



Governing AI and Blockchain in Finance: A Layered Trust Framework

Divyansh Mishra^{1*}, Rekha Agarwal², Rajesh Kumar Mishra³

¹XLRI – Xavier School of Management, Jamshedpur, Jharkhand 831001, India

² Department of Physics, Government Science College, Jabalpur, MP, India-482 0012

³ICFRE–Tropical Forest Research Institute (Ministry of Environment, Forests & Climate Change, Govt. of India),
P.O. RFRC, Mandla Road, Jabalpur, MP-482021, India

Abstract

AI is increasingly embedded into all aspects of financial markets; from credit decisions, compliance processes, trading strategies to payment systems. At the same time, blockchain-based finance has evolved from a speculative niche product into an integral part of the regulated market infrastructure. An integrative review of these two trends is necessary to examine their potential for convergence and how this will necessitate changes in governance. The review uses foundational academic literature in blockchain economics, decentralized finance and algorithmic fairness, as well as regulatory, supervisory and market sources up to October 2026. The authors provide three key findings. Firstly, there has been a structural change in the market: stablecoin capitalizations are estimated to be between approximately USD 270 billion and USD 320 billion. Tokenized real-world assets are concentrated primarily in U.S. Treasuries. The transitional period for the EU Markets in Crypto-Assets Regulation (MiCAR) ends on July 1, 2026. Finally, the U.S. GENIUS Act's rulemaking deadline has passed without a full set of final rules. Secondly, there remains a persistent gap in governance: international reviews show that the implementation of crypto-asset standards varies widely. Furthermore, most security losses result from a few very large attacks. Thirdly, AI agents have started transacting on stablecoin rails prior to the development of supervisory approaches to algorithmic accountability. Finally, the authors propose a five-layered Layered Trust Framework which includes settlement integrity, protocol and code assurance, data and oracle governance, algorithmic accountability, and institutional coordination. Each layer is linked to characteristic risks and governance instruments as well as measurable indicators. Based upon these relationships, the authors derive five testable propositions for future empirical research. The authors conclude that trust in converged AI and blockchain finance is generated by multiple layers of assurance rather than any single technology. Additionally, they believe that the data and algorithmic layers currently represent the weakest areas of governance. Limitations associated with an integrative design, such as relying upon secondary market trackers, are also addressed.

Keywords: blockchain; financial technology; stablecoins; tokenisation; AI governance; regulatory architecture

1. Introduction

Historically, financial systems have relied on intermediary institutions—such as banks that keep records, custodians that protect assets and clearing houses that assure payment—to establish confidence. Nakamoto (2008) suggested that a peer-to-peer network could replace a trusted intermediary in electronic cash by recording each transaction on a time-stamped block of data, which would be protected by proof-of-work. Subsequent economic studies characterized Nakamoto's idea as a way to reduce the cost of validating and



connecting information, which had implications for competition and market structure (Catalini & Gans, 2020). Cong and He (2019) demonstrated that decentralized consensus could encourage new entrants and competition, although the information it provided may also lead to collusion, while Yermack (2017) hypothesized that lower-cost record-keeping and increased transparency regarding ownership could alter the balance of power among stakeholders participating in corporate governance. Between 2024 and 2026, the nature of the field changed. Blockchain-based finance is no longer solely about whether regulators will allow it to exist; it is also about how it will coexist and be regulated alongside conventional finance. The European Union's Markets in Crypto-Assets Regulation (MiCA; European Parliament & Council, 2023) came into full effect on July 1, 2026. After that date, firms providing services relating to crypto-assets within the EU must obtain an authorization or stop operating in the Union (Autorité des marchés financiers [AMF], 2026). Similarly, in the U.S., the GENIUS Act (2025) established a federal regime for payment stablecoins, and its requirements for licensure are scheduled to become effective on January 18, 2027 (Markets Media, 2026). At the same time, the Bank for International Settlements (BIS, 2025) stated that tokenization represents a fundamental transformation of the monetary system, but concluded that stablecoins fall short of meeting the standards required of its primary business. Artificial intelligence is being utilized across many of the same financial functions. According to the Financial Stability Board (FSB, 2025b), AI is dramatically altering the financial sector with advantages such as increased efficiency, improved compliance with regulations, advanced data analysis capabilities and more customized products.

However, the majority of regulatory agencies are still at a very early stage of identifying the potential weaknesses associated with using AI, including reliance on third parties, interconnections among different markets and cybersecurity risks. AI-enabled agents are increasingly being used by payment service providers to manage digital wallets and execute payments using stablecoins (Stablecoin Insider, 2026a; The Block, 2026a).

