Xplore, ACM Digital Library, PubMed, arXiv, and SpringerLink, was used to obtain pertinent literature. Only the sources that were published within the period of 2022 to 2025 were included in the search to be sure that the latest developments and available methods in the area are considered. The period represents the emergent trends and research on the state-of-the-art of the collaboration of federated learning and blockchain technologies with regulatory compliance.

The inclusion and exclusion criteria were very clear, and therefore, the selection of the studies was done. A review of peer-reviewed journal articles and conference papers that dedicated their attention to federated learning, privacy-preserving solutions, blockchain implementation, and KYC or AML compliance was excluded. Empirical, theoretical, or conceptual models were also used to identify a broad range of insights through research that has empirical data, theoretical models, or conceptual frameworks. On the other hand, only peer-reviewed articles, those published within the date limit, and articles irrelevant to the convergence of these technologies and regulatory systems were retained to retain rigour and relevance.

Data extraction was involved to determine the main elements of each of the studies, such as the research design, key findings, methodologies applied and the significance to KYC compliance. These data points were methodically clustered in thematic groupings, which enabled thematic and meaningful interpretation. The thematic analysis was used as the next synthesis to provide the coding, categorisation, and formulation of the general themes that would mark the relationships and gaps in the existing literature. The final result of this process was the creation of a conceptual system that shows how federated learning, privacy-enhancing methods, and blockchain can all serve to ensure that financial systems comply with KYC.

The evaluation of quality was also part of the review. The inclusion of each study was critically evaluated regarding its relevance to the research outcomes, the quality of the methodology, and the impact on the field, in general. The scores were rated on a scale of 1 to 5 based on the following criteria, and only those carrying an average score high enough were incorporated in the final synthesis. This quality check was done to make sure that the review is based on effective and credible research.

Since it was a literature-based integrative review, there was no need to have formal ethical approval. However, the ethical concerns were considered in the proper way of representing the study results and being open in terms of the limitations of the included works. Such cautiousness contributes to the validity and honesty of the conclusions of the review.

Results

Overview of Included Studies

This section presents the summary of the assessed journals on federated and privacy-preserving learning integrated with blockchain, blockchain-enabled MLOps and AI governance frameworks, and blockchain for KYC, AML, and financial compliance, in a tabular form.

Table 1: Federated and Privacy-Preserving Learning Integrated with Blockchain

Author(s)	Key Objective	Method	Key Findings	Identified Gap
Abuzied et al. (2024)	Develop a privacy-preserving federated learning framework for blockchain networks.	Designed a hybrid blockchain-FL architecture, tested on distributed datasets.	Demonstrated reduced privacy leakage and improved training efficiency.	No application to compliance or KYC systems.
Jia et al. (2024)	Propose blockchain-based privacy-preserving multi-	Hybrid blockchain & FL with encryption-based aggregation.	Enhanced model accuracy while maintaining data confidentiality.	No focus on financial or compliance applications.

	task federated learning.			
He et al. (2024) – DPFedBank	Craft privacy-preserving FL for financial institutions with policy pillars.	Federated learning with differential privacy and governance layer.	Balanced model performance with policy-based compliance.	Does not integrate blockchain for auditability.
Baabdullah et al. (2024)	Evaluate blockchain + FL for credit card fraud detection.	Experimental study using blockchain ledger for FL model updates.	Improved fraud detection accuracy and transaction-level privacy.	Lacks full MLOps lifecycle automation and regulatory audit trail.
Kejriwal et al. (2024)	Introduce proof-of-learning consensus for decentralised FL trust.	Conceptual design validated via simulation.	Ensures trustworthiness and traceability in federated model training.	Not yet applied to KYC or AML contexts.
Sameera et al. (2024)	Review privacy-preserving methods in blockchain-based FL.	Systematic review and taxonomy.	Identified encryption, differential privacy, and ZKPs as key enablers.	No financial compliance integration.
Ngoupayou et al. (2025)	Survey on blockchain-based privacy-enhancing federated learning in smart systems.	Literature synthesis of privacy-enhancing methods.	Classified frameworks by blockchain role (audit, storage, access).	Focused on healthcare, not financial KYC.
Mahmood & Jusas (2022)	Develop a multi-layer blockchain-FL security platform.	Multi-tier blockchain ledger for FL updates.	Ensures model provenance and data confidentiality.	No compliance or governance tie-in.
Moulahi et al. (2023)	Blockchain-FL for IoT data privacy.	Architecture integrating FL aggregation with blockchain smart contracts.	Strong privacy with traceable model exchange.	No MLOps or compliance context.
Qammar et al. (2023)	Systematic review on securing FL with blockchain.	Review of over 80 frameworks.	Classified FL-blockchain integrations for data privacy.	Lacks financial or regulatory application scenarios.

