Int. J. Advance Soft Compu. Appl, Vol. 18, No. 1, March 2026
Print ISSN: 2710-1274, Online ISSN: 2074-8523

FinTech and AI technologies for Enhancing Evidence Verification and Dispute Resolution in Financial Litigation

Mohammad Sulieman Jaradat[1], Mwafag Mohammad Rabab'ah[2]

[1]Department of banking and financial technology, Faculty of Business, Ajloun National University, Ajloun, Jordan.
mohamed.jradat@anu.edu.jo
[2] Business & Finance Programs Section, Institute of Public Administration (IPA), Abha, KSA
rababahm@ipa.edu.sa

Abstract

The digitization of financial services represents the redesigning of evidence creation, storage, and challenging in court. Nonetheless, current verification approaches produce delays for fast-moving digital and multifaceted transactions. The paper implements and tests the performance of combining Artificial Intelligence (AI) and Financial Technology (FinTech) to develop the consistency of evidence verification and accelerate dispute resolution through the context of financial litigation. A techno-legal method is presented and is structured of three pillars, which comprise blockchain system for immutable provenance and accurate transactional timestamping including smart contracts; machine-learning analytics aimed at sensing anomalies and fraud patterns through varied payment and ledgers systems; and RegTech modules, which automate AML/KYC procedures, and which attempt to create auditable compliance records. The three pillars enhance three assurance layers, which comprise analytical inference, provenance integrity, and compliance attestation that is combined to a judicial interpretation layer by supporting understandable outputs deigned for evidences reassessment. Based on a sequence of particular scenarios that involve suspected structuring or layering, disputed transfers, and contractual breaches, the study investigates the way the method produces evidence objects, which are interpretable, traceable, and verifiable according to principles that are admissible and due-process. Furthermore, problems of implementation such as bias control, data governance, model risk, and privacy are studied in this paper. As a result, the method is generally applicable, but is particularly based on justice system digitization efforts, including those recently being applied in Saudi Arabia.

Keywords: *FinTech, Artificial Intelligence (AI), Evidence Verification, Financial Dispute Resolution, Blockchain in Litigation.*

Received 19 November 2025; Accepted 2 March 2026

1 Introduction

The digital transformation of financial ecosystems has intensely alerted, conveyed, and tested the creation of financial data through regulatory and judicial contexts.

The proliferation of Financial Technology (FinTech) applications and Artificial Intelligence (AI)-driven analytics has generated volumes related to structured transaction records. The legal systems that are accountable for arbitrating financial disputes maintain involving verification practices that are designed for conventional human-audited or paper-based evidence. The gap incurred between technological enhancements and admissibility demands has led to create issues related to procedural fairness, transparency, and data authenticity within the financial litigation [1], [2].

Throughout jurisdictions worldwide, regulatory organizations and courts are investigating how FinTech infrastructures enhance forensic integrity and evidence authentication. The European Union’s proposed AI regulatory framework implements risk-based obligations to financial-sector related to AI methods by ensuring transparency, accountability and human oversight [1]. Meantime, current research studies technical and lawful prerequisites for admitting ledger-based transactional records, which include expert explanation, provenance, and chain-of-custody [3]. These initiatives collectively indicate to a worldwide move to technically face verification system that can combine judicial accountability and FinTech innovation together.

Despite such improvements, legal institutions encounter continuous issues when rendering machine-generated evidence. AI systems are efficient in exploring patterns and anomalies throughout different transaction networks. These networks fail to meet interpretability and auditability, which are needed by the procedural law. Blockchain emphasizes provenance tracking and immutability while it is not able to provide answers for semantic or contextual questions regarding the commercial meaning of transactions. The resulted gap between legal adjudication and computational verification imposes a hybrid model, which supports the integration of FinTech’s computational rigor with normative safeguards related to lawful systems [3].

This paper highlights such a gap through enhancing a theoretical method for integrating AI and FinTech technologies to improve dispute resolution and evidence verification within the financial litigation. The framework stresses three interconnected legal-policy dimensions, which comprise: (1) admissibility, confirming that digital transactional records achieve evidentiary standards; (2) privacy and governance, implanting compliance with AML/KYC frameworks and data protection throughout FinTech pipelines; and (3) explainability, combining AI-derived anomaly inferences to interpretable forensic narratives that are appropriate for courtroom presentation. The contribution is based on the way improved computational infrastructures can reinforce rule-of-law principles through financial automation.

2 Literature Review

A study on financial markets has reliably emphasized and investigated different issues in relation to the potential of Artificial Intelligence (AI), regulatory adaptation, and insider trading [4], where [11-15] have studied and supported the field and is efficiently implemented in many different related applications. FinTech has transformed the approach of global financial transactions, inclusion, transparency, and promoting efficiency throughout digital payment systems, including decentralized ledgers and open banking. The current research perceives that adopting FinTech platforms represents chances for auditability and up-to-date jeopardies related to algorithmic opacity and systemic bias [5]. As payment infrastructures are currently more data-driven and automated, disputes are progressively relied on verifying electronic transaction trails excluding physical documentation. It is emphasized in [1] that regulatory oversight should develop in parallel, confirming that FinTech innovations continue to be consistent with consumer-protection and evidentiary norms. [30-33]

AI has progressively been implemented as a key analytical means in financial forensics, by allowing money-laundering risk prediction, compliance monitoring, and anomaly detection. In machine learning models, employing graph-based analytics and deep learning methods, can demonstrate non-linear relationships throughout transactions and accounts, which would remain unexplored in conventional auditing systems [6], [7]. However, different researches alert that the admissibility of AI-generated evidence relies on the reproducibility and transparency of the methods by integrating mechanisms for traceability and explainability [1]. Research in understandable AI (XAI) studies how rule-based reasoning, saliency maps, and confidence metrics, can reinforce judicial confidence in algorithmic outcomes.