Therefore, the two technologies are currently interacting directly at the point of execution rather than merely in prototype form. Scholarship examining these developments has generally addressed them individually. Initial studies on the integration of AI and blockchain emphasized their technical complementarity (Dinh & Thai, 2018; Salah et al., 2019). The literature on AI governance, conversely, has developed independently from the literature on distributed ledger technology. Recent conceptualizations of AI governance suggest that AI consists of multiple forms of technology, each having unique risks based upon the environment in which it operates; and that institutional frameworks derived from other disciplines, such as financial system oversight, provide inadequate guidance for establishing appropriate governance structures (Mishra et al., 2026g, 2026k). A review that links market, regulatory and technical evidence is necessary to identify areas where governance of integrated systems is weakest. This paper seeks to answer three research questions. RQ1: What structural developments occurred in market infrastructure and regulation between 2024 and October 2026 that characterize the current state of blockchain-based finance? RQ2: Where do governance shortcomings exist when AI enters into that environment? RQ3: What organizational framework can link risks, tools and measures across both technical and institutional levels? This paper provides a timely overview of market and regulatory evidence, a five-layer Layered Trust Framework, and five propositions for testing empirically. Section 2 outlines the methodology employed in conducting this review. Section 3 outlines the findings of this review and presents the Layered Trust Framework. Section 4 discusses the implications of these findings and provides an assessment of their limitations. Section 5 summarizes the conclusions reached.

2. Methods

As an integrative narrative review, this study combines a narrative review approach with a conceptual framework development component. It is neither a systematic review nor does it purport to cover all relevant literature. There were four types of source materials that formed part of the study. Initially, the most influential academic literature in areas such as blockchain economics, decentralized finance, smart contract security, financial law, and algorithmic fairness were identified as relevant to the study. The bibliographic information of the main journal articles were compared to records held by Crossref. Next, regulatory and supervisory documentation (including publications from the BIS and the FSB, EU legislation and supervisory statements, and US rulemaking notices) published before 14 October 2026 were examined. Then, market information was extracted from various industry trackers and trade-press articles. Due to methodological differences among these latter sources, the data were presented in terms of ranges with corresponding sources and publication dates (see Table 1).

Finally, conceptual frameworks developed previously by the authors related to AI governance, data governance, institutional design, and digital transformation were applied to analyze the AI dimension of the study.

While the sources are utilized for conceptual purposes, they are not intended to serve as empirical evidence. Targeted searches were performed on the internet in October 2026 to find additional information regarding market and regulatory developments. Searches were organized by topic (i.e., stablecoin regulation, MiCA implementation, tokenization, security incidents, AI regulation in finance, agentic payments, digital euro legislation, and energy usage). When feasible, search results were used to find primary documents. If secondary reports were the only option, this was indicated within the body of the paper and referenced in the bibliography. As the search was conducted with specific objectives in mind, it is possible that the review contains an excessive amount of English language and/or western regulatory sources.

Additionally, developments occurring after the specified cut-off date were not included in the study. A thematic synthesis approach was used to analyze the reported risks and governance responses. Risks were categorized based upon where failures occurred (settlement asset, protocol, data input, algorithm, or institutional environment). Each layer was continually refined until every documented risk had a primary location and the relationships between layers could be clearly articulated. Propositions were then created based upon the interfaces between layers and gaps identified in the existing literature. Since there were no human subjects participating in the study, no personal data, no non-public blockchain data, and only publically available/reported materials were used, no ethical issues arose during the course of the study.

Results and Argument

2.1. From trust-minimised ledgers to regulated infrastructure

Blockchain-based financial systems (the first generation of which were developed with Bitcoin at their core) were established to serve a limited purpose: as an un-censorable registry for value transactions (Nakamoto, 2008). Programmable platforms like Ethereum created a general-purpose execution environment upon which lending, trading, and derivative functions could be built as smart contract applications that could interact with each other. Schar (2021) refers to this new DeFi ecosystem as a layered architecture of interconnected protocols where there is no single entity responsible for managing the network, and the trade-off is between reducing risk associated with centralized operators and increasing risk due to vulnerabilities in the underlying software and/or the way the network is governed. Chen & Bellavitis (2020) describe DeFi as a collection of new decentralized business models that use software to replace some of the functions previously performed

by financial intermediaries. There are two key conceptual ideas from the literature that will help frame the discussion that follows.

Firstly, Werbach (2018) notes that while blockchain technology does not eliminate the need for trust, it does shift the location of trust from traditional institutional structures to the code, protocols and individuals/organizations that govern those protocols.

Secondly, Zetzsche et al. (2018)'s legal review demonstrates that distributed architectures create distributed liability, thus creating ambiguity regarding who will be held accountable should a protocol fail. Arner et al. (2016) framed these trends within the larger post-crisis FinTech paradigm in which technology companies, regulators and incumbent financial institutions compete to shape the architecture of finance. The events of 2025-2026 can be viewed as the institutionalization phase of this paradigm; technology has not displaced financial intermediaries but has been integrated into a regulatory framework that requires licensed issuers, custodians and service providers to assume the role(s) to which trust must continue to be placed.