Recent studies emphasise the convergence of federated learning (FL) and blockchain to enhance privacy and trust in decentralised systems. Studies by Abuzied et al. (2024), He et al. (2024), and Baabdullah et al. (2024) demonstrate that integrating blockchain with FL ensures secure aggregation, prevents data leakage, and improves model reliability. Reviews such as Sameera et al. (2024) and Ngoupayou et al. (2025) identify encryption, differential privacy, and zero-knowledge proofs as dominant privacy mechanisms. However, most of these frameworks remain experimental and lack alignment with regulatory compliance, KYC/AML requirements, and MLOps lifecycle automation.

Table 2: Blockchain-Enabled MLOps and AI Governance Frameworks

Author(s)	Key Objective	Method	Key Findings	Identified Gap
Kancherla (2022)	Enhance MLOps pipelines using blockchain for decentralised security.	Conceptual framework for secured model versioning and audit trails.	Improves integrity and trust in the ML lifecycle.	No link to federated privacy or KYC compliance.
Ridwan (2025)	Propose blockchain-enabled provenance tracking for MLOps.	Design of an immutable provenance layer in ML pipelines.	Ensures model accountability and reproducibility.	Does not incorporate federated or privacy-preserving architecture.
Ahnouch et al. (2024)	Optimise DevOps and MLOps architectures for financial compliance.	Financial institution-oriented architecture.	Compliance-aware MLOps with governance modules.	No blockchain or federated privacy element.
Petrović (2022)	Model-driven blockchain-enabled MLOps approach.	Model-based software engineering integrated with blockchain audit layers.	Improves automation and transparency in MLOps.	No discussion on KYC/AML or privacy.
Brahmandam (2025)	MLOps automation for financial compliance and fraud detection.	Conceptual industry review.	Highlights compliance automation via AI pipelines.	Missing blockchain-enabled traceability.

Research on blockchain-integrated MLOps highlights improved model governance, traceability, and auditability across AI pipelines. Kancherla (2022), Ridwan (2025), and Petrović (2022) propose blockchain layers for model provenance and secure versioning, while Ahnouch et al. (2024) and Brahmandam (2025) explore compliance-aware MLOps for financial institutions. These studies underscore blockchain's value in lifecycle transparency but lack integration with federated learning and privacy-preserving techniques, leaving gaps in distributed compliance management.

Table 3: Blockchain for KYC, AML, and Financial Compliance

Author(s)	Key Objective	Method	Key Findings	Identified Gap
Fugkeaw (2022)	Develop privacy-preserving e-KYC using blockchain.	Blockchain-based identity verification model.	Enhances data privacy and regulatory traceability in e-KYC.	Lacks ML or federated learning integration.
Bello et al. (2025)	Analyse blockchain for enhancing KYC and AML compliance.	Business analysis and conceptual modelling.	Blockchain improves transparency and verification integrity.	Absence of ML pipeline integration.
Divya et al. (2025)	Blockchain-based KYC to enhance credit allocation.	Prototype and system simulation.	Improves lending fairness and compliance.	Does not implement federated or

				privacy-preserving ML.
Xiong et al. (2025) – REGKYC	Present REGKYC for privacy and compliance enforcement.	Cryptographic framework combining blockchain and compliance logic.	Enables privacy-preserving, regulation-compliant KYC.	No AI/MLOps lifecycle integration.
James et al. (2025)	Explore privacy-preserving techniques for blockchain KYC/CDD.	Comparative review of cryptographic and privacy protocols.	Highlights zero-knowledge and differential privacy potential.	No integration with AI or MLOps workflows.
Oluwaferanmi (2025)	Smart compliance in AI-blockchain AML monitoring.	Critical analysis of AI-blockchain in regulatory compliance.	Identifies interoperability and governance challenges.	Missing federated and lifecycle governance aspects.
Sunday et al. (2025)	AI-driven AML infrastructure development.	Conceptual model for compliance modernisation.	Suggests AI-Blockchain synergy for AML efficiency.	No MLOps lifecycle or federated privacy dimension.
Sak (2024)	Study of KYC/AML technologies in DeFi.	Analytical review.	Highlights blockchain-based compliance monitoring mechanisms.	Does not involve federated ML or MLOps integration.

Literature on blockchain-enabled compliance, including Fugkeaw (2022), Bello et al. (2025), Divya et al. (2025), and Xiong et al. (2025), shows blockchain's capacity to enhance KYC/AML processes through data immutability and cryptographic verification. James et al. (2025) and Zhou et al. (2024) further advocate privacy-preserving methods like zero-knowledge proofs to safeguard customer data. Despite these gains, most studies omit AI-driven automation, federated model training, and MLOps orchestration, limiting their applicability to real-time, adaptive compliance systems.

Table 4: Synthesis and Conceptual Gap

Dimension	**Current Status in Literature**	**Gap Identified**
Federated Learning + Privacy Preservation	Extensively studied for healthcare, IoT, and finance separately (Abuzied 2024; He 2024; Baabdullah 2024).	Rarely integrated with MLOps lifecycle automation or compliance enforcement.
Blockchain Integration	Used for auditability, provenance, and secure communication (Mahmood & Jusas, 2022; Qammar, 2023).	Minimal connection to AI lifecycle management or regulatory logic.
MLOps Lifecycle Management	Growing in financial systems (Kancherla 2022; Ahnouch 2024; Ridwan 2025).	Missing privacy-preserving and federated learning elements.

