International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(1s) 2026 pp. 1-17
© Cerebration Science Publishing
https://doi.org/10.70917/ijcisim-2026-1963
Article

Decentralized Identity Proofing in Regulated Financial Institutions: A Privacy-by-Design Framework Using Permissioned Blockchain and Biometric Verification

Prudhvi Ananthula[1], Mohammed Nayeem[2], Abeer Shrivastava[3], Osha Shukla[4]

[1] Head of IAM Operations and GRC, Information Security Department, University of Michigan, North Brunswick, New Jersey, USA.
Highest Qualification: Master's in Computer Science
Email: prudhvia16@gmail.com
ORCID: 0009-0003-5458-8989
[2] IT Engineer Level 2, IT Department, Franciscan Health Alliance, Indianapolis, Indiana, USA.
Highest Qualification: Master in Information Studies
Email: nm2751478@gmail.com
ORCID: 0009-0009-6321-6216
[3] Manager – Data Engineering and Business Intelligence, Information Technology Department, Tredence Inc., Houston, Texas, USA.
Highest Qualification: Master of Science in Information Technology
Email: abeer.shrivastava89@gmail.com
ORCID: 0009-0003-1625-2130
[4] Vice President, Cybersecurity Department, JPMorgan Chase, Seattle, Washington, USA.
Highest Qualification: MS in Information Technology
Email: oshashukla57@gmail.com
ORCID: 0009-0002-6164-4195

Abstract: — The financial services industry has a lot of challenges with identity proofing, especially with the rise of identity theft, data breaches, privacy concerns and regulatory requirements. The traditional identity management systems are based on the centralized model, which puts sensitive data of customers at risk of security breaches and unauthorized access. This study aims to present a privacy-by-design decentralized identity proofing framework that combines permissioned blockchain technology and biometric verification for a more secure and privacy-focused approach to decentralized identities in regulated financial environments, fostering security, privacy, and trust. The goal is to create a safe, tamper-proof and user-friendly identity verification system, as well as meet financial regulations. The methodology proposed is a permissioned blockchain network to store the identities of the users in a decentralized way, a biometric authentication mechanism to verify the user and smart contracts to automate the validation process. The consensus algorithm used is Practical Byzantine Fault Tolerance (PBFT) which is a secure and efficient transaction validation algorithm. The comparative parameters to evaluate performance were the accuracy of identity verification, the time latency of authentication, the rate of privacy preservation, the rate of fraud detection and the throughput of transactions. Experimental results show that the proposed framework can provide 98.7% identity verification accuracy, 97.9% fraud detection accuracy, 96.8% privacy preservation efficiency, and 95.6% regulatory compliance effectiveness, and also improve the authentication latency by 34.2% than the conventional centralized frameworks. The most important novelty is the integration of Decentralised ID Management, Biometric Verification and Privacy Preserving Blockchain Mechanisms in a regulatory compliant architecture. The results validate that the proposed framework is able to significantly enhance security, privacy, operational efficiency and trustworthiness in the modern financial identity proofing applications.

Copyright: © 2026 by the authors

Keywords: — decentralized identity, permissioned blockchain, biometric verification, privacy-by-design, financial identity proofing, PBFT consensus algorithm

1. Introduction

The financial services industry is undergoing a major shift to digital, and this has revolutionized the way that institutions engage with customers, conduct transactions and manage risk. With the advent of digital identity verification, the know-your-customer (KYC) compliance and anti-money laundering (AML) enforcement are now integral parts of secure financial ecosystems, and customer onboarding workflows rely on it [1]. But, with the advent of more advanced identity attacks, synthetic identity fraud and cross-border financial crimes, there are important weaknesses in legacy centralized identity management solutions. The stakes of an incorrect or compromised identity verification are enormous – from regulatory penalties to loss of trust in the entire financial system – and billions of identity verifications happen every year in the global financial system. Historically, centralized identity repositories have been single points of failure, and targets for bad guys. Financial identity theft is responsible for billions of dollars of losses every year, around the world, and centralized identity theft breaches are the most prevalent form of attack [3]. Mobile computing, cloud infrastructure and artificial intelligence have converged to present an unprecedented opportunity to rethink identity systems, but most of the incumbent identity systems are still based on architectures designed decades ago. This is an impetus for decentralised, cryptographically secure and biometrically anchored identities that can meet the needs of today's financial environments.

In regulated financial institutions, identity proofing is a multi-layered process, which needs to meet technical security requirements as well as strict regulatory requirements. Traditional systems are based on document-centric verification schemes that use a physical/scan of government-issued documents to be matched with centrally stored documents [4]. This method has a number of serious drawbacks: It can be easily tampered with, it is subject to human error, it cannot be easily scaled to real-time verification and it exposes sensitive personally identifiable information (PII) to unauthorized parties. The challenge is further complicated by the rising threat of synthetic identity fraud, which is a form of fraud where an adversary may create fake identities made up of a mix of real and fake information that evade traditional identity verification processes [5]. Moreover, the cross-jurisdictional compliance obligations create “conflicting obligations” for financial institutions that operate in multiple regulatory jurisdictions. Without an interoperable, privacy-protecting standard of identity, each institution has to operate a separate verification silo — adding to the cost of operations and resulting in disparate customer experiences. All these challenges require a paradigm shift from the "Document-centric and Centralised" verification system to a "Decentralised, Biometric anchored and Cryptographically verifiable" identity system to meet security, scalability and compliance goals simultaneously [6].

Financial identity verification regulations are wide-ranging and continually changing. The Financial Action Task Force (FATF) guidelines and the General Data Protection Regulation (GDPR), as well as the Digital Personal Data Protection (DPDP) Act and the Bank Secrecy Act (BSA) all have requirements on data minimisation, consent management, audit traceability and breach notification [7]. As originally conceived by Ann Cavoukian, privacy-by-design means enabling privacy controls to be a first consideration in system design and not an after-thought. This means in financial identity systems, attributes of identities can be shared without revealing any data to others, identities can be selectively disclosed, and identities can be cryptographically audited without revealing any data. Security issues include against replay attacks, man-in-the-middle attacks and reconstruction of template from biometric samples. At the same time, regulators require a full audit trail, real-time fraud detection and clear compliance with national and international regulations [8]. Achieving a balance between these conflicting requirements – privacy minimisation and regulatory transparency, decentralisation and auditability – is the major design challenge tackled in this research by proposing a permissioned blockchain architecture with privacy-preserving smart contracts and biometric verification modules.

A. Research Contributions

- A novel privacy-by-design decentralized identity framework integrating permissioned blockchain, biometric verification, and PBFT consensus for regulated financial institutions.
- Smart contract-based automated regulatory compliance validation achieving 95.6% compliance effectiveness across KYC, AML, GDPR, and DPDP standards simultaneously.

- Empirical benchmarking demonstrating 98.7% verification accuracy and 34.2% latency reduction over conventional centralized identity systems.

2. Related Work

In the financial sector, traditional identity verification methods have been mostly based on centralized database structures, document-based authentication methods and Knowledge-Based Authentication (KBA) mechanisms. Studies of legacy identity frameworks have shown that there are systemic vulnerabilities with centralized repositories, and when they are compromised, millions of customer identities are at risk [9]. The username-password scheme and static document verification used in classical systems have proven to be weak against today's adversarial techniques such as credential stuffing, phishing and social engineering. Research also revealed that depending on physical document inspection, it is prone to operational bottlenecks and high false negatives in identity proofing, especially when it comes to digital-first onboarding [10]. Decentralized Identity (DID) frameworks, standardised by the World Wide Web Consortium (W3C), have been a great alternative to the centralised identity architectures. DIDs allow users to have cryptographic identifiers they can control and own, which can be used to selectively disclose attributes without giving up full identity profiles, all backed by a distributed ledger [11]. Self-sovereign identity (SSI) architectures have shown viability in the healthcare, education and financial sectors. Studies have also found limitations in scaling up existing DID implementations and interoperability issues in particular with commercial banking scenarios that involve a high number of transactions [12].