2.2. Market structure, 2025–2026

The data provided in Table 1 identifies three distinct trends and a fourth that is starting to emerge. The first trend relates to the emergence of stablecoins as the most prominent on-chain money. As of May 2026, aggregate capitalisation of stablecoins exceeded USD 323 billion.

Although a less aggressive estimate by the Bank for International Settlements (BIS) placed this figure closer to USD 270 billion for March 2026, with USDT and USDC accounting for 95% of total outstanding amounts (Stablecoin Insider, 2026b). A more recent estimate published in July 2026 by Stablecoin Insider (2026c) estimated the aggregate capitalisation of stablecoins to be USD 318.3 billion on 2 August 2026. The wide variance among estimates suggests there does not exist an authoritative source for tracking these numbers and therefore any conclusions that rely upon the precise magnitude of these figures should be viewed with scepticism. A second trend relates to the tokenisation of traditional assets. Tokenisation of traditional assets has occurred, but it is limited in scope.

For example, a tracker reported that USD 346.1 billion of tokenised assets existed across 47 different asset categories in September 2026, with stablecoins representing approximately 86% of the total (KuCoin News, 2026). If one excludes stablecoins, estimates of tokenised real-world assets vary widely depending on the tracker and definition used, ranging from approximately USD 48 billion to approximately USD 60 billion (FXStreet, 2026; KuCoin News, 2026). Among all types of tokenised assets, only United States Treasury products appear to have reached production scale maturity. These products accounted for approximately USD 15 billion of tokenised assets distributed across approximately 100 assets. Conversely, tokenised real estate accounted for only approximately USD 457 million and an estimated 97% of tokenised asset value fell outside of the reach of United States retail investors (FXStreet, 2026).

Thus far, tokenisation has functioned primarily as an institutional collateral and cash-management tool rather than a mechanism for facilitating retail investment. A third trend relates to security losses. Security losses are concentrated and are increasingly tied to nation-state-sponsored actors. Chainalysis' 2026 Crypto Crime Report as reported by Fortune (2025) indicated that more than USD 3.4 billion was stolen through cyberattacks in 2025. Approximately 59% of these thefts were attributed to North Korea and two-thirds of these thefts resulted from three attacks, including the February 2025 attack on the Bybit exchange. Chainalysis also reported that there were 158,000 personal wallet compromises in 2025, which was roughly three times the number of compromises in 2022 (Fortune, 2025). A fourth pattern relates to machine participants. On-chain AI-agent payment activity was reported to be approximately USD 50 million from

approximately 40,000 agents in March 2026 (BlockEden, 2026, citing Bloomberg). This represents a very small percentage of the aggregate volume of stablecoins.

Nonetheless, the infrastructure for expanding this activity is currently under development: since the week of July 23, 2026 all Coinbase Business customers have been able to accept USDC payments directly from AI agents via the x402 standard (Stablecoin Insider, 2026a).

Therefore, the issue of governance is anticipatory and not reactive.

Table 1

Selected Market and Security Indicators, 2025–2026

Indicator	Reported value	As of	Source	Caveat
Aggregate stablecoin capitalisation	About USD 270 bn (BIS snapshot) to about USD 323 bn (record)	Mar–May 2026	Stablecoin Insider (2026b)	Depends on methodology
Stablecoin capitalisation	USD 318.3 bn	2 Aug 2026	Stablecoin Insider (2026c)	Single aggregator
Stablecoin concentration	USDT and USDC above 95% of outstanding amounts	Mar 2026	Stablecoin Insider (2026b)	Secondary report of BIS data
All tokenised assets	USD 346.1 bn across 47 classes; stablecoins about 86%	12 Sep 2026	KuCoin News (2026)	Exchange news item citing Token Terminal
Non-stablecoin tokenised assets	About USD 48–60 bn	Jul–Sep 2026	FXStreet (2026); KuCoin News (2026)	Definitions differ by tracker
Tokenised US Treasuries	About USD 15 bn across about 100 assets	Jul 2026	FXStreet (2026)	Press summary of industry research
Tokenised real estate	About USD 457 mn	Jul 2026	FXStreet (2026)	As above
Tokenised value outside US retail reach	About 97%	Jul 2026	FXStreet (2026)	As above
Crypto stolen	Over USD 3.4 bn; about 59% attributed to North Korea	2025	Fortune (2025)	Press report of Chainalysis data
On-chain AI-agent payments	About USD 50 mn across about 40,000 agents	Mar 2026	BlockEden (2026)	Blog citing Bloomberg

Note. Figures are reported as published by each source and are not harmonised. Trackers differ in coverage and definitions, so values should be read as indicative ranges. bn = billion; mn = million.