KYC/AML Compliance Enablement	Addressed using blockchain and AI (Fugkeaw 2022; Xiong 2025; Bello 2025).	Absent in integrated federated-MLOps frameworks.
Unified Framework Need	Not applicable	Literature lacks a federated, privacy-preserving MLOps architecture that embeds blockchain-enabled compliance logic for KYC/AML in financial systems.

Collectively, current studies prove the progress of federated privacy, blockchain-based trust, and MLOps governance, but these practices exist in their own bubbles. There exists no single framework that combines federated learning, auditability with blockchain, and compliance-driven MLOps in the financial system in KYC or AML. The literature thereby shows that the gap is critical, namely, a federated, privacy-safe MLOps architecture incorporating the blockchain to enable regulatory compliance, ultimately, providing transparency, security, and automation across end-to-end financial AI operations.

The search of the literature presented the articles that comply with the inclusion criteria to have a wide range of blockchain-facilitated federated learning (FL) and privacy-preserving machine learning (PPML) applications, and in the financial systems, in particular. Some extensive surveys include Qammar (2022) that systematically overviews the securing of federated learning with blockchain technology, and deals with essential privacy and security issues in the context of distributed learning. On the same note, a more general survey of blockchain-based federated learning and data privacy is provided by Chhetri et al. (2023), with the authors identifying the continuously growing variety of decentralised data analytics systems and frameworks.

Although this is broad, the interplay of blockchain-enabled FL and explicit Know Your Customer (KYC) or identity attestation in financial systems has not been fully investigated. Most available research is focused not on identity verification per se, but on related financial use cases like fraud detection or credit risk assessment. As an example, the paper by Ahmed and Alabi (2024) is a systematic review of cryptocurrency fraud detection based on secure and scalable federated learning frameworks, based on blockchain, highlighting solutions to mitigate fraud with the help of decentralised learning, but without the comprehensive implementation of the KYC/AML (Anti-Money Laundering) compliance functionality. Other articles, such as Divya et al. (2025) and Bello et al. (2025), address blockchain-based KYC applications and AML compliance through the business lens, yet they have a tendency not to tie them to highly developed federated learning and PPML methods.

Architectural Patterns

Many of these studies point to architectural conventions, which entail permissioned or consortium blockchains to strike a balance between governance, trust, and performance in the context of many institutions. Controlled participation in the case of permissioned blockchains is essential and important in the financial situation where regulatory compliance and privacy are essential. Model update hashes or audit trails, or identity credential anchors, are often stored in immutable model ledgers and guarantee transparency and resistance to tampering as reported by Mahmood and Jusas (2022) and Chen et al. (2025).

Federated learning models mostly follow the horizontal FL, whereby the involved parties possess separate datasets on users but have common feature spaces. Vertical FL, the situation where the sets of the features are distributed between the institutions, is less popular but is also discussed in a growing body of work, such as Li et al. (2025), who introduce blockchain-federated learning models to assess supply chain credit risks with vertically partitioned data.

The use of smart contracts is a common motif, as it is used to guarantee policy adherence, automate the process of contribution verification, administer rewards, and hold people accountable. These types of programmable contracts form the basis of incentive schemes such as rewarding honest participation in tokens or reputation scores, as explored in such papers as Bello et al. (2025) and Sharma et al. (2025).

Privacy and Security Techniques

The techniques presented in the literature reviewed for preserving privacy are generally made of differential privacy, secure aggregation, homomorphic encryption, and zero-knowledge proofs. The implementation is both different and broad in the studies. As an example, Jia et al. (2024) discuss privacy-preserving schemes based on blockchain and multiparty secure computations, including attribute-based encryption to protect model updates in the course of collaborative training.

The main security threats are addressed, such as model poisoning, inference attack, free-riding and single points of failure. Hybrid blockchain-FL systems tend to suggest approaches to checking the integrity of updates in the model, screening out bad entries, and rewarding good behaviour, as described by Qammar et al. (2023) and Chen et al. (2025). Democratic methods include Proof-of-Learning consensus (Kejriwal et al., 2024) and decentralised forms of governance (Alsagheer et al., 2023), and help address the risks of distributed AI pipes.

Blockchain Roles and Identity Attestation

The main purpose of blockchain is often based on audit logging that cannot be modified: the history of model updates, the activity of participants, and compliance events, which can be traced and held accountable and are described in Kilroy et al. (2023) and Ridwan (2025). Participation and honest reporting are motivated by the application of reward and incentive schemes in the form of tokenisation schemes or reputation schemes, and also provide long-term cooperation between several parties (Bello et al., 2025; Sharma et al., 2025).

Nevertheless, more elaborate descriptions of the mechanisms of credential attestation and identity verification are less commonly elaborated. Although most frameworks explain how verifiable credentials may be issued and anchored on-chain, explicit integration of KYC and AML compliance functionality, e.g. credential revocation, selective disclosure, policy enforcement, and legal deanonymization, is frequently omitted or not described in some detail. The literature on privacy-safe KYC enforcement based on blockchain, such as Xiong et al. (2025) and Sak (2024), gives some information on how this can be applied, but none of them integrates this with federated learning and PPML at scale.