Blockchain technology provides a secure system for protecting financial data's integrity, by supporting record authentication and preventing unauthorized modification. Research in Frontiers in Blockchain highlights its evidentiary importance, perceiving that consensus validation and immutability can strengthen the transaction logs credibility when presented in court [3]. Nonetheless, courts should create contextual understanding of blockchain to ensure that data is not changed, and is lawfully interpreted or created effectively. As a result, lawful introduce hybrid governance models, which integrate cryptographic assurance with standardized forensic protocols and expert testimony [8], [16-18].

RegTech improves FinTech by providing and enhancing real-time regulatory monitoring, and automating compliance. In its 2023 digital-transformation guidance, the FAFT supports distributing ledgers and implementing AI to develop and verify AML/KYC by addressing the potential of supervisory technology (SupTech) to enhance judicial fact-finding procedures. In [2], further observations ensure that AI- driven RegTech systems could expedite the resolution of financial disputes by ensuring traceable audit trails, which must satisfy evidentiary and regulatory standards. However, these systems should be aligned with privacy methods such as comparable data-protection laws and the EU General Data Protection Regulation (GDPR) to confirm lawful processing and proportionality. [26-29]

Although substantial progress has been produced, notable gaps still exist in the previous studies. In particular, the majority of existing methods aim to highlight legal evidence management and FinTech compliance in an independent manner resulting in disjointed governance. While AI has established achievement in fraud analytics, some researchers investigated its enhancement with blockchain provenance or aimed to adapt it to court processes. Additionally, experiential validation of RegTech tools for evidentiary determinations are kept limited, by ensuring admissibility in varied jurisdictions. The current study presents these gaps by improving and supporting oriented FinTech–AI model that encounters lawful verification, accentuating explainability, privacy, and admissibility as introductory criteria for dependable and reliable digital evidence within the financial litigation.

3 Methodology

This research improves an exploratory and conceptual method, which supports and combines Financial Technology (FinTech) infrastructures with Artificial Intelligence (AI) analytics, including blockchain verification techniques to improve the trustworthiness of digital evidence in financial litigation. The framework intellectualizes an end-to-end evidence verification pipeline, which includes four main layers: anomaly detection, data acquisition, blockchain anchoring, and AI-based and regulatory compliance auditing. Each layer provides an increasing measure of evidentiary trust, which is evaluated and articulated in several judicial contexts.

3.1 Integration of FinTech and AI Modules

The produced method combines related FinTech transaction schemes with AI anomaly detection engines to enhance the determination and clarification of doubtful or disputed financial activities. Transactional records are derived from institutional data vaults, open-banking interfaces, or digital payment networks by securing particular Application Programming Interfaces (APIs). This data is time-stamped and hashed onto a blockchain ledger, and emphasizing demonstrable chain-of-custody and immutable provenance. Thereafter, AI models deploy understandable machine learning algorithms such as Gradient Boosted Trees and Shapley-value interpretability where probabilistic anomaly scores are calculated for every transaction by enumerating deviations from normative

$$P_{anom}(x_i) = \frac{e^{-\lambda\, d(x_i,\mu)}}{\sum_{j=1}^{N} e^{-\lambda\, d(x_j,\mu)}} \qquad (1)$$

Equation 1 describes the AI Anomaly Probability Function (AAP), where Panom(x_i) denotes the probability that a transaction xi is a given anomalous for its distance $d(x_i, \mu)$, which is derived from the mean behavioral profile μ of comparable transactions, and λ denotes the sensitivity parameter controlling model responsiveness. High-probability anomalies with High anomaly probabilities improves forensic analysis and regulatory supervision.

3.2 Blockchain for Traceability and Authenticity

Blockchain represents the evidentiary backbone of the method, which provides immutable anchoring of financial data and emphasizes that any change on fundamental records is cryptographically explorable. In line with recommendations derived from current judicial blockchain research [3], [8] every hash transaction and metadata are verified in a permissioned blockchain, which integrates nuanced access control for regulators, auditors and courts. This method enables transparent traceability based on conforming it with privacy necessities under related methods as the equivalent financial data laws and the EU General Data Protection Regulation (GDPR) methods. [34-35]

Regulatory Technology (RegTech) modules line with AI and blockchain layers to mechanize the assessment of compliance verification for Know-Your-Customer (KYC) and Anti-Money Laundering (AML) requirements. The system performs persistent validation in contradiction of rule-based thresholds and dynamic sanctions lists through preserving a digital audit trail, which achieves evidentiary and supervisory standards. Not only can this automation speed dispute resolution, but can further improve accountability and consistency in managing financial evidence [2], [9].

To quantify the reliability of a digitally verified record, an Evidence Verification Confidence (EVC) metric is introduced to collect contributions derived from compliance integrity, accuracy of AI anomaly detection, and blockchain immutability. Every component can be normalized to a confidence score (0 - 1).

$$EVC = \alpha\, I_b + \beta\,(1 - P_{anom}) + \gamma\, C_r \qquad (2)$$

In Equation 2, I_b denotes the blockchain integrity confidence, while Panom denotes the anomaly probability that is derived from Equation 1, and Cr denotes the compliance reliability coefficient. Weights α, β, and γ are determined as α + β + γ = 1, by permitting legal experts to regulate the emphasis of the method on regulatory compliance, anomaly absence, and immutability based on case context.

3.3 Workflow and Data Flow Diagram

Accountability and confidentiality are prioritized by the proposed method within the verification process. This method prevents the direct process of Personally Identifiable

Information (PII) by providing cryptographic hashing and tokenization so that the entire sensitive attributes are securely anonymized and pseudonymized.

Every decision in AI is systematically logged to allow post-hoc auditability and interpretability by integrating it with over- sight mandates and transparency that are introduced by the European Union's Artificial Intelligence Act (2024), and which are compared with worldwide standards of AI governance. Moreover, the design preserves adaptability of cross-jurisdiction and adheres to the Financial Action Task Force (FATF) guidelines on financial integrity and digital transformation [1], [9].