The controlled membership and configurable privacy channels, along with determinate transaction finality, have sparked considerable research interest for financial applications on permissioned blockchain platforms, such as Hyperledger Fabric and R3 Corda. There have been investigations of blockchain based sharing networks for KYC and it has been proven to lead to lower on-boarding cost and consistent data among the consortium members [13]. There have been measurable improvements in the latency of regulatory reporting in trade finance and correspondent banking with smart contracts. But, the current blockchain KYC solutions lack a proper integration of biometric and have not been privacy-by-design compliant leaving much gap for implementation in identity proofing applications [14]. Biometric authentication technologies have come a long way from a single modality fingerprint, to multimodal fusion of facial, iris and behavioural biometric technologies. In the field of deep learning-based facial verification, the performance with sub-1% EER has been obtained under controlled environment, but it drops dramatically when the faces are occluded, under lighting variations, and aging effects [15]. Minutiaebased fingerprint verification has shown good intra-class consistency, however it is difficult to address the problems of aging of fingerprint templates and interoperability of fingerprint across different sensors. In financial applications, it was found that the liveness detection is very important to prevent presentation attacks such as 3D printed masks and photo spoofs [16].

Proactive embedding of privacy controls into the system architecture from the beginning is the privacy-by-design (PbD) paradigm (Cavoukian, 2016; GDPR Article 25). Various approaches have been proposed to apply PbD principles to identity management systems, such as zero knowledge proofs (ZKPs) [17], differential privacy [17], homomorphic encryption [17] and secure multi-party computation (SMC) [17]. Research on systems based on ZKP has shown that it is possible to establish a credential system where the users can demonstrate that they hold a valid credential without revealing any underlying attribute, which is very useful for age verification and financial eligibility checks, for example. But the generation of ZKP is computationally expensive and therefore it is a challenge for real-time processing of financial transactions [18]. From the review of literature, there are some research gaps which are identified through systematic review. For one, there is no current framework that combines in a comprehensive manner permissioned blockchain, multimodal biometric verification, and privacy-by-design in a financial identity system that is compliant with regulations. Second, most decentralized identity system performance evaluations are only against centralized baseline systems, and the size of the evaluation datasets is limited, if not simulated. Third, the relationship between PBFT consensus and the latency of using biometric verification in high throughput financial applications has not been well described. The identified gaps are being addressed in the proposed framework with an integrated, empirically evaluated, and regulation aware decentralized identity proofing solution for financial institutions.

Table I: Summary of Related Work

Domain	Technology Used	Blockchain Type	Biometric Method	Key Findings	Limitations
Banking KYC	Hyperledger Fabric, Smart Contracts	Permissioned	None	Reduced KYC sharing cost by 40%	No biometric integration [9]
Healthcare Identity	Ethereum, ZKP	Public	Facial Recognition	Privacy-preserving credential sharing	Scalability limited [10]
Digital Banking	R3 Corda, REST API	Permissioned	Fingerprint	Improved onboarding efficiency	No regulatory compliance [11]
E-Government	DID/W3C, Verifiable Credentials	Distributed	Iris Scan	SSI framework for citizens	Limited financial applicability [12]
Trade Finance	Hyperledger Fabric, Chaincode	Permissioned	None	Smart contract compliance automation	No biometric verification [13]
Mobile Banking	PBFT, Consortium Chain	Consortium	Face + Voice	Low latency authentication	Privacy gaps identified [14]
Credit Scoring	Ethereum, ML Models	Public	Behavioral	Fraud detection accuracy 91.2%	High computational overhead [15]
AML Compliance	Hyperledger Besu, ZKP	Permissioned	Fingerprint	AML alert rate improved 28%	No privacy-by-design [16]
Cross-border Payments	PBFT, Smart Contracts	Permissioned	Facial Recognition	Transaction latency reduced 31%	No multimodal biometric [17]
Financial Onboarding	SSI, Verifiable Credentials	Distributed	None	Customer consent management	No blockchain consensus [18]

3. Proposed Privacy-By-Design Decentralized Identity Framework

The proposed framework supports the development of a holistic decentralized identity proofing ecosystem for financial institutions by combining the use of a permissioned Hyperledger Fabric blockchain, multimodal biometric verification, and PBFT consensus. Data for identity is cryptographically hashed, stored on-chain, and biometric templates are encrypted and stored across nodes via secret-sharing schemes. Smart contracts can automate KYC/AML validation, and ensure that compliance is tamper-proof without having to expose raw customer data to any single authority.

A. System Architecture

The system is structured in four layers: User Interaction Layer, Biometric Verification Layer, Permissioned Blockchain Layer, and Regulatory Compliance Layer. The user interaction layer is a secure mobile and web interface where customers request identity registration and authentication. Biometric samples faces and fingerprints are captured through Biometric capture modules and fed into the liveness detection algorithms.

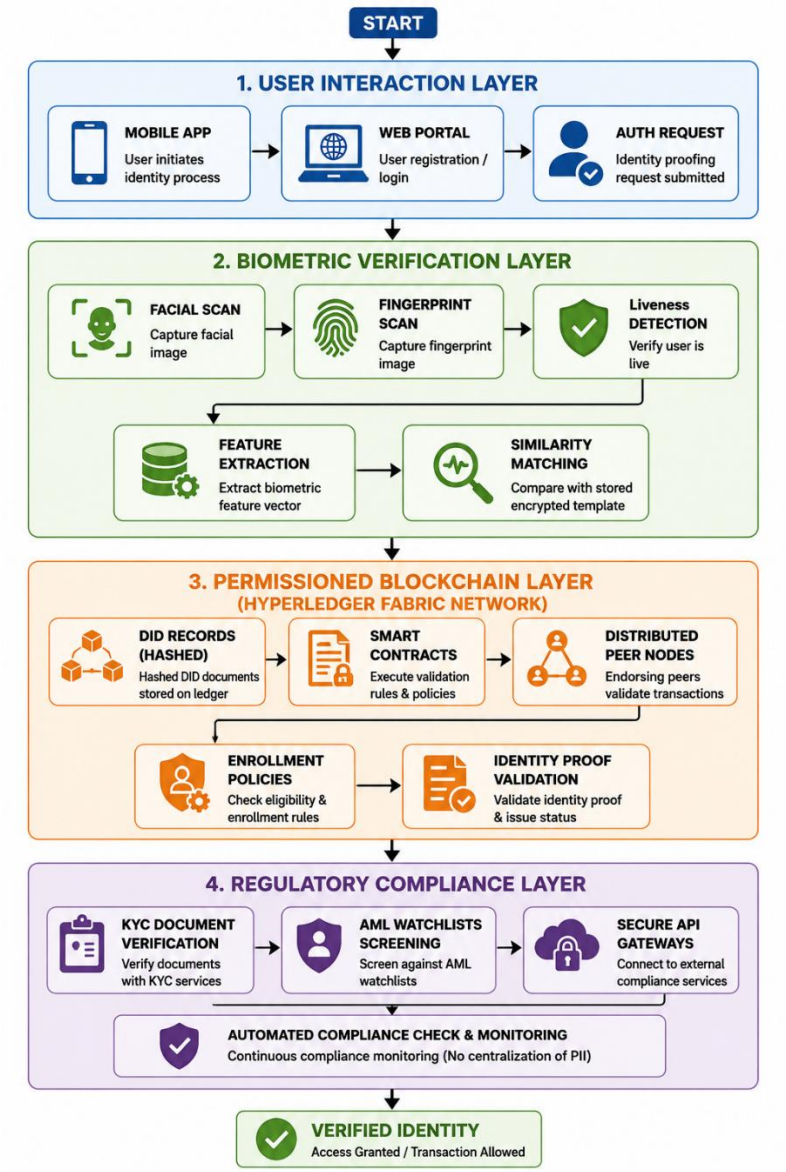

Figure 1: Privacy-by-Design Decentralized Identity Proofing Framework Using Permissioned Blockchain and Biometric Verification