Regulatory and Compliance Features

Regulatory considerations are a common area that is considered but seldom taken to heart within system design and assessment. Other studies touch on the topic of data localisation, privacy regulations (including GDPR), auditability, and retention policies, which reflect fears in the context of cross-border financial data sharing (Bogucanin Volic, 2022; Lawal et al., 2025). Nonetheless, not many studies empirically estimate their systems in regulatory adversarial contexts how platforms react to regulator demands to access data or revoke credentials, which is an essential ability in practical KYC/AML compliance.

Empirical Evaluation and Performance

The majority of the studies give simulations or small-scale experiments, which prove that privacy-preserving mechanisms bring only reasonable losses to the model accuracy or performance. Such works focus on the trade-offs of privacy and utility, overhead in communication, blockchain transaction costs, latency, and throughput.

For instance, Baabdullah et al. (2024) and He et al. (2024) demonstrate that federated learning models based on blockchain ensure high levels of privacy but provide feasible accuracy in fraud classification and risk evaluation of finances. However, issues such as scalability, cost-efficiency, and real-time responsiveness are still persistent, which are reviewed by Kumar (2025) and Panda (2025).

Discussion of Key Findings

Trade-offs and Gaps

A synthesis of the reviewed literature indicates that there are a number of critical trade-offs and gaps that need to be filled in order to take blockchain-enabled federated learning (FL) to the next level of financial KYC systems.

Privacy and Utility

There is an underlying conflict between privacy and the utility of the models. When applied to preserve privacy, techniques that possess strong privacy guarantees, like the high amount of differential privacy noise, or computation-intensive cryptographic algorithms, including homomorphic encryption or zero-knowledge proof, typically cause lower model performance and higher latency or communication costs. This trade-off is well-documented in such works as Jia et al. (2024) and Baabdullah et al. (2024), who prove that there is a very thin line between protecting sensitive financial information and getting realistic performance indicators in the case of fraud detection or credit score-related applications.

Auditability and Privacy

The blockchain ledgers of immutable history enable strong auditability and traceability of the federated learning processes, which proves particularly useful in terms of compliance and transparency of the regulatory environment. But such unchangeability may come into conflict with privacy laws, including the General Data Protection Regulation (GDPR) of the EU, which codifies rights to data minimum and the right to erasure. Even many of the reviewed systems, such as the one discussed by Qammar et al. (2022) and Ridwan (2025), fail to resolve this tension completely, as they often lack mechanisms of selective data redaction or flexible policy execution that would meet the legal criteria without undermining auditability.

Scalability

One particular constraint that is shared by most of the frameworks is that they are mostly tested only in controlled and small-scale situations. The cost of computation and communication of federated learning, privacy-preserving machine learning (PPML) with blockchain is high, but in practice, financial networks consist of a large number of participants, with diverse capabilities, and data volumes. The limited literature, including Chen et al. (2025) and Kumar (2025), experimentally targets the validation of performance at scale, or overcomes latency and throughput issues in a production setting, which suggests that there is still a lack of scalability readiness.

Identity Attestation

Identity Attestation represents a device that can be applied to establish a new regulatory body. Even though identity verification and credential attestation are the core elements of financial compliance, the literature rarely captures the complexity of the real-world KYC and AML regulations. Dynamically updating policies, credential revocation, selective disclosure, and legal deanonymization under authorised conditions are the major characteristics that are hardly enforced and properly analysed. Both Xiong et al. (2025) and Bello et al. (2025) state that the regulatory and jurisdictional issues of data sharing across borders are still open. This loophole explains why there is a necessity for structures that not only facilitate strong identity management but are also flexible to changing legal conditions.

Governance and Incentives

An issue of governance, that is, who issues credentials, how the blockchain network is managed and policed, and the nature of incentives to ensure honest participation, is usually assumed rather than actually designed. These are recognised as open design challenges in many works, such as those by Alsagheer et al. (2023) or Sharma et al. (2025), which do not provide information about the governance models applied and the incentive alignment mechanisms. Trust, regulatory compliance and long-term sustainability highly depend on effective governance, particularly in decentralised financial ecosystems.

Implications for Financial Systems

This review demonstrates that a combination of federated learning (FL), privacy-preserving machine learning (PPML), and blockchain technology truly holds a lot of potential in improving the process of KYC and identity verification in financial systems. Nevertheless, when it comes to making a shift between research prototypes and tests and a real-life implementation, there are a few critical issues that need to be resolved in order to make those solutions viable, scalable, and compliant.

Configurable and Modular Architectures

Design of flexible and modular system architectures is one of the leading necessities. Banks and other financial institutions have a wide range of jurisdictions that have different regulatory frameworks, privacy statutes, and policies of the institution. KYC solutions should therefore permit dynamically configured privacy policies: e.g. the amount of privacy noise, or cryptography configuration, or other privacy requirements; and can flexibly adjust identity credential schemas to suit the needs of a particular region. This modularity ought to be applied to the governance policies too, so that institutions can tailor the access controls, the consent mechanisms, and the revocation protocols to their local compliance requirements and possibly to the organisation structures.