As depicted in Figure 1, the evidence verification pipeline follows a sequential procedure in blockchain anchoring, AI-based anomaly detection, data acquisition, and normalization with explainability (e.g., Panom(x)). The verified results are accumulated into a courtroom-ready evidence bundle, assessed by RegTech compliance modules, and provided for judicial interpretation. Additionally, the figure illustrates the dashed feedback arrows, which represents human and ex post review techniques that improve transparency by optimizing explanations, anchoring parameters, and compliance validations throughout iterative evaluation cycles.

4 The proposed model

4.1 Workflow

The FinTech–AI evidence verification system is formed as a multi-actor architecture, which combines the components of technical verification with institutional decision-makers. Fundamentally, the system allows to function transactional data that are gained from FinTech platforms and financial organizations by transforming them into integrity-verified evidence packages, and making them accessible to courts and regulators through organized interfaces.

From a supply's view, banks, payment service providers, and other FinTech entities provide and function in ingestion gateways, which ensure the forensic integrity of extracted transactional records. Such records are normalized, hashed, and anchored over a permissioned blockchain to provide provenance and explore subsequent tampering [3], [8], [10]. The anchored data are afterwards handled by AI- based anomaly detection engines and explainable AI (XAI) layers, by creating human-interpretable rationales and anomaly probabilities [6], [10], [19].

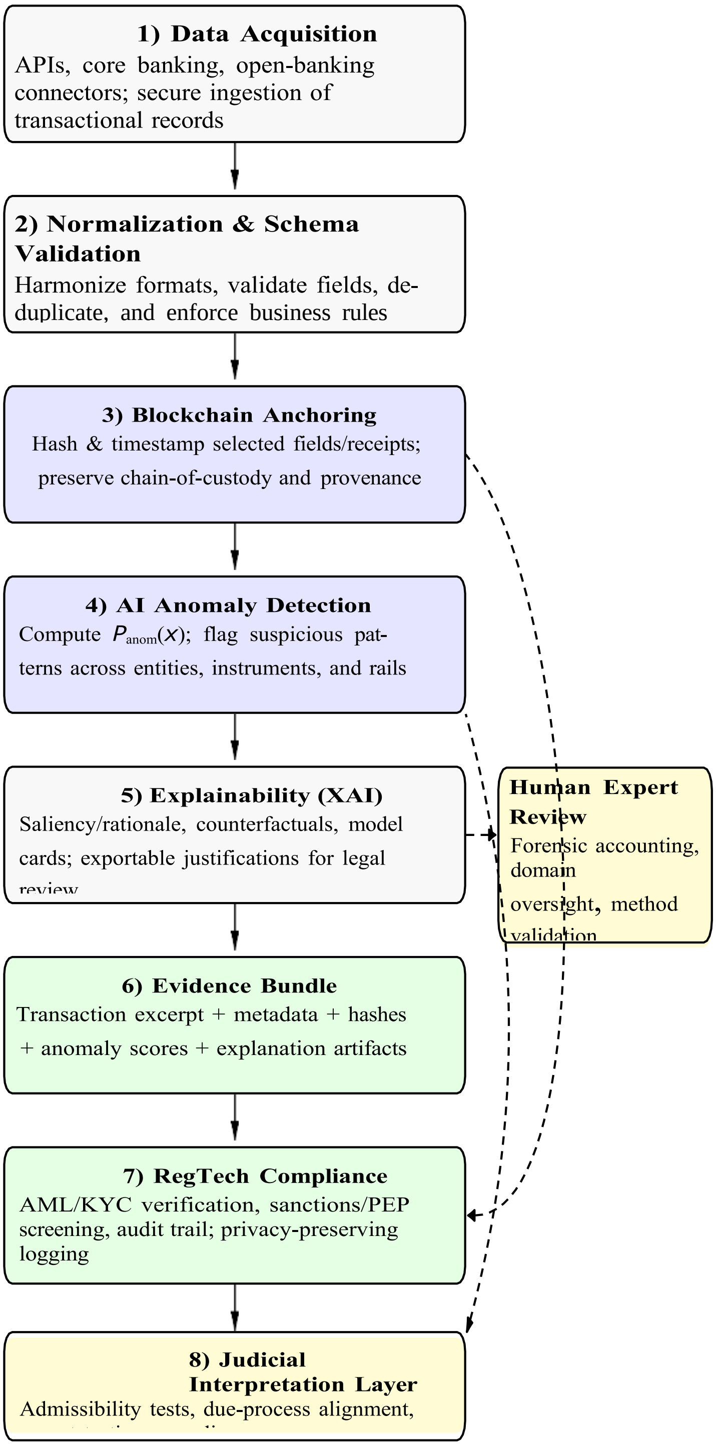
1) Data Acquisition
APIs, core banking, open-banking connectors; secure ingestion of transactional records
2) Normalization & Schema Validation
Harmonize formats, validate fields, de-duplicate, and enforce business rules
3) Blockchain Anchoring
Hash & timestamp selected fields/receipts; preserve chain-of-custody and provenance
4) AI Anomaly Detection
Compute $P_{\text{anom}}(x)$; flag suspicious patterns across entities, instruments, and rails
5) Explainability (XAI)
Saliency/rationale, counterfactuals, model cards; exportable justifications for legal review
Human Expert Review
Forensic accounting, domain oversight, method validation
6) Evidence Bundle
Transaction excerpt + metadata + hashes + anomaly scores + explanation artifacts
7) RegTech Compliance
AML/KYC verification, sanctions/PEP screening, audit trail; privacy-preserving logging
8) Judicial Interpretation Layer
Admissibility tests, due-process alignment,

Fig. 1. The evidence verification pipeline system of the FinTech–AI Evidence Verification Workflow

From a governance's view, regulatory authorities retrieve the evidence bundles via RegTech dashboards, which encompass automated AML/KYC controls, including sanctions screening by achieving the most effective practices that are determined by the UK Finance and FATF for AI-enabled supervision [2],[9]. A structured view similar to these bundles are provided to quasi-judicial authorities and courts such that these authorities are improved via expert commentary, legal framework, and standardized reporting formats, which integrate several admissibility evaluations and procedural guarantees [1].