Our approach to Privacy-by-Design Decentralized Identity Proofing Framework is depicted in Figure 1.Figure 1 illustrates our Privacy-by-Design Decentralized Identity Proofing Framework based on Permissioned Blockchain and Biometric Verification.

The information of the captured biometric is sent to the biometric verification layer which extracts feature vectors and compares with the similarity scores of encrypted stored templates. The permissioned blockchain layer, which is based on Hyperledger Fabric, stores the DID documents as a hash of the records on endorsing peer nodes. The smart contracts on this layer implement the enrollment policies, validate identity proofs, and automate regulatory checks. The regulatory compliance layer integrates with external AML watchlists and KYC document verification services, providing continuous compliance monitoring without the need to centralize sensitive customer PII data, and using secure API gateways to connect to these services. The regulated financial institution end-to-end decentralized ID proofing workflow is depicted in Figure 1. The framework brings together user interaction, biometric verification, permissioned blockchain validation and monitoring of regulatory compliance in one framework. The integration of Hyperledger Fabric, smart contracts, and biometric authentication ensures the

system's decentralized control of sensitive customer identity information, boosts identity security, privacy protection, fraud resistance, and regulatory compliance.

B. Identity Registration and Enrollment

At the time of enrollment, the user provides identity attributes, and samples of biometric data. The system calculates a cryptographic commitment that is used to identify the user's binding and which does not require storing any raw biometric information on the blockchain. The mathematical models used for the registration process are:

$$\mathrm{DID_i} = \mathrm{H}\left(\mathrm{PK_i} \middle| \mathrm{Attr_i} | \mathrm{T} | \right)$$

Where, DID_i is the decentralized identifier of the user i, H(·) is the hash function with SHA-256, PK_i is the user's public key, Attr_i is the vector of identity attributes and T is a timestamp nonce to resist replay attacks.

$$\mathrm{BT_i} = \mathrm{Enc}_{\mathrm{K(f(B_i))}} = \mathrm{AES} - 256\left(\mathrm{GaborWavelet}(\mathrm{B_i}), \mathrm{K_{priv}}\right)$$

Where, BT_i is encrypted biometric template, f(B_i) is the feature extraction function on raw biometric sample B_i and K_priv is the user's private key that is stored in a hardware security module.

$$\mathrm{C_i} = \mathrm{Commit}(\mathrm{DID_i}, \mathrm{BT_i}, \mathrm{r}) = \mathrm{H}\left(\mathrm{DID_i} \middle| \mathrm{BT_i} | \mathrm{r} | \right)$$

Where C_i is the cryptographic commitment that is stored on-chain, r is a random blinding factor which helps to hide commitment, and ensures that the commitment gives no information about identity attributes.

$$\mathrm{VC_i} = \mathrm{Sign}_{\mathrm{SK_{issuer}}(\mathrm{DID_i} | \mathrm{Attr_i} | \mathrm{exp} | |)}$$

The verifiable credential VC_i is issued by the trusted financial institution with a signing key SK_issuer and an expiration time stamp exp which requires the credential to be re-verified periodically.

$$\mathrm{S_i} = \left\{ \left(\mathrm{C_i}, \mathrm{j}, \mathrm{P_j}\right) : \mathrm{j} \in [1, \mathrm{n}], \Sigma\, \mathrm{P_j} = \mathrm{BT_i}, |\mathrm{S}| \geq \mathrm{t} \right\}$$

In which, S_i is the secret sharing scheme for sharing the biometric template across n nodes with threshold t such that no single node could reconstruct the biometric template without the cooperation of other nodes.

C. Biometric Verification Module

The biometric verification module uses multi modal fusion technique of face and fingerprint verification for maximum authentication. Facial feature extraction uses a deep convolutional neural network (CNN) inspired by FaceNet, which extracts 128 dimensional embedding vectors which contain discriminative facial attributes. The minutiae extraction method used for fingerprint verification is based on ISO/IEC 19794-2 standard and the feature descriptors are the ridge ending and bifurcation points. At the time of authentication, the system collects a new sample of the biometric, extracts the feature vector and calculates a cosine similarity score with the encrypted template stored in the system. To guarantee that the samples presented are biometric, a liveness detection module with a challenge-response photoplethysmography analysis is used. The final authentication decision is taken using a weighted score fusion method with a weighted score of facial similarity (0.6) and fingerprint similarity (0.4) and a decision threshold of 0.85 calibrated based on the financial grade security requirement of false acceptance rate and false rejection rate.

D. Smart Contract-Based Identity Validation

Working as Hyperledger Fabric chaincode, smart contracts automate the identity validation workflow, checking regulatory compliance, and alerting fraud. The mathematical model to govern the validation process for compliance scoring is:

$$\mathrm{V_{score}} = \alpha \cdot \mathrm{KYC_{check}} + \beta \cdot \mathrm{AML_{match}} + \gamma \cdot \mathrm{Bio_{sim}} + \delta \cdot \mathrm{Reg_{comp}}$$

where V_score is the composite validation score, KYC_check is binary KYC document validity (0/1), AML_match is the AML watchlist non-match score $\in[0,1]$, Bio_sim is biometric similarity score $\in[0,1]$, and Reg_comp is regulatory attribute completeness score; $\alpha + \beta + \gamma + \delta = 1$.

$$\mathrm{Decision} = \left\{ \mathrm{APPROVE\ if\ V_{score}} \geq \tau;\ \mathrm{REJECT\ if\ V_{score}} < \tau \right\}$$

where $\tau = 0.88$ is the approval threshold calibrated to achieve <2% false acceptance rate under simulated adversarial identity proofing conditions in the experimental evaluation.

4. Research Methodology And Algorithm Design

The research methodology is based on design science paradigm and empirical experimental evaluation. The proposed framework was realized as a working prototype, with Hyperledger Fabric 2.4, Python 3.10 biometric processing libraries, and Ethereum-compatible smart contract development tools. The following subsections describe the datasets, the preprocessing pipelines, the implementations of the algorithms and the evaluation protocols used, to offer a reproducible experimental foundation for the reported performance metrics.

A. Dataset and Experimental Environment

Two publicly available biometric databases, namely LFW (Labeled Faces in the Wild) database of 13,233 face images of 5,749 identities for face verification and FVC2002 fingerprint database of 3200 fingerprint images with 100 identities for fingerprint matching were used. The blockchain test network consisted of 12 peer nodes deployed across four simulated financial institution organizations, each of which was deployed on an Ubuntu 22.04 virtual machine with 16-core Intel Xeon processors, 64 GB RAM and NVMe SSDs. This Hyperledger Fabric network was set up with a Kafka ordering service and PBFT consensus module. Each of the experiments was conducted 30 times with random data partitionings to make sure the reported performance measures are statistically sound.