Optimization and Engineering of performance

The performance factor should be the most important one, considering that there is a computational and communication overhead caused by the integration of FL, PPML, and blockchain. The cryptographic methods need to be carefully chosen and streamlined to reduce the latency and consumption of resources, including lightweight homomorphic encryption, secure multiparty computation, or succinct zero-knowledge proofs. Furthermore, new solutions, such as off-chain data storage, sidechains, or layer-2 solutions, may be used to decrease the load on the primary blockchain, which, in turn, will improve the scalability and throughput. The protocol used in communication should be simplified to restrict the bandwidth consumption, particularly in the case of federation with a large number of participants, without affecting security or privacy.

Robust Governance Models

Clear governance frameworks are very important in regard to trust and accountability of financial systems. This involves the establishment of authoritative bodies that are to issue identity credentials and oversee their lifecycle, such as revocation of identity credentials and renewal. It is also paramount to have clear policies regarding deanonymization, i. e. when and how legal authorities may obtain access to anonymised data or cause selective disclosure in accordance with regulatory directives. Dispute resolution mechanisms, accountability of the participants and dealing with misbehaviour mechanisms should be formalised to provide integrity and collaboration among the consortium members or network participants.

User and Regulatory Transparency

Lastly, it is important to incorporate principles of transparency in the beginning. Privacy as a design approach needs to be incorporated in the development of a system, and user consent must be clearly obtained; privacy-protecting strategies must not be an afterthought. The selective disclosure tools ought to enable the users to provide only the minimum information necessary to meet the KYC requirements, which minimises the exposure to sensitive information. Further, the system should be designed to be audited to offer regulators verifiable records of compliance activities and credential utilisation without interfering with user confidentiality. The balance is needed, both to be under strict data protection standards like GDPR, and to be able to make correct oversight and risk control.

Recent Frameworks in Practice

Some of the recent studies provide a depiction of the major elements of a federated and privacy-friendly MLOps model using blockchain to facilitate KYC and AML compliance within financial systems. These models offer practical perspectives on privacy/regulatory/technical issues trade-offs in real-life scenarios, directly answering some of the gaps and trade-offs mentioned previously in this review.

Fed RD: Vertically Partitioned and Horizontally Partitioned Data Secure Training

Khan et al. (2024) aim to cover a very important practical issue in financial systems in which data is distributed vertically and horizontally across the institutions. Their Fed RD model incorporates secure multiparty computation and differential privacy to ensure data privacy is maintained throughout training a model.

This methodology is very applicable in KYC and AML, where the institutions can have different identity or transactional data characteristics. The fact that the framework offers formal privacy guarantees with acceptable trade-offs when it comes to accuracy accords in line with the empirical evaluation results found in the discussion above that highlight the need to keep privacy, model performance, and communication efficiency in tight control in complex financial settings. The Fed RD design also allows the optimisation of privacy-performance of cryptography and secure computation with the help of hybrid cryptography (Khan et al., 2024).

DPFedBank: Policy-Driven Federated Learning with Local Differential Privacy

He et al. (2024) suggest a federated learning architecture, called DPFedBank, that is specifically designed to address the privacy and security issues of financial institutions. To mitigate the risks that have been caused by malicious participants and external adversaries, DPFedBank combines the concept of local differential privacy (LDP) with cryptographic protection and an inbuilt policy layer.

The policy-oriented nature behind this framework is a direct response to the fact that the architectures must be modular and configurable to accommodate jurisdictional and institutional variability, as highlighted in the implications section. The minimal invasiveness of its privacy and utility decisions embodies the trade-off optimisation issues found earlier, such as showing by empirical analysis that it is possible to ensure privacy without having to highly sacrifice model quality or introduce undue communication cost (He et al., 2024). This strengthens the need to have privacy privacy-preserving design that does not impact operational performance, as is the case in most of the existing frameworks.

REGKYC: Regulated KYC on-Blockchain Fulfilment: Chemical-based Access Control

The REGKYC model created by Xiong et al. (2025) is an example of how blockchain could be applied to implement complicated, dynamic policy frameworks in KYC and AML systems and maintain privacy and regulatory responsibility. The design of REGKYC with the implementation of the Attribute-Based Access

Control (ABAC) system is specifically designed to meet the requirements of flexible governance models, as explained above, because the design allows KYC attributes to be verified flexibly, and the policy is enforced as part of a smart contract.

One of the contributions that REGKYC makes is that it supports the notion of authorised deanonymization, a feature that addresses the reality-regulation gap through permitting authorities to disclose the identity of wrongdoing parties under most circumstances, but not in privacy-upholding conditions. This characteristic addresses the severe dilemma of the irreconcilability of immutable audit logs and privacy regulations, such as the right to erasure, which has been observed in the context of privacy and auditability trade-offs. Using the immutability of blockchain and the cryptographic security of blockchain, REGKYC promotes the level of trust and transparency, which overcomes the issues of governance and incentive alignment mentioned above (Xiong et al., 2025).