2.3. Regulatory architecture

Regulatory bodies have developed an agreement regarding the principle of equal treatment for all activities with the same risk profile.

However, there are still many areas where this principle is being applied inconsistently. The Financial Stability Board (FSB) released a review in October 2025 regarding the status of implementation of its crypto-asset recommendations.

While the review noted significant advancements in the implementation process, it also highlighted significant gaps and inconsistencies in the regulatory frameworks for crypto-asset service providers and global stablecoin arrangements.

Additionally, the review noted that very few jurisdictions had completed stablecoin frameworks. The FSB warned that inconsistency in the implementation process could create opportunities for regulatory arbitrage and hinder effective oversight of the global market.

Furthermore, the review noted that data collection and reporting requirements for service providers and issuers were lagging behind other components of the framework (FSB, 2025a). Table 2 provides a list of the major regulatory instruments and their current status. The EU is the furthest along in developing a common set of rules for financial markets. Provisions in MiCA relating to asset-referenced and e-money tokens went into effect in July 2024. The remainder of MiCA came into effect in December 2024 (European Parliament & Council, 2023). A transitional period for existing providers ended on 1 July 2026. Providers who have not received authorization prior to this date are expected to conduct an orderly wind down of their operations based upon pre-approved plans. ESMA has advised investors that not all of the existing providers will receive authorization (AMF, 2026).

In contrast to the EU, the U.S. has chosen a legislative approach to regulate payment stablecoins. The GENIUS Act (2025) imposes requirements on issuers of payment stablecoins including reserve, redemption, disclosure, licensing and supervisory requirements. Upon effectiveness, which is scheduled for 18 January 2027, the GENIUS Act will prohibit anyone from issuing a payment stablecoin in the United States without a federal or state license (Markets Media, 2026). A statutory deadline for implementation of regulations under the GENIUS Act was set for 18 July 2026. This deadline was missed without a final regulation issued, resulting in a short timeframe for implementation (The Block, 2026b). On 17 August 2026, the U.S. Department of the Treasury released a proposed regulation defining when a stablecoin is deemed to be issued in, or offered or sold into, the United States (Markets Media, 2026). Public-sector models for stablecoins differ greatly from private-sector issuer models. The BIS (2025) evaluated stablecoins using three criteria: singleness (acceptance at par), elasticity (timely discharge of obligations without gridlock) and integrity (safeguards against financial crime). The BIS concluded that stablecoins did not meet these criteria and recommended a single ledger incorporating tokenized central bank reserves, tokenized commercial bank money and tokenized government bonds. The euro area exemplifies public sector alternatives to private sector-issued stablecoins. On 23 June 2026, the European Parliament's Economic and Monetary Affairs Committee passed a resolution supporting a digital euro by a vote of 43-14 (ForkLog, 2026). In July 2026, the plenary session of the European Parliament approved a negotiating mandate for trilogue discussions on a digital euro by a vote of 416-169. If negotiations are successful, a digital euro could be operationalized as early as 2029 (Sumsb, 2026). Auer et al. (2020) provide an earlier comparison of factors driving the development of central bank digital currencies. Regulation of AI affects users through the application of AI. High-risk applications of AI include credit scoring, which is identified in Annex III of the EU AI Act (European Parliament & Council, 2024). Following the Digital Omnibus on AI, approved by the European Parliament on 16 June 2026 and by the Council on 29 June 2026, the deadline for compliance for Annex III systems was extended from 2 August 2026 to 2 December 2027. Some other obligations retained their original deadlines (Gibson, Dunn & Crutcher LLP, 2026; Secure Privacy, 2026).

Therefore, AI-based credit decisions made on or in relation to blockchain platforms will be subject to higher risk obligations later than the crypto-asset service rules that are currently applicable. There will be an interim period during which the two regulatory frameworks are not aligned.

Table 2 Principal Regulatory Instruments and Their Status

Instrument or event	Jurisdiction	Status to 14 October 2026	Framework layers
MiCA, Regulation (EU) 2023/1114	EU	Fully applicable; maximum transitional period ended 1 July 2026 (AMF, 2026)	L1, L5
GENIUS Act, Pub. L. No. 119-27	US	Enacted July 2025; effective date expected 18 January 2027; 18 July 2026 rulemaking deadline passed without a full final rule set; Treasury proposed rule 17 August 2026 (Markets Media, 2026; The Block, 2026b)	L1, L5
FSB crypto-asset framework and thematic review	Global	October 2025 review reports significant gaps and inconsistencies in implementation (FSB, 2025a)	L5
BIS unified-ledger proposal	Global	Policy proposal in the Annual Economic Report 2025; stablecoins judged to fall short of singleness, elasticity and integrity (BIS, 2025)	L1
Digital euro	Euro area	Committee position 23 June 2026; plenary mandate in July; trilogue under way; issuance possible from 2029 (ForkLog, 2026; Sumsb, 2026)	L1
EU AI Act as amended by the Digital Omnibus on AI	EU	Annex III high-risk obligations, including credit scoring, deferred to 2 December 2027 (Gibson, Dunn & Crutcher LLP, 2026; Secure Privacy, 2026)	L4
FSB report on monitoring AI adoption	Global	October 2025; authorities' monitoring of AI vulnerabilities at an early stage (FSB, 2025b)	L4, L5