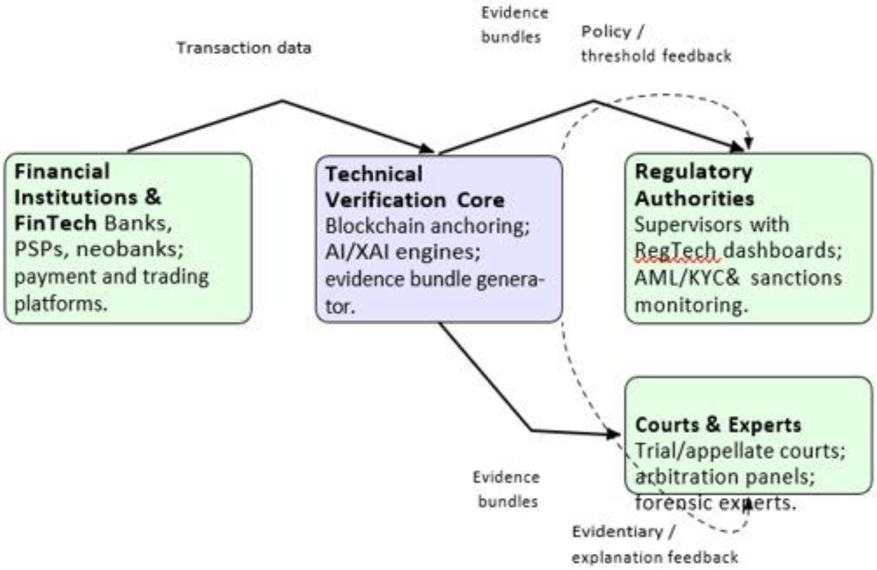
Evidence bundles
Policy / threshold feedback
Transaction data
Financial Institutions & FinTech Banks, PSPs, neobanks; payment and trading platforms.
Technical Verification Core Blockchain anchoring; AI/XAI engines; evidence bundle generator.
Regulatory Authorities Supervisors with RegTech dashboards; AML/KYC& sanctions monitoring.
Courts & Experts Trial/appellate courts; arbitration panels; forensic experts.
Evidence bundles
Evidentiary / explanation feedback

Fig. 2. High-level institutional architecture of the FinTech–AI evidence verification and consumption by courts and regulators

As shown in Figure 2, the technical verification core is situated between the institutional consumers and financial data sources, which are represented as a mediating layer for translating raw transaction logs into understandable, verifiable, and structured evidence objects.

4.2 Contractual Payment Dispute Use Case

To establish the framework's implementation, assume that there is a contractual payment dispute occurring between a supplier and a corporate client. The client claims that a high-value payment failed to be executed where the supplier upholds the transferred funds on time according to the contract.

In the first phase, related payment records are obtained by the financial, involving settlement confirmations, authorization logs, and initiation messages via a secure extraction pipeline system. These records are normalized and hashed in a cryptographical manner where their digests are anchored on the blockchain together with verifiable timestamps.

Any inconsistency occurring between anchored hashes and live records can signal a possible integrity breach [3]. Afterwards, the AI anomaly detection module assesses the series of payments, calculates anomaly probabilities for the disputed transaction that is relevant to the history of the client's payment outlines, and differentiates different transactions within the same subdivision. If a disputed transaction is based on raised anomalous scores, this can support the claimant position through determining departures from regular payment behavior. However, lower anomaly scores can strengthen the supplier's argument. The XAI layer provides Transaction level descriptions such as unbalanced timing a typical counterparty produces or irregular transaction amount that depends on in judicial proceedings to describe the conclusions of the particular method [6].

After that, the RegTech component functions different sanctions check and applies the AML/KYC in the involved parties by logging the entire justifications and decisions. In fact, these checks can uncover whether the transaction is delayed or blocked as a result of regulatory alerts, thus, explaining whether a non-execution was due to regulatory or contractual reasons. In the final phase, the system creates an evidence bundle, which involves normalized transaction records, anomaly scores, compliance outcomes, anchored hashes, and explanations.

This bundle is delivered to the court, and is supported via expert testimony to enhance and integrate adjudication of the payment dispute pursuant to procedural and evidentiary rules.

4.3 Decision Confidence Propagation Over Institutions

The Evidence Verification Confidence (EVC) metric presented in Equation 2 measures the reliability of individual evidence bundles in a procedural way at the level of the identified system. Courts and regulators, which represent institutional actors, can obviously assess a collection of evidentiary materials and not concentrating on the analysis of transactions on a standalone basis. To identify this cause, an average confidence score for a collection of M bundles related to a particular dispute is calculated based on Equation 3:

$$\overline{EVC} = \frac{1}{M}\sum_{k=1}^{M} EVC_k \ , \qquad (3)$$

Where EV Ck indicates to the verification confidence of the k-th bundle.

In the institutional phase, decision confidence not only relies on the evidence's technical reliability, but also on the quality of both judicial scrutiny and regulatory review. Assume that Greg ∈ [0, 1] denotes a normalized regulatory governance score, which detects the robustness and completeness of RegTech-based compliance checks, and Gcourt ∈ [0, 1] denotes a normalized judicial governance score, which influences the expert cross-examination, depth of adversarial testing, and legal analysis. Consequently, an institutional decision confidence metric is defined as:

$$C_{inst} = \vartheta_1 \, EVC + \vartheta_2 \, G_{reg} + \vartheta_3 \, G_{court} \tag{4}$$

subject to $\vartheta_1 + \vartheta_2 + \vartheta_3 = 1$ and $\vartheta_i \geq 0$ for $i = 1, 2, 3$.

This formation integrates different case categories and jurisdictions of the related significance of technical verification, judicial scrutiny, and regulatory oversight. For instance, jurisdictions that provide priority for judicial discretion can select $\theta_3 > \theta_1$, θ_2, while supervisory environment with increased levels of automation can prioritize Greg and EVC.