Integrating These Frameworks with Broader Findings

Collectively, these structures reflect a viable development of achieving blockchain-enabled federated learning systems that are specific to financial KYC/AML. They point to the practical requirement of modular and policy-based architectures that can be adjusted to regulatory diversity and operational requirements, a fundamental suggestion of the preceding discussion.

The nature of the challenges that REGKYC seeks to fill, namely the approaches to governing and fulfilling regulatory obligations, has been recognised as a vulnerability in existing literature, with the suggested strategies that deanonymization is authorised by default and implemented using blockchain technology, to prove the necessity of transparent and legally supported mechanisms of attesting identities. The balance of privacy and utility of DPFedBank is a good example of how local differential privacy and efficient cryptographic primitives can address the overhead concerns, which justifies the need to optimise privacy-performance trade-offs. The emphasis of Fed RD on the manipulation of horizontally and vertically partitioned data is one of the blueprints in managing the actual distributed data situation in financial networks.

All these contributions are part of the larger response to pilot deployments involving real-world datasets and network conditions, the standardisation of identity credentials in support of selective disclosure and revocation, and governance frameworks with defined roles and authorities (Xiong et al., 2025; He et al., 2024; Khan et al., 2024). They accentuate that such multi-layered designs, including privacy, auditability, governance, and regulatory flexibility, are the only way federated and privacy-conscious MLOps systems can move beyond prototypes to trustworthy and deployable financial KYC system solutions.

Conclusion

This review has analysed the new intersection of federated learning (FL), privacy-preserving machine learning (PPML), and blockchain technologies when it comes to aiding Know Your Customer (KYC) procedures, identity verification, and fraud detection in financial systems. The literature at hand proves the technical viability of incorporating the technologies into one to improve the level of privacy, guarantee auditability, introduce incentive systems, and partially achieve decentralised identity attestation.

Nevertheless, a number of major gaps undermining practical implementation are still present despite the promising developments. These are difficulties in realising regulatory realism, and the structures will need to be more attuned to complex KYC/AML demands like revocation and selective disclosure of the credentials, which are dynamic. Scalability issues remain, and most of the proposed architectures have only been tested in small or simulated situations, and it is not clear how they will perform in the real world with large numbers of participants. Additional development is needed in creating and maintaining a sound identity credentialing system, such as governance, trust model and legality compliance. In addition, the trade-offs that exist between privacy and auditability are unresolved issues that require creative solutions to balance data security and regulatory disclosure.

These problems are critical in shifting the theoretical frameworks and pilot studies to scalable, secure, and legally acceptable systems that can be used to protect the identity of the user and financial integrity in decentralised settings. In the future, interdisciplinary cooperation is needed in order to address such gaps and enable the practical use of FL, PPML, and blockchain in the process of managing financial identity.

Recommendations

As the findings and discussion suggest, we offer the following recommendations to researchers, system developers, financial institutions and regulators who seek to design and implement federated and privacy-preserving MLOps systems specific to KYC/AML in financial systems:

Standards-Based and Flexible Identity Credential Systems

The identity credential systems should be constructed so as to enable such advanced functions as selective disclosure, where the users can only show the required attributes of compliance or verification. They ought to include a means of revocation of credentials, sound cryptographic evidence, and cross-border links with other financial institutions and jurisdictions. The need to deanonymize on the part of legal provisions in regulations should be incorporated in a wise manner. The involvement with already existing standard bodies or the contribution to the creation of new standards will help to get more of them adopted and to achieve interoperability.

Pilot Deployments in the Real World

In order to leave the theoretical approach and small-scale simulation, it is important to be involved in real-world pilot projects with financial institutions. These pilots are supposed to engage substantial participant populations, realistic identities and transaction data and work within realistic network and operational constraints. These deployments will allow for exhaustively measuring system performance, privacy leakage risks, latency, cost implications, and other usability considerations, which will be invaluably useful to refine and scale.

Secure Strong Governance and Trust Formulas

The governance structures should be made clear, and the roles and obligations of the credential issuers, verifiers, regulators, and the entities involved must be outlined. These models are meant to explain the legal authorities that are to conduct deanonymization and credential revocation, and dispute resolution. Consortium or permissioned blockchain networks would be a good idea to have a governance framework, where the predetermined roles and liabilities would increase the level of trust and accountability among the stakeholders.

Ensure Regulatory Alignment and Adaptability

Structures should also be flexible in nature so as to adapt to various and changing regulatory settings. This also involves adherence to data protection regulations, cross-border data transfer, standardised KYC attributes, and the process of conducting periodical updates to the policy. Legal and compliance professionals are important to engage in the system design stage so that technical capabilities are matched with legal requirements and that future requirements, like compliance with legislation, can be hedged.

Maximise Privacy-Performance Trade-off

The development and combination of efficient cryptographic primitives, reducing the number of computations, should be the main focus of research efforts. Some of the techniques to reduce performance bottlenecks are compressing model updates, cutting back on the quantity of communication rounds in federated learning, and hybrid designs utilising off-chain computation, sidechains, or trusted execution environments. Finding a compromise between privacy conservation and system performance is important towards viable implementation.