Note. Layers refer to the Layered Trust Framework in Section 3.6. Status reflects sources available to 14 October 2026.

2.4. The risk surface of blockchain finance

Code Risk. Smart Contracts perform exactly what they were coded to do. Atzei et al.'s (2017) classification of attack types against Ethereum Contracts arising from the intersection of programmer mistakes, blockchain properties, and execution environment illustrate how difficult it may be to fix an exploited weakness in a Smart Contract after a transaction has been confirmed. Given the size of the 2025 loss reported by Chainalysis (Fortune, 2025), it would seem that Operational and Key Management Security, rather than just Contract Logic, is a primary source of risk. **Data Risk.**

While a Blockchain can ensure that data remains unaltered once it is recorded, it cannot ensure that data from outside the chain was accurate upon recording. Caldarelli (2020) discusses the Oracle Problem and argues that while Oracles introduce the trust assumptions of the organizations providing their data into the System, the reliance on Oracles will decrease with increased trust in the overall System. Tokenized Assets provide a clear example of this exposure: A token representing a Treasury Fund or a Pool of Loans will only be as reliable as the attestation that links the token to the underlying asset. **Illegal Finance Risk.** Foley et al. (2019) found that a significant portion of Bitcoin users and transactions during the time frame they examined were involved in illegal activities, and the Bank for International Settlements (BIS) (2025) identified integrity as one of the three criteria that stablecoins fail. Regulatory action focuses on tracking and service provider accountability (AMF, 2026; FSB, 2025a). **Energy and Sustainability.** de Vries (2018) highlighted the rapidly increasing energy demands of Proof-of-Work Mining. According to the Ethereum Foundation (n.d.), the 2022

transition from Proof-of-Work to Proof-of-Stake resulted in an estimated reduction of Energy Consumption of the Network of approximately 99.95%. This demonstrates that Consensus Design is a Governance Variable; however, this is a Developer Estimate and not an Independent Audit. Mishra et al. (2026e) frame Digital Transformation and Sustainability as Converging Strategic Challenges; a framework that is relevant to both the Energy Footprint of Distributed Ledgers and AI Computations.

2.5. The convergence of AI and blockchain

Complementary Relationships Early studies identified two types of complementarities. On the one hand, AI supports blockchain technology, e.g., via the sharing of verifiable and secure data.

On the other hand, AI supports blockchain technology via analytics and automation (Dinh & Thai, 2018). Salah et al. (2019) reviewed the first type of relationship and discussed open research problems. In the financial industry, the second type of relationship is evident in the area of compliance and analytics, where the FSB (2025b) identified increased compliance with regulations and enhanced data analysis capabilities as potential benefits of utilizing AI. Autonomy vs. Irreversibility What is new in 2026 is the convergence of the two technologies during the actual execution phase. An AI agent that has the ability to sign transactions can complete those transactions at the speed of machines.

In addition, once a stablecoin transaction is completed on a public blockchain, it cannot typically be reversed. Stripe's co-founder anticipated a significant amount of agent-based commerce occurring through stablecoins (The Block, 2026a).

2.6. Furthermore, merchants are currently developing products to accept stablecoins (Stablecoin Insider, 2026a).

Therefore, the source of errors will shift from human approval to specification: the limitations placed on the agent and its wallet will serve as the primary safeguard. The conceptual literature regarding alignment addresses the general issue of ensuring that systems pursue goals that are truly advantageous as opposed to simply being technically aligned with the goals established (Mishra et al., 2026b). In a smart contract, the analogue is quite direct since code executes the specifications and not the intentions of the user.