By explicitly highlighting the contribution of every institutional performance within Cinst, the proposed method simplifies transparent discussion with regards to the relative weight that is allocated for automated verification against human judgement pursuant to evolving discussions on AI governance in law and finance [1], [7].

5 Integration with Judicial Information Systems

The practical influence of the proposed method relies on how it is supported with available case management platforms and judicial information systems. Integration is performed based on standardized APIs, which reveal evidence bundles with their determined confidence scores to authorized parties, judges, and court clerks. User interfaces are formulated to illustrate technical particulars in different accessible formats, by linking visual anomaly patterns' summaries with narrative descriptions and evident indicators of blockchain integrity status [5].

This integration points to significant deliberations that include audit logging, confidentiality, and access control. Role-based access techniques guarantee that sensitive financial particulars are only observable to parties with legitimate interest where the entire modifications and accesses of digital case files are documented for accountability. While courts implement systems with electronic filing design, the evidence bundles, which are formed by the FinTech–AI framework are enclosed as structured exhibits, including their cryptographic fingerprints, which enable later integrity verifications into them.

Table 1 provides a recap of the principal legal advantages and issues that are relevant to the fundamental techniques in the proposed method, including indicative mitigation strategies. The mapping represents the dual role of AI and FinTech by identifying their ability to improve evidentiary strength and integrate procedural efficiency. At the same time, creating new sources of opacity, governance gaps, and bias if not exposed to effective regulation.

TABLE I: Technologies related to the proposed method and their principal legal advantages, jeopardies, and mitigation strategies

Technology	Primary Legal Benefit	Primary Legal Risk	Indicative Mitigation

		/Concern	Strategy
Blockchain anchoring of transaction hashes	Reinforces chain-of-custody and produces post-hoc tampering detectable; enhances authenticity of digital records [3], [8].	The issue of over-reliance on technical immutability without evaluating context or lawfulness of the underlying data.	Integrates blockchain proofs with recognized extraction processes and expert testimony; adopt standards for forensic acquisition and documentation.
AI anomaly detection and XAI explanations	Improves the detection of suspicious or typical payment or ubnormal patterns; pro- vides structured rationales that are tested in court [6].	Model opacity, data bias, and difficulties in replicating or challenging algorithmic outputs; possible due- process issues.	Use understandable methods and recognized training data; preserve reproducible model versions and logs; allows cross-examination and adversarial testing of AI-created evidence.
RegTech compliance modules (AML/KYC, sanctions)	Automates regulatory checks and provides auditable compliance trails; can explain whether non-execution was contractual or regulatory in origin [2], [9].	The issue of false positives or rigid rule enforcement causing unfounded blocking of transactions; liability questions when automated decisions are incorrect.	Periodic authentication of rulesets; human-in-the-loop review for high-impact decisions; obvious distribution of responsibility between technology providers and institutions.
Judicial and expert interfaces consuming evidence bundles	Enhances consistency and efficiency of evidence review; centralizes access to explanations and verified digital records [1].	Information overload or confusion of technical indicators; irregular access to technical expertise over courts.	Offers guidance and training for lawyers and judges; regulate report formats; motivates using independent technical experts in complicated cases.

5 Discussion

5.1 Regulatory and Supervisory Implications

The FinTech–AI evidence verification method contains straightforward consequences on how regulators produce formation of supervising digital financial infrastructures. By supporting RegTech compliance methods, AI-based anomaly detection, and blockchain anchoring through a coherent pipeline (see Figures 1 and 2), the method is aligned with a developing regulatory importance on understandable, auditable, and risk-based use of AI within financial services [1], [2]. Supervisory authorities may influence the Evidence Verification Confidence (EVC) metric in Equation 2 as an organized indicator related to the technical strength of digital evidence. Nonetheless, the institutional confidence metric in Equation 4 provides further holistic views, which obviously integrates judicial governance and regulatory contributions.

Nevertheless, these existing metrics are not able to reveal regulators from accomplishing their particular independent evaluations related to model institutional accountability, data provenance, and model risk. As accentuated in current studies on AI governance in finance, it is essential for supervisors to comprehend data dependencies, calibration choices, and modelling assumptions, which support any quantitative measure, which significances to abridge evidentiary reliability [7]. From a practical perspective, this involves integrating Cinst and EVC into wider supervisory review procedures and not treating them as self-explanatory or conclusive indicators.

5.2 Interpretation and Contestation of Metrics by Regulators and Courts

Regulators and courts may treat the Cinst and EVC metrics as informative but also treating it as contestable artefacts. Regulators may examine how weights (α, β, γ) and (θ1, θ2, θ3) in Equations 2 and 4 are identified on whether they influence documented supervisory priorities, for example, as consumer protection or AML/KYC robustness, and how delicate the subsequent scores are to updates in parameter choices or data quality. Courts can investigate the case of whether these weights implant normative judgments that must be within the scope of legal, and not within technical decision-makers, and whether different experts can sensibly determine substitutional configurations that causes to obtain various results.

From an evidentiary view, judges can treat increased Cinst or EVC values as a single component within a mosaic of proof, and not as dispositive evidence of lawfulness or authenticity. Cross-examination of technical experts can place emphasis on the training data that is exploited to evaluate anomaly probabilities, the operationalization related to governance scores Greg and Gcourt, and the AI documented error rates methods. This aligns with prevailing developments in treating algorithmic and probabilistic evidence when courts accentuate obtaining methodological transparency and the chance for contested challenge [3], [8].

5.3 Advantages of Procedural Efficiency, Auditability, and Transparency

In spite of these forewarnings, the method provides alternative advantages for procedural efficiency, auditability, and transparency. Blockchain anchoring enhances the traceable lineage of financial records and strengthens chain-of-custody documentation, by simplifying the demands imposed on regulators and courts to authenticate that digital evidence has maintained its integrity [3]. Integrating XAI layers with AI-based anomaly detection facilitates the provision of further efficient allocation of investigative resources through the determination of the encountered patterns and transactions, which ensure intensified review, and possibly speeding resolution timelines within complex dispute contexts [6].