Privacy, Consent and Transparency of the User should take precedence.

The systems must be structured with a user-centric approach, including a clear consent mechanism that will educate users on how their identity data and attributes are processed. Such capabilities as selective sharing and data or credential revocation rights should be built in. Clear information about the use of data and privacy policies not only makes users trustful, but also provides compliance with the principles of regulatory legislation, like the data minimisation and user control requirements of GDPR.

Install Extensive Monitoring, Auditing and Accounting Systems

It is essential to integrate audit trails, logs, and accountability systems into smart contracts and blockchain elements. These characteristics enable regulators to check the adherence to policies and give clear attribution of duties among the participants. Open and unchangeable documentation ensures credibility in the system and promotes proper supervision, conflict management, and control.

Include Ethics and Fairness in mind

There must be continuous surveillance to identify and reduce biases in identity verification, risk-scoring or fraud detection models lest the specific groups are treated unfairly or discriminated against. The review and oversight processes must be ethical and should be part of the system deployment process to maintain fairness, equity, and social responsibility in the entire lifecycle of the KYC and AML solutions.

Contribution of Authors

All the authors contributed significantly to every section of the article.

Conflicts of Interest

There is no conflict of interest to declare.

References

Abdulrauf, H., Lawal, A. A., Mba, A. N. U., Ademola, C., Yusuf, Z. B., Babatayo, S., & Ayinde, I. (2025). Artificial Intelligence in Journalism: A Narrative Review of Opportunities, Challenges, Ethical Tensions, and Human-Machine Collaboration. American Journal of Arts and Human Science, 4(4), 5–18. https://doi.org/10.54536/ajahs.v4i4.5963

Abuzied, Y., Ghanem, M., Dawoud, F., Gamal, H., Soliman, E., Sharara, H., & Elbatt, T. (2024). A privacy-preserving federated learning framework for blockchain networks. Cluster Computing, 27(4), 3997-4014.

Adebowale, A. M., & Akinnagbe, O. B. (2023). Cross-platform financial data unification to strengthen compliance, fraud detection and risk controls. World J Adv Res Rev, 20(3), 2326-2343.

Ahmed, A. A., & Alabi, O. O. (2024). Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review. IEEE Access, 12, 102219-102241.

Ahnouch, M., Elaachak, L., & Ghadi, A. (2024). Optimizing DevOps and MLOps for Financial Institutions: Architecture and Compliance.

Aidoo, S., & Int Dip, A. M. L. (2025). The Role of Blockchain in AML Compliance: Potential Applications and Limitations.

Alsagheer, D., Xu, L., & Shi, W. (2023). Decentralized machine learning governance: Overview, opportunities, and challenges. IEEE Access, 11, 96718-96732.

Baabdullah, T., Alzahrani, A., Rawat, D. B., & Liu, C. (2024). Efficiency of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection (CCFD) Systems. Future Internet, 16(6), 196. https://doi.org/10.3390/fi16060196

Bello, A. A., Oduro, D. A., Manu, E. O., Bello, A. D., Leo, A. O., Ukatu, C. E., & Okika, N. (2025). Enhancing Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance using blockchain: A business analysis approach. Iconic Research and Engineering Journals, 8(9), 297-305.

Bogucanin Volic, S. (2022). Federated Learning in Autonomous Vehicles Setting-GDPR perspective.

Brahmandam, B. A. (2025). MLOps in Finance: Automating Compliance & Fraud Detection.

Chen, R., Dong, Y., Liu, Y., Fan, T., Li, D., Guan, Z., ... & Zhou, J. (2025, April). FLock: Robust and Privacy-Preserving Federated Learning based on Practical Blockchain State Channels. In Proceedings of the ACM on Web Conference 2025 (pp. 884-895).

Chhetri, B., Gopali, S., Olapojoye, R., Dehbashi, S., & Namin, A. S. (2023, June). A survey on blockchain-based federated learning and data privacy. In 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1311-1318). IEEE.

Divya, G., Sadanandha, N. V., Prudhvi, M., Kumar, B. A., & Rani, J. S. (2025). Enhancing Credit Allocation With Blockchain-Based KYC. International Journal of Computational Learning & Intelligence, 4(2), 440-447.

Fugkeaw, S. (2022). Enabling trust and privacy-preserving e-KYC system using blockchain. IEEE Access, 10, 49028-49039.

He, P., Lin, C., & Montoya, I. (2024). DPFedBank: Crafting a Privacy-Preserving Federated Learning Framework for Financial Institutions with Policy Pillars. arXiv preprint arXiv:2410.13753.

James, V., Adekola, P., Taofeek, A., & John, B. (2025). Privacy-Preserving Techniques in Blockchain KYC/CDD: Balancing Compliance and User Data Protection.

Jia, Y., Xiong, L., Fan, Y., Liang, W., Xiong, N., & Xiao, F. (2024). Blockchain-based privacy-preserving multi-tasks federated learning framework. Connection Science, 36(1), 2299103.