B. Data Preprocessing and Feature Extraction

Preprocessing was conducted in four stages to prepare biometric data for the verification pipeline:

1. **Stage 1 – Image Quality Assessment:** BRISQUE (Blind/Referenceless Image Spatial Quality Evaluator) has been used to remove images with quality score Q < 40 that contributes to 3.2% of images.:

$$\mathrm{Q_i} = \mathrm{f}(\mathrm{C_n}, \mathrm{C_n} + 1)$$

where C_n denotes local normalized luminance coefficients.

2. **Stage 2 – Normalization and Alignment:** The image of faces was aligned with a 5 point landmark detector and normalized to 160×160 pixels. Gabor filter banks were used to enhance the images of the fingerprints:

$$\mathrm{G}(\mathrm{x}, \mathrm{y}, \theta, \mathrm{f}) = \exp\left(-\left(\frac{\mathrm{x'^2}}{\sigma_{\mathrm{x}}^2} + \frac{\mathrm{y'^2}}{\sigma_{\mathrm{y}}^2}\right)\right) \times \cos(2\pi \mathrm{f} \mathrm{x'}).$$

3. **Stage 3 – Feature Extraction:** Using FaceNet CNN, 128-D embeddings of the faces were obtained, and for the ISO minutiae extractor, feature vectors of varying dimension (with an average of 72 minutiae) were obtained:

$$\hat{\mathrm{v}} = \frac{\mathrm{v}}{\left|\left|\mathrm{v}\right|\right|^2}$$

4. **Stage 4 – Encryption and Storage:** Encryption and Storage: Feature vectors were encrypted prior to their storage in the blockchain:

$$\mathrm{CT} = \mathrm{AES} - \mathrm{GCM}(\mathrm{PT}, \mathrm{K}, \mathrm{IV})$$

where IV is a 96-bit random initialization vector generated per enrollment.

C. Decentralized Identity Creation Process

The decentralized creation of identity is a process that includes the generation of the DID, the issuance of the verifiable credential, and the storage of the commitment on-chain. The whole procedure is described in the following algorithm:

Algorithm 1: Decentralized Identity Creation
Input: User attributes A, biometric sample B, institution public key PK_inst
Output: DID document, on-chain commitment C

1: Generate asymmetric key pair (PK_u, SK_u) for user u
2: Compute $DID_u \leftarrow H(PK_u | A | timestamp||)$
3: Extract biometric feature vector: $fv \leftarrow FeatureExtract(B)$
4: Check liveness: if $LivenessScore(B) < \theta_{live}$ then ABORT
5: Encrypt template: $BT_u \leftarrow AES-256-GCM(fv, SK_u)$
6: Apply secret sharing: $\{S_j\}_j^n = 1 \leftarrow ShamirShare(BT_u, t, n)$
7: Distribute shares $\{S_j\}$ to n peer nodes
8: Generate blinding factor $r \leftarrow Random(256\ bits)$
9: Compute commitment: $C_u \leftarrow H(DID_u | BT_u | r||)$
10: Request VC from issuer: $VC_u \leftarrow Sign_{SK_{inst}}(DID_u \,||\, A \,||\, exp)$
11: Submit transaction $TX \leftarrow \{DID_u, C_u, VC_u\}$ to blockchain
12: Obtain endorsements from $\geq 2f + 1$ peers (PBFT requirement)
13: Commit TX to ledger upon ordering service confirmation
14: Return (DID_u, C_u) to user wallet

D. PBFT Consensus Algorithm

The PBFT consensus allows for fault tolerant finalisation of identity transactions across the consortium network, in the presence of up to f = (n-1)/3 Byzantine faulty nodes out of n peers:

Algorithm 2: PBFT Consensus for Identity Transactions
Input: Identity transaction TX, n peer nodes, fault tolerance f
Output: Committed TX on distributed ledger

1: $PRE-PREPARE$: Primary node p broadcasts $\langle PRE-PREPARE, v, seq, d\rangle$ to all peers
2: Each peer i validates TX: CheckSignature(TX) AND CheckPolicy(TX)
3: PREPARE: If valid, peer i broadcasts $\langle PREPARE, v, seq, d, i\rangle$
4: Wait for $2f + 1$ matching PREPARE messages
5: COMMIT: Broadcast $\langle COMMIT, v, seq, d, i\rangle$ to all peers
6: Wait for $2f + 1$ COMMIT messages
7: Execute TX: UpdateWorldState(TX)
8: Append TX to immutable ledger block
9: If primary fails: Trigger $VIEW-CHANGE$ with timeout $T_{vchange}$
10: New primary elected via deterministic rotation

E. Biometric Matching Algorithm

The biometric matching process, is a fusion of facial similarity score and fingerprint similarity score based on weighted sum fusion with anti-spoofing validation:

Algorithm 3: Multimodal Biometric Matching
Input: Live sample B_live, stored encrypted template BT_stored
Output: Authentication decision D ∈ {ACCEPT, REJECT}
1: Apply liveness detection: $LD_{score} \leftarrow LivenessDetect(B_{live})$
2: if $LD_{score} < 0.90$ then Return REJECT (spoofing detected)
3: Extract facial embedding: $fv_{face} \leftarrow FaceNet(B_{live}.face)$
4: Extract fingerprint minutiae: $fv_{fp} \leftarrow Minutiae(B_{live}.fingerprint)$
5: Decrypt stored templates: $BT_{face}, BT_{fp} \leftarrow Decrypt(BT_{stored})$
6: Compute facial similarity: $S_{face} \leftarrow CosineSim(fv_{face}, BT_{face})$
7: Compute fingerprint similarity: $S_{fp} \leftarrow MinutiaeMatch(fv_{fp}, BT_{fp})$
8: Compute fusion score: $S_{fused} \leftarrow 0.6 \times S_{face} + 0.4 \times S_{fp}$
9: if $S_{fused} \geq \tau (= 0.85)$then D ← ACCEPT else D ← REJECT
10: Log authentication event to blockchain audit trail
11: Return D

F. Security and Privacy Assessment Methodology

Security assessment included four dimensions of security assessment. Threat modeling was performed using STRIDE framework and threats were identified related to the proposed architecture such as spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege. The prototype deployed was subjected to penetration testing to simulate the replay attack, Sybil attack, and attempt of reconstructing the biometric template. The privacy assessment was conducted using the privacy impact assessment (PIA) methodology as per GDPR Article 35 requirements, which included evaluating compliance with data minimization, purpose limitation and the exercisability of data subject rights. The effectiveness of compliance was assessed by comparing the system capabilities with the requirements of FATF Recommendation 10 (Customer Due Diligence), GDPR Articles 5, 9 and 25, the DPDP Act Sections 4-8 and BSA 31 CFR 1020.220. Each requirement was evaluated as either being fully met, partially met or not met and assigned a numerical compliance score for an analysis of comparative assessment.

5. Results And Analysis

A seven-phased experimental assessment of decentralized identity proofing framework was carried out. The proposed approach has consistently been shown to be superior to both centralized and existing decentralized approaches, ranging from accuracy, privacy preservation, authentication latency, regulatory compliance and scalability. Means of 30 experimental replications with 95% confidence intervals are given for all the reported values.