From a supervisory standpoint, the direct combination of RegTech modules with evidence pipelines may cause obtaining machine-readable audit logs by permitting further timely and detailed control over the AML/KYC compliance and relevant requirements [2], [9]. When supported with the structured method (see Figure 1), such capabilities provide further intelligible and uniform flow of information from transaction creation to evidentiary submission.

5.4 Risks of AI Bias, Opacity, and Over-Reliance

New issues are presented by current technologies when developing evidentiary strength. AI methods that are trained in historical financial data can recreate available biases when treating particular transactional types or customer groups, by possibly influencing transactions that are flagged as anomalous and how those flags are explained [5], [6]. In the absence of transparent documentation regarding the characteristics of training data, feature selection procedures, involving judicial and regulatory decisions, and method’s performance over sub-populations, decisions of regulators and courts may encounter negative outcomes for particular groups.

Opacity continues to form an essential key challenge in this context. Despite improvements in using XAI techniques, it is not possible to entirely solve issues related to the communication of complex method behavior without obtaining technical expertise.

Rendering complex method behavior into forms, which are comprehensible to non-technical legal audiences is still restricted. The institutional confidence metric Cinst incompletely highlights this issue by keeping technical reliability separate from governance quality. Nonetheless, the fundamental AI elements should remain achieving minimum standards of contestability and explain-ability. Additionally, there exists a wider governance jeopardy such that organizations may highly depend on obtaining high-level scores, handling them as objective benchmarks without interrogating error bounds, limitations, and fundamental assumptions [7], [1].

5.5 Data Protection and Privacy Considerations

Data protection and privacy issues are noticeable when financial evidence shifts towards organizational limits.

While the method reduces direct handling of personally determined information by using hashing and tokenization, the collection of compliance indicators, anomaly scores, and transaction-level metadata persists to highlight possible re-identification issues when linked with external data sources. Courts and regulators should accordingly emphasize that accessing to evidence bundles is subject to stringent access control and that any secondary use of data is still balanced and legal in accordance with appropriate privacy rules, such as the GDPR and analogous regulations that exist in other jurisdictions [1], [9].

Furthermore, the persistent retention of anchored hashes raises concerns about data-minimization standards and erasure rights. While hashes are not necessarily rescindable, lawful discussions on whether hashes fall into the personal data scope and how they are treated when individuals exercise their data rights is investigated [8]. Consequently, the proposed method should be underpinned by governance policies, which determine access controls, retention periods, and different processes to comply with data-subject requirements while conserving the integrity of evidentiary reliability. [20-25]

5.6 Global, Principle-Based Policy Implications

From a policy view, the proposed method underpins the improvement of global, principle-based strategies when using both AI and FinTech evidentiary contexts. Rather than proposing particular metrics or technique, regulators and standard-setting organizations can clearly set out high-level demands for human oversight, documentation, and transparency when leaving room for implementing particular jurisdiction [2], [9]. Examples of such principles comprise: (i) obvious isolation of roles among adjudicators, verifiers, and evidence producers, (ii) obligatory documentation of designing the method, performance, and training data, and (iii) enforceable audit trails for human and technical decisions within the lifespan of evidence.

International coordination is significant when providing the nature of cross-border for several financial disputes and transactions. Different organizations as the FATF, including judicial networks and regional supervisors can influence theoretical tools such as Cinst and EVC to form comparative deliberations regarding different adequate levels of risk, the balance between human judgment and automation, and the minimum evidence-quality thresholds. The challenge is to interrelate such tools throughout appropriate governance methods, which maintain procedural safeguards and judicial independence, and which emphasize that computational measures must inform without averting lawful reasoning.

6 Conclusion and future work

6.1 Summary of Contributions

This paper improves a theoretical method and provides a set of metrics for supporting both Financial Technology (FinTech) infrastructures and Artificial Intelligence (AI) analytics within the evidentiary fabric of financial litigation. Starting from the observation that regulators and courts are progressively encountering with multifaceted digital transaction paths, which surpass the capacity of conventional verification techniques, an end-to-end pipeline method, which integrates secure data acquisition, normalization, blockchain anchoring is introduced in this research where explainability (XAI), AI-based anomaly detection, and RegTech compliance checks into a coherent evidentiary verification process are also involved. The method is established based on a contractual payment dispute use case and articulated institutionally that are relevant to a structure that combines financial institutions and FinTech providers with courts, regulators, and expert witnesses.

The method presents two quantitative measures, which comprise the Evidence Verification (EVC) metric at evidence-bundle level and institutional confidence metric Cinst at the governance level. Both measures are represented to explain how judicial scrutiny, regulatory oversight, and technical integrity collectively form decision confidence. In this context, the method responds to current calls in the existing studies for AI financial services systems, which are auditable and transparent [1], [2], [7]. By explicitly decomposing the roles of compliance assurance, blockchain integrity, institutional governance, and anomaly detection, further balanced and informed debates of these roles are enabled for evidentiary evaluation.

6.2 Governance and Regulatory Significance

Based on a supervisory and regulatory view, the proposed method demonstrates that FinTech infrastructures need to be improved from commercial or operational applications to perform efficiently as compliance and forensic tools.

Blockchain anchoring reinforces the chain-of-custody of digital financial records, where XAI and AI anomaly detection methods offer scalable techniques to determine suspicious patterns and outline the grounds on why particular transactions justify closer scrutiny [3], [6]. RegTech elements are joined firmly with this pipeline by simplifying real-time or near-real-time auditability and creating machine-readable logs, which improve supervisory oversight and integrate the employment of global standards such as the FATF's digital transformation principles [2], [9].

The institutional structure elucidates the interfaces among technical verification providers, regulators, courts, and financial organizations by addressing the potential efficiencies and the governance issues of this supported system. Significantly, the method averts demonstrating Cinst and EVC as determinative or self-sufficient scores. On the other hand, it allocates them as instruments, which do not substitute but inform normative judgments of supervisory authorities and judicial actors, and hence, positioning them by evolving the most effective practices in AI governance within the financial domain [1], [7].