Thus, when an AI agent manages a smart-contract wallet, a specification gap can result in a permanent loss. This hypothesis regarding error is presented as a basis for designing and testing, not as an established fact. Fairness and Data Machine-learning credit models produce distributional impacts that continue to exist even when lending becomes tokenized. Using U.S. mortgage data, Fuster et al. (2022) demonstrated that Black and Hispanic borrowers were less likely to benefit from the introduction of machine-learning-based default models. Mehrabi et al. (2021) surveyed the various forms of biases and definitions of fairness that allow for assessment of such impacts. Mishra et al. (2026f) examine fairness, bias and justice in algorithmic systems. Mishra et al. (2026d) contend that intelligent systems can only be trusted to the extent that the data they receive is reliable. Oracles and on-chain transaction history are the data sources for blockchain-based finance. As such, if they are employed to train or trigger credit and risk models, the data governance considerations of provenance, representativeness and consent will apply directly. The evidence regarding fairness provided above relates to traditional credit markets. Its application to blockchain-based lending is a proposal rather than an observation (see P4). Concentration and Dependency The FSB (2025b) identified reliance on a limited number of third-party AI service providers as an operational vulnerability. Similarly, blockchain finance exhibits a pattern of concentration in terms of stablecoin provision by two issuers (Stablecoin Insider, 2026b). Mishra et al. (2026h) asserted that AI power resides in physical infrastructure that is geographically concentrated and under the control of specific entities.

Therefore, convergence exacerbates concentration. An agentic payment stack may simultaneously rely on a few model providers, a few wallet/facilitator providers and a few stablecoin issuers. Enterprise Deployment and Institutional Context Mishra et al. (2026a) describe AI-enabled smart systems constructed on cloud/edge infrastructure, large-scale data pipelines and increasingly autonomous decision-making processes. This is the environment into which financial institutions are now integrating blockchain settlement. Mishra et al. (2026c) investigate how AI is affecting managerial decision-making in relation to planning, organizing, staffing, leading and controlling. The controlling aspect is where assurance concerning automated financial processes resides. Broad-based studies relating to AI in socio-economic development and relating to AI in law, finance and environmental governance (Mishra et al., 2026i, 2026j) provide the larger institutional context for these issues.

2.7. The Layered Trust Framework

The above evidence indicates that confidence in converged AI and blockchain finance is generated through the existence of assurance at multiple distinct levels, and when one level fails, those failures will propagate to other layers. The Layered Trust Framework (Figure 1, Table 3) categorizes these layers. Each layer is based upon where the failure occurs rather than what specific technology it utilizes. Layer 1 concerns settlement and monetary integrity; this includes whether the settlement asset acts as money (i.e., accepts par value, has ability to provide settlement under stress, and resists illicit uses), which are the BIS (2025) test criteria. Layer 2 involves protocol and code assurance; this includes consensus, smart contracts, key management, and operational security. Layer 3 relates to data and oracle governance; this includes the provenance, redundancy, and privacy of off-chain data consumed by blockchains and models. Layer 4 concerns algorithmic accountability; this includes model risk, fairness, explainability, and constraints on autonomous agents. Layer 5 relates to institutional and regulatory coordination; this includes licensing, supervision, allocation of liability, and cross-border consistency. Based on the preceding discussion, two design principles emerge. The first is the "weakest-layer" principle: the overall trust in a product/service will be limited by the weakest assured layer.

Thus, robust settlement assurance cannot offset unconstrained agent decision-making or uncontrolled data input into a model. The second is the "interface" principle: a large number of actual incidents occur at the interfaces between layers. An example would be when a contract (Layer 2) relies on an oracle (Layer 3) that provides input to a model (Layer 4) whose decision results in stablecoin settlement (Layer 1) under a license recognized only in some jurisdictions (Layer 5). The practical application of the Layered Trust Framework is as an assurance map: for every product/service, the operator lists all controls and indicators at each layer and identifies layers that do not contain any evidence. Given the evidence reviewed, Layers 3 and 4 appear to be the least developed in terms of supervisory practice. Supervisory data/reporting requirements for crypto-assets remain significantly behind other areas of crypto-asset regulation (FSB, 2025a); AI monitoring by authorities is at an early stage (FSB, 2025b); and the EU's high-risk AI obligations have been delayed until December 2027 (Secure Privacy, 2026).