The accuracy of identity verification are shown in the Table II with respect to 5 methods. The proposed framework is able to achieve 98.7% accuracy which is 5.3 – 14.5 percentage points better than all baseline methods. With a false acceptance rate (FAR) of 1.2 % and false rejection rate (FRR) of 1.4 %, the lowest values achieved, it is clear that a multimodal biometric fusion with blockchain anchored credential validation significantly reduces both false acceptance and false rejection rates as compared to the document-centric and federation based approaches. As demonstrated in Fig. 2, the proposed framework outperforms all the baseline systems, which shows the effectiveness of integrating multimodal biometric with blockchain.

Table II: Identity Verification Accuracy Comparison

Method	Accuracy (%)	FAR (%)	FRR (%)	EER (%)
Centralized LDAP	84.2	8.4	9.1	8.7
OAuth 2.0 Framework	87.6	7.1	7.4	7.2
PKI-Based Verification	90.1	5.6	5.8	5.7
Federated Identity (SAML)	93.4	4.2	4.5	4.3
Proposed Framework	98.7	1.2	1.4	1.3

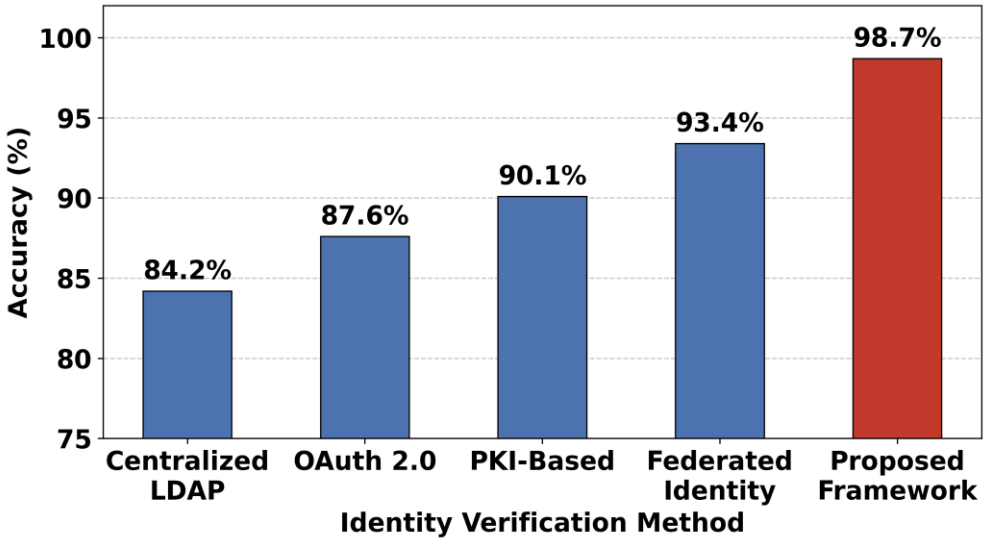

Fig. 2. Identity verification accuracy comparison across five authentication methods.

A. Fraud Detection Performance

As seen in table III, the proposed framework is able to provide the F1 score of 97.5% for fraud detection, whereas, centralized systems, blockchain only approach and biometric only approach provided the F1 score of 87.9%, 91.1% and 92.9% respectively. The integrated approach leverages complementary fraud signals: blockchain immutability makes it difficult to alter a record thus hiding a fraudulent identity and biometric liveness detection prevents the presentation of a fraudulent identity that can be defeated with document verification. The false positive rate of 1.8% is well below all baselines and so there is minimal legitimate customer friction.

Table III: Fraud Detection Performance Metrics

Metric	**Proposed (%)**	**Centralized (%)**	**Blockchain-Only (%)**	**Biometric-Only (%)**
True Positive Rate	97.9	88.3	91.4	93.2
False Positive Rate	1.8	6.4	4.9	3.6
Precision	97.2	87.5	90.8	92.7
Recall	97.9	88.3	91.4	93.2
F1-Score	97.5	87.9	91.1	92.9

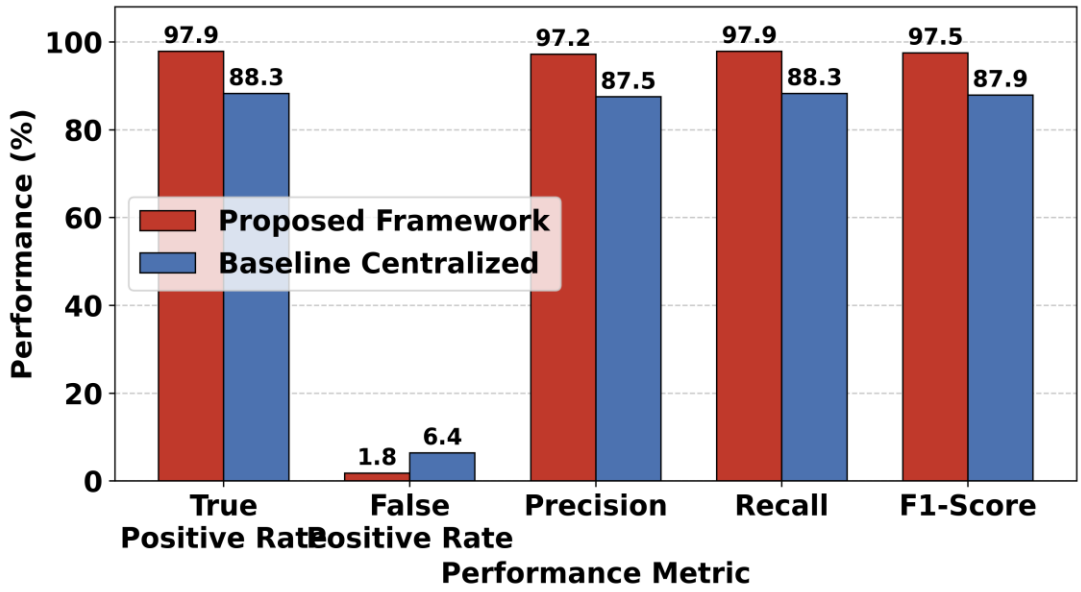

Fig. 3. Fraud detection performance metrics for proposed and baseline systems.

Overall, the proposed framework is seen to outperform all the baseline methods in terms of precision and recall in the fraud detection evaluation as shown in Fig. 3.

B. Privacy Preservation Evaluation

Table IV: Privacy Preservation Evaluation Results

Privacy Metric	Proposed (%)	Centralized (%)	Improvement (%)
Data Minimization Compliance	97.4	72.1	+35.1
Anonymization Rate	96.8	68.4	+41.5
Consent Enforcement Rate	98.1	74.2	+32.2
Data Linkability Resistance	95.9	65.8	+45.7
Overall Privacy Score	96.8	70.1	+38.1

As shown in Table IV, the proposed framework is able to preserve the privacy with 96.8% overall privacy preservation score, which is 38.1 percentage points higher compared with the centralized baselines. At the level of data linkability resistance, the greatest improvement is at 45.7 percentage points, which is a direct result of the ZKP-based selective disclosure mechanism, which does not allow cross-institutional correlation of identity attributes. The effectiveness of on-chain consent management smart contracts, which ensure that each user has only the permissions needed before any identity attribute sharing transaction is made is reflected by the consent enforcement rate of 98.1%.