6.3 Limitations

Notwithstanding its promise, this research possesses many significant limitations. Initially, the proposed method remains exploratory and theoretical, and is still not empirically validated when utilizing real-world case set of data or applied in procedural judicial or regulatory cases. Although the mathematical concepts for Cinst and EVC are

While the mathematical constructs for EVC and Cinst are internally compatible, their perceived legitimacy, stability, and calibration must be examined based on different simulation researches, stakeholder feedback, and pilot implementations. Afterwards, the model mainly highlights transaction-level financial evidence where other forms of digital evidence are not taken into account. Such examples of these forms involve unstructured communications, system logs, and contractual correspondence, or forms that act efficiently in financial disputes.

Additionally, the debate on data-subject rights, data protection, and privacy remains importantly within high levels. However, such debate is stranded in recent discussions on personal data and blockchain. The detailed classification of hashed records related to various data protection practices and forming different techniques for reconciling evidentiary integrity with rights such as objection or erasure demands increased technical and doctrinal analysis [8]. Finally, while the framework is envisioned to remain internationally appropriate, it does not thoroughly highlight jurisdiction-particular functional rules or alterations in evidentiary doctrines, which is likely to influence the way regulators and courts receive and weigh processed evidence in an algorithmic manner.

6.4 Future Research Directions

Many paths for future research take these limitations into consideration. One promising direction for future research represents empirical assessment, which is performed by applying the proposed method throughout monitored environments, including partially or synthetically anonymized transactional sets of data. This relies on examining the behavior of Cinst and EVC within several different conditions of governance configurations, model performance, and quality of data. For instance, this research may reveal how sensitive organizational trust is when exposed to changes through anomaly thresholds, variations in blockchain anchoring standards, or other various approaches that quantify regulatory and judicial governance scores.

A second direction comprises the extension of the proposed method to smart-contract and agentic contexts. Since contractual relationships are highly based on self-executing code that is implemented on disseminated ledgers, extensive research on how smart contracts are supported in evidence pipelines, how disputes regarding their interpretation or implementation are taken in EVC-like metrics, and how agentic AI systems that act on behalf of different organizations are subject to accountability and audited. This connects to wider progress on AI agents within financial markets, including their supervision with respect to courts and regulators.

A third path is to extend the treatment of multi-jurisdictional and cross-border disputes. Given those financial transactions regularly functions over several legal regimes, the future research can produce various methods for differentiating or harmonizing verification trust and organizational governance scores, which are featured by varying policies of requirements, proof, supervisory philosophies, and privacy rules. Comparative analysis can test the coherence of the proposed method by implementing different related EU-oriented methods. For instance, emphasizing AI regulation and data protection), common-law evidence doctrines, and jurisdictions experiencing rapid digitalization that is relevant to justice systems.

Lastly, there is a need for interdisciplinary research that integrates different perspectives of social science, computer science, and legal scholarship to validate how influenced bodies, lawyers, judges, regulators observe and apply quantitative metrics such as Cinst and EVC. Qualitative research, involving scenario-based experiments and interviews with practitioners can determine whether these metrics are able to improve trust and understanding in digital evidence or whether they fail to produce current opacity forms and over-reliance on technical artefacts. By highlighting such questionable challenges, it is significant to emphasize that AI and FinTech techniques that achieve robustness instead of adversely affecting the accountability, fairness, and transparency of financial dispute resolution.

References

[1] European Commission, Corporate Sustainability Reporting Directive (CSRD), 2023. [Online]. Available: https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en

[2] International Sustainability Standards Board (ISSB), IFRS S1 and IFRS S2 Sustainability Disclosure Standards, 2023. [Online]. Available: https://www.ifrs.org/groups/international-sustainability-standards-board/

[3] Task Force on Climate-related Financial Disclosures (TCFD), TCFD 2021 Status Report, 2021. [Online]. Available: https://www.fsb-tcfd.org/publications/

[4] M. Elbes, T. Alrawashdeh, E. Almaita, S. AlZu’bi, and Y. Jararweh, “A platform for power management based on indoor localization in smart buildings using long short-term neural networks,” Transactions on Emerging Telecommunications Technologies, vol. 33, no. 3, p. e3867, 2022.

[5] A. Abusukhon and S. AlZu’bi, “New direction of cryptography: A review on text-to-image encryption algorithms based on RGB color value,” in Proc. 7th Int. Conf. Software Defined Systems (SDS), 2020, pp. 235–239.

[6] A. Al-Arjan, M. Rasmi, S. AlZu’bi, et al., “Intelligent security in the era of AI: The key vulnerability of RC4 algorithm,” in Proc. Int. Conf. Information Technology (ICIT), 2021, pp. 691–694.

[7] M. La Torre, F. Mango, A. Cafaro, and S. Leo, “Does the ESG index affect stock return? Evidence from the Eurostoxx50,” Sustainability, vol. 12, no. 16, p. 6387, 2020.

[8] A. Nasir, K. Shaukat, K. I. Khan, I. A. Hameed, T. M. Alam, and S. Luo, “Trends and directions of financial technology (FinTech) in society and environment: A bibliometric study,” Applied Sciences, vol. 11, no. 21, p. 10353, 2021.

[9] A. T. M. Faruq and M. A. R. Chowdhury, “Financial markets and ESG: How big data is transforming sustainable investing in developing countries,” arXiv preprint arXiv:2503.06696, 2025.

[10] A. A. Davidescu, I. Bîrlan, E. M. Manta, and C. M. Geambas, “Artificial intelligence in ESG and sustainable finance: A bibliometric analysis of research trends,” in Proc. Int. Conf. Business Excellence, 2025, pp. 1506–1517.

[11] B. I. Dar, N. Badwan, and J. Kumar, “Investigating the role of FinTech innovations and green finance toward sustainable economic development: A bibliometric analysis,” International Journal of Islamic and Middle Eastern Finance and Management, vol. 17, no. 6, pp. 1175–1195, 2024.