Kancherla, V. M. (2022). Enhancing MLOps with Blockchain: Decentralized Security for AI Pipelines. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3(2), 80-89.

Kejriwal, D., Pujari, T., & Goel, A. (2024). Blockchain-Enabled Trustworthy AI: Decentralized Federated Learning with Proof-of-Learning Consensus. Journal of Information Systems Engineering and Management, 10 (44). https://doi.org/10.52783/jisem.v10i44s.8694

Khan, M. S. I., Gupta, A., Seneviratne, O., & Patterson, S. (2024, October). Fed-RD: Privacy-preserving federated learning for financial crime detection. In 2024 IEEE Symposium on Computational Intelligence for Financial Engineering and Economics (CIFEr) (pp. 1-9). IEEE.

Kilroy, K., Riley, L., & Bhatta, D. (2023). Blockchain tethered AI: Trackable, traceable artificial intelligence and machine learning. " O'Reilly Media, Inc.".

Kumar, G. (2025). Architecting Scalable and Resilient Fintech Platforms with AI/ML Integration. Journal of Innovative Science and Research Technology, 10(4), 3073-3084.

Lawal, A. A., Abdulrauf, H., Yusuf, Z. B., Babatayo, S., & Ayinde, I. (2025). Risk fatigue and the infodemic: Understanding declining public responsiveness to health campaigns, mitigation strategies, and public health impact. Magna Scientia Advanced Research and Reviews, 2025, 14(2), 150-157. https://doi.org/10.30574/msarr.2025.14.2.0099

Li, C., Liu, J., Li, X., & Pei, B. (2025). A blockchain and federated learning based model for supply chain credit risk assessment. Advances in Intelligent Decision Technologies, 19(3), 201–217. https://soapubs.com/index.php/aidt/article/view/334

Mahmood, Z., & Jusas, V. (2022). Blockchain-Enabled: Multi-Layered Security Federated Learning Platform for Preserving Data Privacy. Electronics, 11(10), 1624. https://doi.org/10.3390/electronics11101624

Ngoupayou Limbepe, Z., Gai, K., & Yu, J. (2025). Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey. Blockchains, 3(1), 1. https://doi.org/10.3390/blockchains3010001

Oluwaferanmi, A. (2025). Smart Compliance: Opportunities and Pitfalls in Deploying AI-Blockchain Systems for Real-Time AML Monitoring.

Panda, S. (2025). Scalable Artificial Intelligence Systems: Cloud-Native, Edge-AI, MLOps, and Governance for Real-World Deployment. Deep Science Publishing.

Petrović, N. (2022). Model-Driven Approach to Blockchain-Enabled MLOps.

Qammar, A., Karim, A., Ning, H., & Ding, J. (2023). Securing federated learning with blockchain: a systematic literature review. Artificial intelligence review, 56(5), 3951–3985. https://doi.org/10.1007/s10462-022-10271-9

Ridwan, L. (2025). Intelligent Data Provenance Tracking: Blockchain-Enabled Trust Framework for MLOps Pipelines.

Sak, M. H. (2024). KYC/AML Technologies in Decentralized Finance (DeFi).

Sameera, K. M., Nicolazzo, S., Arazzi, M., Nocera, A., KA, R. R., Vinod, P., & Conti, M. (2024). Privacy-preserving in blockchain-based federated learning systems. Computer Communications, 222, 38-67.

Sharma, A., Chandrakar, P., Kumari, S., & Chen, C. M. (2025). FinSec: A Consortium Blockchain-Enabled Privacy-Preserving and Scalable Framework For Customer Data Protection In FinTech. Peer-to-Peer Networking and Applications, 18(3), 131.

Sunday, A. I., Jinadu, S. O., Alaka, E., Abiodun, K. D., & Peter-Anyebe, A. C. (2025). Leading the development of AI-Driven AML and Compliance Infrastructure to Modernize US Financial Crime Prevention System Across Digital and Traditional Platforms. International Journal for Multidisciplinary Research (IJFMR), 7 (4).

Suzuki, S., Yasuda, K., Fujie, N., & Abe, R. (2024). Current status of decentralized identifiers and verifiable credentials. Electronic Society for Social Informatics, 18(1), 42–58. https://www.jstage.jst.go.jp/article/essfr/18/1/18_42/_article

Umakor, M. F., Iheanyi, I., Ofurum, U. D., Ibecheozor, U. H. B., & Adeyefa, E. A. (2025). Federated learning for privacy-preserving fraud detection in digital banking: balancing algorithmic performance, privacy, and regulatory compliance. Iconic Res Eng J, 9(1), 215-31.

Xiong, X., Huth, M., & Knottenbelt, W. (2025). REGKYC: Supporting Privacy and Compliance Enforcement for KYC in Blockchains. Cryptology ePrint Archive.

Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. Journal of Information Security and Applications, 80, 103678.

Zhuk, A. (2025). Beyond the blockchain hype: addressing legal and regulatory challenges. SN Social Sciences, 5(2), 11.