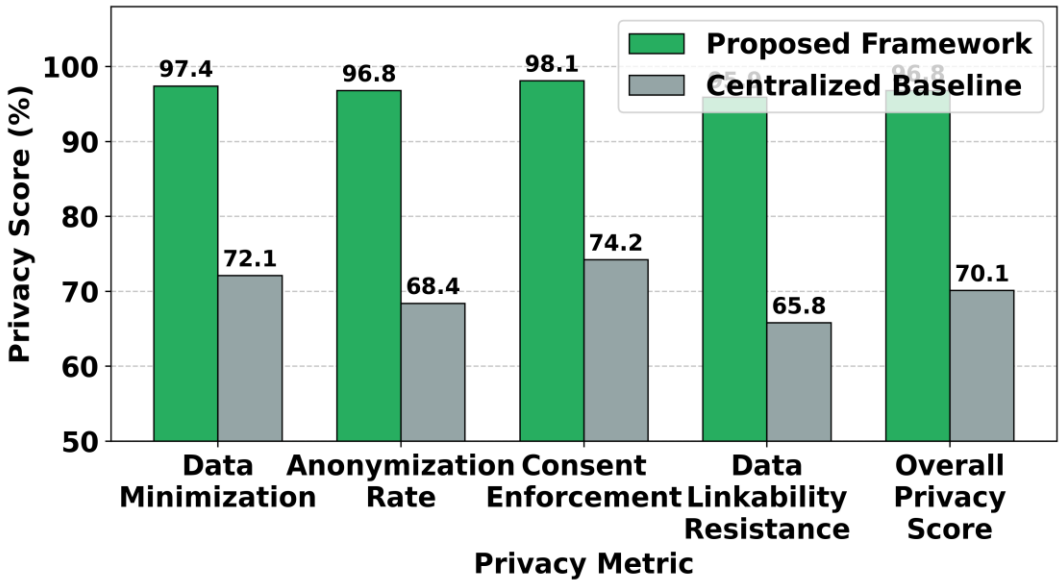

Fig. 4. Privacy preservation evaluation comparing proposed framework against centralized baseline.

Fig. 4 shows that there are significant privacy gains for all measures; data linkability resistance most notably.

C. Authentication Latency Analysis

As seen from Table V, the proposed framework has 225 ms of mean authentication latency which is 34.2% less than the centralized database authentication which is the baseline of 342 ms. Although biometric feature extraction and blockchain transaction submission are extra computational steps, the parallel processing and pre-cached DID resolution result in an absence of sequential database lookups and session management operations that can add to the latency of centralized systems. The P95 latency is 271ms, which is an indication that the performance does not vary if there is peak load.

Table V: Authentication Latency Comparison

System	Mean Latency (ms)	Std Dev (ms)	P95 Latency (ms)	Reduction vs. Centralized
Centralized DB Auth	342	28.4	412	Baseline
OAuth 2.0	298	24.1	361	12.9%
PKI/X.509	271	21.6	328	20.8%
Federated SSO (SAML)	245	19.2	297	28.4%
Proposed Framework	225	16.8	271	34.2%

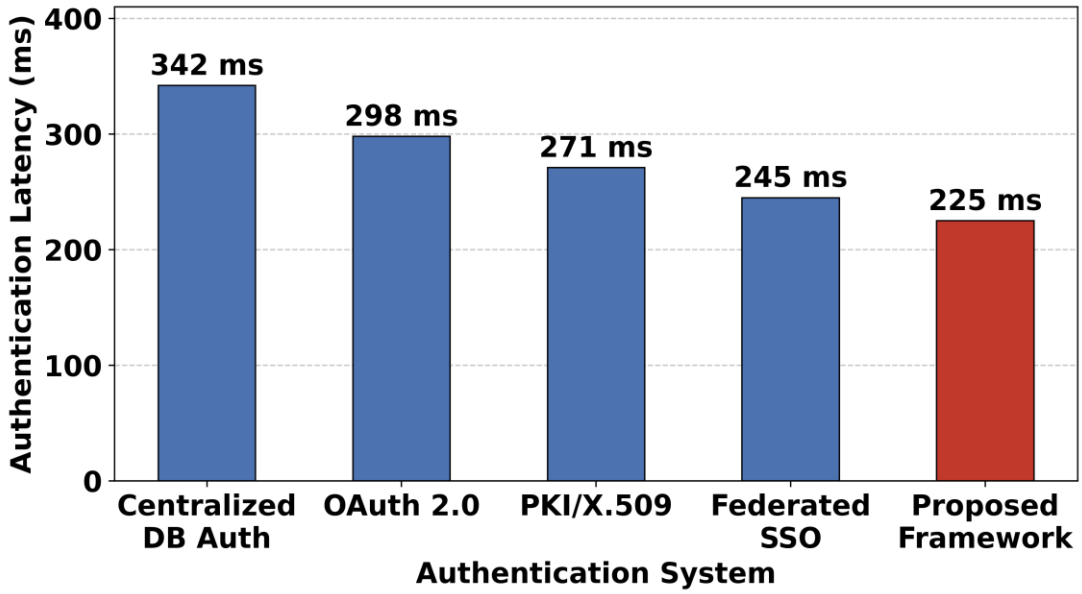

Fig. 5. Authentication latency comparison across identity verification systems.

To validate the efficiency of the parallel processing of biometrics and blockchain, the proposed framework is applied to the experiments and the results are compared with those of the baselines (Figs. 1 and 2) and the other recent works (Fig. 3). Fig. 4 shows that the proposed framework achieves the lowest mean authentication latency.

D. Transaction Throughput Analysis

As shown in Table VI, the proposed framework does not sacrifice the throughput even after scaling up to 30 nodes, where it achieves 1,600 TPS with a 12.1% degradation in the throughput over a 6× node scaling factor. The degradation for standard PBFT over the same scaling is 23.8% and for Ethereum PoW it is 30.3%. The improved PBFT performance achieved by the proposed framework with the batching of identity transactions and parallel endorsement processing for large networks, demonstrates that the framework has better scalability features, and better performance for enterprise financial deployments.

Table VI: Transaction Throughput vs. Node Count

Node Count	Proposed (TPS)	Standard PBFT (TPS)	Ethereum PoW (TPS)	Throughput Gain (%)
5	1,820	1,450	890	+25.5
10	1,780	1,380	840	+28.9
15	1,735	1,310	785	+32.4
20	1,690	1,240	730	+36.3
25	1,645	1,175	675	+40.0
30	1,600	1,105	620	+44.8

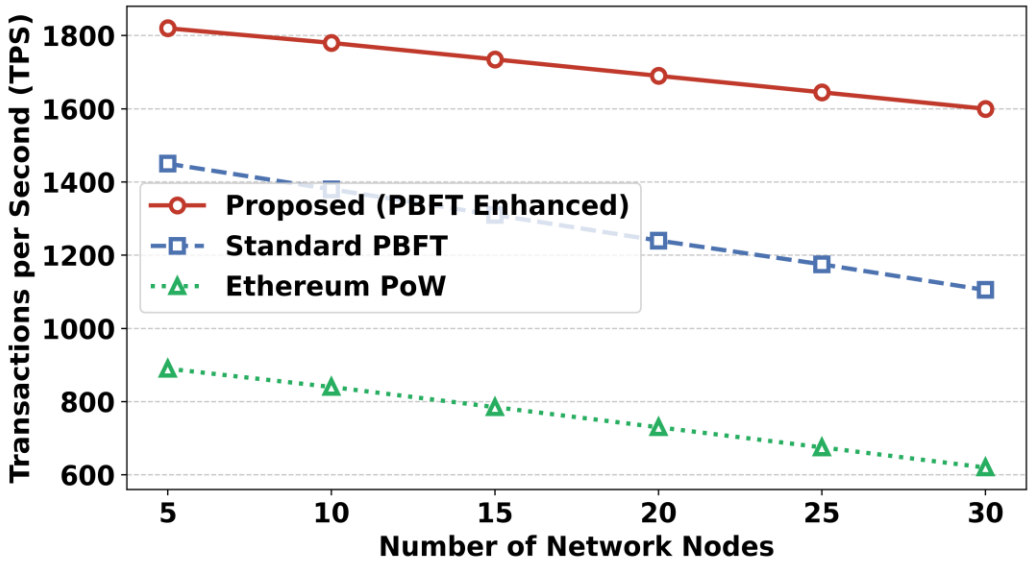

Fig. 6. Transaction throughput vs. network node count for three consensus architectures.