[12] C. Sood, “From trees to tokens: AI and the digital renaissance of carbon markets,” SSRN Electronic Journal, 2025.

[13] H. A. Al-Khawaja, “Studying the mediating role of blockchain on the impact of the use of financial technology (FinTech) on the competitive advantage of banks,” Journal of Infrastructure, Policy and Development, vol. 8, no. 9, p. 6477, 2024.

[14] M. A. Naeem, S. Karim, M. R. Rabbani, A. Bashar, and S. Kumar, “Current state and future directions of green and sustainable finance: A bibliometric analysis,” Qualitative Research in Financial Markets, vol. 15, no. 4, pp. 608–629, 2023.

[15] B. Dai, J. Zhang, and N. Hussain, “Policy pathways through FinTech and green finance for low-carbon energy transition in BRICS nations,” Energy Strategy Reviews, vol. 57, p. 101603, 2025.

[16] A. M. Elhady and S. Shohieb, “AI-driven sustainable finance: Computational tools, ESG metrics, and global implementation,” Future Business Journal, vol. 11, no. 1, p. 209, 2025.

[17] K. L. Christiansen, “Relegitimising the voluntary carbon market: Visions of digital monitoring, reporting and verification,” Environment and Planning A: Economy and Space, 2024.

[18] A. Jones et al., “AI for climate impacts: Applications in flood risk,” NPJ Climate and Atmospheric Science, vol. 6, no. 1, p. 63, 2023.

[19] F. Taghizadeh-Hesary and S. Hyun, Green Digital Finance and Sustainable Development Goals. Cham: Springer, 2022.

[20] M. M. R. Domingo, “The impact of artificial intelligence on ESG: A conceptual framework for practitioners and policymakers,” Journal of Management for Global Sustainability, vol. 13, no. 1, p. 2, 2025.

[21] O. I. K. Olanrewaju, G. O. Daramola, and D. E. Ekechukwu, “Strategic financial decision-making in sustainable energy investments: Leveraging big data for maximum impact,” World Journal of Advanced Research and Reviews, vol. 22, no. 3, pp. 564–573, 2024.

[22] V. K. Ponnusamy et al., “A comprehensive review on sustainable aspects of big data analytics for the smart grid,” Sustainability, vol. 13, no. 23, p. 13322, 2021.

[23] E. S. A. A. Al-Taani, O. M. Shubailat, H. A. Al-Khawaja, M. A. A. Al-Zaqeba, and L. A. Elhesenat, “The mediating effect of supply chain transparency between blockchain technology adoption and sustainable supply chain performance,” Journal of Cultural Analysis and Social Change, pp. 992–1008, 2025.

[24] A. R. Alshehadeh, M. A. A. Al-Zaqeba, M. S. Jaradat, H. A. Al-Khawaja, and H. Hatamleh, “The impact of the Internet of Things on creative accounting practice using big data,” International Journal of Data and Network Science, vol. 9, no. 4, pp. 1129–1140, 2025.

[25] A. H. M. Al-Taani et al., “The influence of tax and customs policies on the success of supply chains: Evidence from Jordan,” International Journal of Advanced and Applied Sciences, vol. 12, no. 9, pp. 241–251, 2025.

[26] A. R. Alshehadeh, M. Al-Zaqeba, A. Qtaishat, H. Al-Khawaja, and E. Al-Wreikat, “Digitalization and sustainable development goals: Enhancing electronic financial reports quality in banking,” Data and Metadata, vol. 4, p. 734, 2025.

[27] H. A. Al-Khawaja, A. R. Alshehadeh, F. A. Aburub, A. Matar, and O. H. Althnaibat, “Intelligent solutions for insider trading and regulatory challenges in financial governance,” Data and Metadata, vol. 4, p. 680, 2025.

[28] H. H. Al-Kasasbeh, N. Albalawee, H. A. Al-Khawaja, and A. K. Qtaishat, “Legal challenges of using AI and big data in public administration: Administrative liability, data protection, and public services efficiency,” International Journal of Sustainable Development & Planning, vol. 20, no. 6, 2025.

[29] A. R. Alshehadeh, H. H. A. Eid, H. A. Al-Khawaja, M. A. A. Al Houl, and M. S. Jaradat, “Liquidity indicators, fund utilization efficiency, and their impact on profitability in commercial banks,” International Journal of Innovative Research and Scientific Studies, vol. 8, no. 1, pp. 812–823, 2025.

[30] H. A. Al-Khawaja and F. A. Aburub, “Blockchain for securing data storage in digital banking services,” SN Computer Science, vol. 6, no. 1, p. 56, 2025.

[31] Y. S. AbuAbbas, I. Jebril, M. A. Samara, H. A. Al-Khawaja, and M. A. A. Al Houl, “The impact of artificial intelligence on internal audit quality,” in Proc. Conf. Sustainability and Cutting-Edge Business Technologies, Springer, 2025, pp. 12–21.

[32] M. A. Samara, H. A. Al-Khawaja, Y. S. AbuAbbas, I. Jebril, M. S. Jaradat, and M. M. S. Alzubi, “The impact of artificial intelligence on the accuracy of final financial reports in Jordanian public shareholding industrial companies,” in Proc. Conf. Sustainability and Cutting-Edge Business Technologies, Springer, 2025, pp. 34–41.

[33] A. Althunibat et al., "Strengthening IoT healthcare security: Master-code multi-factor authentication against deepfake threats," in Proc. Conf. Sustainability and Cutting-Edge Business Technologies, Springer, 2025, pp. 272–282.

[34] D. N. B. Omar et al., "The role of AI in financial modelling and forecasting in commercial banks in Jordan," in Proc. Conf. Sustainability and Cutting-Edge Business Technologies, Springer, 2025, pp. 96–106.

[35] M. A. Al-Zaqeba et al., "The effect of implementing AI-driven customs processes on trade facilitation efficiency in Jordan," in Proc. Conf. Sustainability and Cutting-Edge Business Technologies, Springer, 2025, pp. 105–117.