Table 3 *The Layered Trust Framework: Risks, Instruments and Indicators*

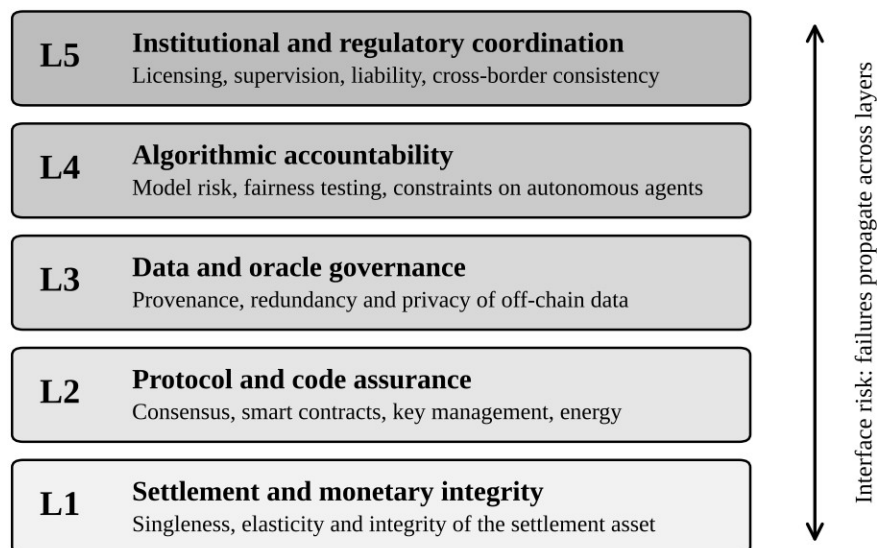
Layer	Characteristic risks	Governance instruments	Indicative indicators
L1 Settlement and monetary integrity	Loss of peg; inadequate reserves; redemption runs; illicit use through unhosted wallets	Reserve, redemption and disclosure rules (MiCA; GENIUS Act); tokenised central bank money; traceability controls	Peg deviation; reserve disclosure frequency; redemption time under stress; share of flows with traceable counterparties
L2 Protocol	Smart-contract exploits;	Independent audits and formal	Loss per unit of value at risk;

and code assurance	key compromise; consensus failure; energy demand	verification; key-management standards; incident disclosure; consensus design	time to detect incidents; share of audited contracts; energy per transaction
L3 Data and oracle governance	Oracle manipulation; weak provenance of tokenised-asset attestations; privacy leakage	Source redundancy; attestation standards; data-governance policies; data-lineage records	Independent sources per data feed; attestation latency; share of tokens with verified custody evidence
L4 Algorithmic accountability	Biased credit models; unconstrained agents; concentration in model providers	Model validation and fairness testing; agent spending limits, allow-lists and human override; AI Act compliance	Group disparity metrics; share of agent payments under policy constraints; erroneous-transfer rate; provider concentration index
L5 Institutional and regulatory coordination	Regulatory arbitrage; fragmented licensing; liability gaps	Supervisory cooperation; mutual recognition; explicit liability allocation; international monitoring	Jurisdictions with finalised frameworks; time to authorisation; cross-border information exchanges

Note. Instruments and indicators are illustrative and are intended to be adapted to each product and jurisdiction.

Figure 1

The Layered Trust Framework for Converged AI and Blockchain Finance



Note. Layers are defined by the locus of failure they address. The weakest layer bounds overall trust, and many incidents arise at interfaces between layers.

The five propositions presented here have been based on the framework and the literature review conducted. All of them are formulated as hypotheses, which could be tested using empirical methods.

P1 (least assured layer). Incidents of loss and severity of incidents related to converged AI and Blockchain financial products will be better predicted by the least assured layer than the average level of assurance provided by all layers. This hypothesis can be empirically tested using incident databases categorized by layer.

P2 (oracle and data coupling). Products where off-chain input data is controlled through documented provenance and redundancy at the source will experience less oracle-attributed incidents compared to similar products that do not control their off-chain input data.

P3 (limitations of agent). Payments initiated by an AI agent that is subject to policy limitations (spending limits, allowable counterparties, and human intervention if payment amount exceeds certain threshold) will lead to lower rates of irrecoverable mispayments than payments made by an AI agent without policy limitations.

P4 (transfer of bias). Credit scoring models developed with machine learning algorithms used in tokenized or decentralized lending platforms without bias testing will replicate or exacerbate the biases observed in credit scoring models developed with machine learning algorithms used in traditional credit markets (Fuster et al., 2022).

P5 (regulatory alignment). The higher degree of alignment between regulatory frameworks across jurisdictions regarding stablecoins and service providers will reduce regulatory arbitrage-driven relocation of activities. The staggered implementation of MiCA and the GENIUS Act represent a unique opportunity for empirical comparison.

3. Discussion

Implications for regulators: The evidence supports a use-based approach to regulation, where regulators regulate according to the type of activity and its risks and not according to the type of underlying technology. This approach is consistent with the FSB's principle of "same activity, same risk, same regulation" (FSB, 2025a). There are priority gaps in supervisory data, in monitoring of provider concentration (FSB, 2025b), and in aligning the timelines of the EU's existing crypto-asset rules with those of the U.S.'s high-risk AI rules, which have yet to arrive. The GENIUS Act's compressed implementation window (The Block, 2026b) demonstrates the costs associated with passing legislation quicker than the regulatory capacity exists. Conceptual work on institutional design indicates that existing models of financial oversight are useful for governing AI, but are insufficient in themselves.