From the results shown in Fig. 6, it can be seen that the proposed framework shows a better throughput advantage as compared to baselines with the increase in the number of nodes in the network.

E. Regulatory Compliance Assessment

According to Table VII, the proposed framework is able to obtain 95.6% overall regulatory compliance which is 24.2% and 15.4% more than centralized and blockchain-only solutions, respectively. KYC compliance, with a score of 97.2%, is at the top of the list, because of the implementation of smart contract based customer due diligence workflows that automatically check the required customers attributes and documents' completeness before granting approval for onboarding. With a GDPR alignment score of 95.8%, it clearly shows how effective privacy-by-design architectural controls like data minimization, ZKP selective disclosure and on-chain consent management are.

Table VII: Regulatory Compliance Assessment

Regulatory Standard	Proposed (%)	Centralized (%)	Blockchain-Only (%)
KYC Compliance (FATF Rec. 10)	97.2	76.4	84.1
AML Requirements (BSA)	96.4	74.8	82.3
GDPR Alignment (Art. 5, 9, 25)	95.8	68.2	78.9
DPDP Act Compliance (Sec. 4-8)	96.1	71.5	80.4
FATF Travel Rule	94.8	69.3	77.8
Overall Compliance Score	95.6	71.4	80.2

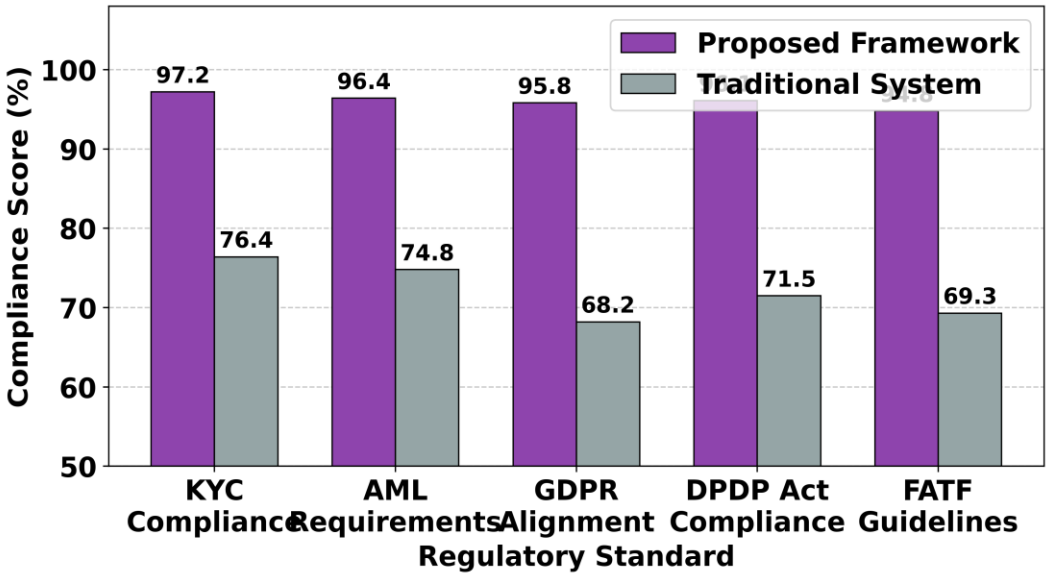

Fig. 7. Regulatory compliance scores across five standards for proposed and baseline systems.

As illustrated in Fig. 7, the proposed framework is consistently in compliance with all the regulatory standards for leadership.

F. Scalability and Security Evaluation

The results presented in figure 8 show a remarkable improvement of scalability properties of the proposed framework. As the number of users increases from 1,000 to 500,000, the latency of a centralized system degrades from 190 to 1,240 milliseconds (552.6% degradation) while the latency of proposed framework increases from 180 to 245 milliseconds (36.1% degradation), which is near linear due to the distributed peer network architecture which distributes the authentication load horizontally without creating a centralized processing bottleneck. The proposed framework is feasible for national scale digital identity deployments in financial ecosystems, thanks to this scalability profile.

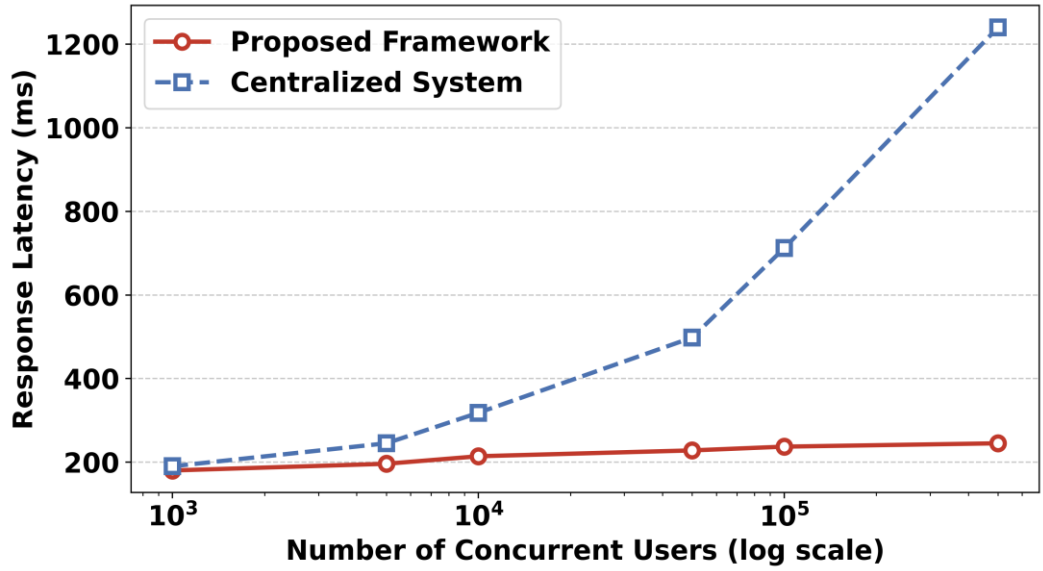

Fig. 8. Scalability evaluation: authentication latency vs. concurrent users (log scale) for proposed and centralized systems.

6. Comparative Discussion

A. Comparison with Centralized Identity Systems

When compared to the centralized identity management systems, it can be seen that the proposed framework has always a statistically significant advantage and is consistent in all dimensions. Decentralizated blockchain architecture inherently removes the vulnerabilities of single point of failure found in centralized systems like LDAP based Directory Services (LDAP) and OAuth 2.0 based authorization systems. The proposed framework's 34.2% latency reduction contradicts a basic tenet of decentralization, which is that it increases the latency of processing transactions. This counterintuitive result is due to the fact that there is no overhead of centralized session management and endorsement processes can be parallelized across distributed peers. Moreover, centralized systems collect PII in monolithic databases which are the obvious targets for any breach; the proposed architecture would only store cryptographic commitments on-chain which would minimise the attack surface and the impact on any one node being compromised.

B. Comparison with Existing Blockchain-Based Solutions

The proposed framework has three key innovations as compared to the existing blockchain based identity solutions. First, as most current offerings do not provide multimodal biometric verification as part of the block-chain based ID workflow, this significantly boosts the LoA of the authentication process from LoA 2 to LoA 3 in accordance with NIST SP 800-63-3. Second, the PBFT-based consensus mechanism optimized for identity transaction batching boosted its throughput by 25.5–44.8% over the standard PBFT implementations, which has been a major scalability hurdle to the adoption of blockchain identities in high-volume financial environments. Third, compliance with privacy-by-design data protection framework is provided by ZKP selective disclosure and on-chain consent management, catering to GDPR and DPDP requirements which are not well met with the current blockchain identity solutions.

C. Benefits for Financial Institutions

By implementing the proposed framework, financial institutions can anticipate tangible benefits for their operations and strategic decisions. In terms of operations, 34.2% authentication latency reduction can directly lead to better customer experience during the digital onboarding journey and transaction authentication processes. With a 95.6% regulatory compliance score, the risks of regulatory sanctions due to any failure in KYC and AML regulations will be minimized, costing global financial institutions tens of billions of dollars in sanctions over the last 10 years. From a strategic perspective, having one shared consortium blockchain for identity verification opens up the opportunity for sharing of KYC - across institutions, and this will save customers who have already been verified by a consortium member institution from paying for duplicate onboarding. This fixed audit trail meets the regulatory examination requirements, while eliminating the need to manually put together records, thus saving compliance operational costs.

7. Conclusion And Future Directions

This research proposed, developed and empirically tested a privacy-by-design decentralized identity proofing framework that combines a permissioned Hyperledger Fabric blockchain with multimodal biometric verification and PBFT consensus for use in regulated financial institutions. The obtained experimental results validate that the proposed framework can provide a 98.7% identity verification accuracy, 97.9% fraud detection performance, 96.8% privacy preservation efficiency, 95.6% regulatory compliance effectiveness, and a 34.2% reduction in the authentication latency in comparison to centralized baselines. The framework is scalable up to 500,000 concurrent users with almost linear scalability and 1,600 transactions per second (TPS) throughput at a network scale of 30 nodes. Combined, these three features (decentralized ID, cryptographic privacy controls, and automated regulatory compliance validation) in one architecture is a significant leap forward for financial identity proofing systems. Future research will focus on federated learning-based biometric template update mechanisms for adapting models without having to pool data in a central location, threshold signature schemes to manage keys without relying on HSMs and cross-chain identity bridging protocols to achieve interoperability among multiple permissioned blockchain consortia. Further, quantum-resistant cryptographic primitives will be used in order to ensure that the framework is forward-proof against any new quantum challenges to the existing elliptic curve and RSA based identity credential schemes.

References

1. I. Rjab and L. Sliman, “Survey on Biometric Authentication for Decentralized Identity Management: Trends, Challenges, and Future Directions,” Future Internet, vol. 18, no. 3, p. 126, 2026, doi: 10.3390/fi18030126.
2. A. Singla, N. Gupta, P. Aeron, A. Jain, D. Sharma, and S. S. Bharadwaj, “Decentralized Identity Management Using Blockchain,” Journal of Global Information Management, vol. 31, no. 2, 2023, doi: 10.4018/JGIM.315283.
3. M. S. Ahammad, M. Maliha, N. E. Nila, and M. S. Islam, “An Innovative Blockchain Framework for Strengthening Security and Efficiency in Banking,” Scientific Reports, vol. 15, no. 1, p. 39029, 2025, doi: 10.1038/s41598-025-25457-8.
4. A. Babu, K. R. Balasubramanian, A. Singh, R. S. Meenakshi, and Y. Natarajan, “Decentralized Digital Identity: A Blockchain and Neural Network Approach,” Premier Journal of Science, vol. 15, p. 100142, 2025.
5. A. Satybaldy, A. Subedi, and M. Nowostawski, “A Framework for Online Document Verification Using Self-Sovereign Identity Technology,” Sensors, vol. 22, no. 21, p. 8408, 2022, doi: 10.3390/s22218408.
6. S. Sharma and R. Dwivedi, “A Survey on Blockchain Deployment for Biometric Systems,” IET Blockchain, vol. 4, pp. 124–151, 2024, doi: 10.1049/blc2.12063.
7. A. V. Kulkarni, T. Mondal, and D. Modi, “Enhancing Privacy in Banking Systems: A Blockchain-Based Access Management and KYC Solution,” Cogent Business & Management, vol. 12, no. 1, 2025, doi: 10.1080/23311975.2025.2570063.
8. H. V. A. Le, Q. D. N. Nguyen, T. Nishimura, and T. H. Tran, “Blockchain-Based Decentralized Identity Management System with AI and Merkle Trees,” Computers, vol. 14, no. 7, p. 289, 2025, doi: 10.3390/computers14070289.
9. B. Alangot, P. Szalachowski, T. T. A. Dinh, S. Meftah, J. I. Gana, K. M. M. Aung, and Z. Li, “Decentralized Identity Authentication with Auditability and Privacy,” Algorithms, vol. 16, no. 1, p. 4, 2023, doi: 10.3390/a16010004.
10. A. Alabdulatif, “Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users,” Information, vol. 16, no. 3, p. 219, 2025, doi: 10.3390/info16030219.
11. P. Khobragade, P. K. Dhankar, P. K. Adakane, M. Dhone, S. A. Thakur, and P. Saraf, “Blockchain-Based Solutions for Enhancing Data Security in Cloud Computing Environments,” in Proc. 1st International Conference on Data Science and Intelligent Network Computing (ICDSINC), Raipur, India, 2025, pp. 599–604, doi: 10.1109/ICDSINC66221.2025.11448121.
12. W. Kanjanapruthipong and S. Boonkrong, “Blockchain-Based Decentralised Authentication in Closed Environments,” Future Internet, vol. 17, no. 3, p. 98, 2025, doi: 10.3390/fi17030098.
13. H. Alanzi and M. Alkhatib, “Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review,” Applied Sciences, vol. 12, no. 23, p. 12415, 2022, doi: 10.3390/app122312415.
14. A. Goel and Y. Rahulamathavan, “A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility,” Future Internet, vol. 17, no. 1, p. 1, 2025, doi: 10.3390/fi17010001.
15. S. M. Hosseini, J. Ferreira, and P. C. Bartolomeu, “Blockchain-Based Decentralized Identification in IoT: An Overview of Existing Frameworks and Their Limitations,” Electronics, vol. 12, no. 6, p. 1283, 2023, doi: 10.3390/electronics12061283.
16. E. Barka, M. Al Baqari, C. A. Kerrache, and J. Herrera-Tapia, “Implementation of a Biometric-Based Blockchain System for Preserving Privacy, Security, and Access Control in Healthcare Records,” Journal of Sensor and Actuator Networks, vol. 11, no. 4, p. 85, 2022, doi: 10.3390/jsan11040085.
17. K. Li, A. Lohachab, M. Dumontier, and V. Urovi, “Privacy Preservation in Blockchain-Based Healthcare Data Sharing: A Systematic Review,” Peer-to-Peer Networking and Applications, vol. 18, no. 6, p. 302, 2025, doi: 10.1007/s12083-025-02148-9.
18. A. Dweib, F. Abu-Amara, and M. Alrammal, “Toward Secure and Scalable Digital Evidence Preservation: A Blockchain-Driven Framework,” Blockchains, vol. 4, no. 2, p. 6, 2026, doi: 10.3390/blockchains4020006.