Therefore, adapting Layer 4 supervision through incremental changes rather than transplanting it from other areas of supervision is a viable option. Implications for institutions: Institutions that integrate AI agents with blockchain settlement systems must consider constraint design as a critical component of risk control. Constraint design involves establishing boundaries for agent authority, documenting the provenance and redundancy of each oracle and attestation upon which a token relies, evaluating credit models for unequal outcomes prior to driving on-chain decisions, and identifying provider concentrations within the model, wallet, and issuer stacks. The assurance map provided in Section 3.6 can provide a framework for reporting to senior management. Implications for research: Research into the propositions requires data that are currently poorly supported. As shown in Section 3.2, industry tracker data differ significantly in their estimates of total market size. Independent and definitionally consistent datasets on tokenized assets, stablecoin transactions, and agent transactions would add credibility to the field. Coding incident taxonomies by layer would enable direct testing of Proposition 1. Designing quasi-experiments based on the effective dates of MiCA and the GENIUS Act would enable empirical investigation of Proposition 5. Tensions and open questions: A tension exists between the BIS (2025) position regarding tokenized central bank and commercial bank money as the primary form of money, and a U.S. statute authorizing the licensing of private payment stablecoins (The Block, 2026b; Markets Media, 2026). The direction taken by regulatory bodies will influence Layer 1 development for years to come. Whether regulatory controls on autonomous agents emerge via

regulation, via payment network rules, or via voluntary industry standards remains undetermined, and will significantly impact how rapidly Layer 4 develops. Limitations: This is an integrative review, and not a systematic review. Its scope is intentional. The majority of market data originates from industry trackers and trade press reporting whose methodological transparency is limited. Several of these data points are presented as ranges for this reason. All regulatory facts presented herein are accurate as of October 14, 2026 and may change rapidly. Some sources cited herein regarding AI governance are conceptual chapters and are utilized for contextualization purposes only and do not constitute empirical evidence.

Finally, utilizing previously published works by the authors creates a potential for self-citation bias that readers should evaluate.

4. Conclusion

The primary questions regarding blockchain-based finance have now shifted to institutional issues: who creates these systems, who will oversee them, who is responsible if something goes wrong, and how do you prove they work correctly? At the same time, artificial intelligence (AI) has been introduced into some of those same areas and we've already seen AI agents running on stable coin rails, adding another level of autonomy to the settlement process. We can never go back. We used the market, regulatory and technical data to demonstrate how the structure of finance changed from 2024 to 2026. We identified where there are gaps in governance and proposed a layered trust framework that links risk to each instrument/indicator across the five layers. The central idea is that trust in converged systems is dependent on all parts of the entire stack. And it is limited by the least assured layer. Currently, the data and algorithmic layers are the least governed. The five propositions outline a research agenda for testing this claim and for developing the necessary datasets for that testing. For regulators and institutions, the practical consequence is to supplement the settlement-focused regulation emerging in the EU and US with specific expectations for data providence, model accountability and restrictions on autonomous agents.

Acknowledgments

We are very much thankful to the authors of different publications as many new ideas are abstracted from them. Authors also express gratefulness to their colleagues and family members for their continuous help, inspirations, encouragement, and sacrifices without which this work could not be executed. Finally, the main target of this work will not be achieved unless it is used by research institutions, students, research scholars, and authors in their future works. The authors will remain ever grateful to Dr. Neelu Singh, Director, ICFRE Tropical Forest Research Institute, Jabalpur, Director, XLRI – Xavier School of Management, Jamshedpur & Principal Government Science College, Jabalpur who helped by giving constructive suggestions for this work. The authors are also responsible for any possible errors and shortcomings, if any in the paper, despite the best attempt to make it immaculate.

5. Declarations

Ethics statement. This study is an integrative review of published literature, public regulatory documents and publicly reported market data. It involved no human participants, personal data or non-public blockchain data, and ethics approval was therefore not required.

Conflict of interest. Conflict of interest and funding statements are provided on the title page to preserve blinding.

Data availability. All sources are publicly available and are listed in the reference list. Table 1 records the source and date for each market indicator.

References

- [1] Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of Fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47(4), 1271–1319.
- [2] Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In M. Maffei & M. Ryan (Eds.), *Principles of security and trust* (Lecture Notes in Computer Science, Vol. 10204, pp. 164–186). Springer.
- [3] Auer, R., Cornelli, G., & Frost, J. (2020). *Rise of the central bank digital currencies: Drivers, approaches and technologies* (BIS Working Papers No. 880). Bank for International Settlements. <https://www.bis.org/publications/work880.htm>
- [4] Autorité des marchés financiers. (2026). *End of the MiCA transitional period: ESMA sets out its expectations of professionals and warns retail investors*. <https://www.amf-france.org/en/news-publications/news/end-mica-transitional-period-esma-sets-out-its-expectations-professionals-and-warns-retail-investors>
- [5] Bank for International Settlements. (2025). The next-generation monetary and financial system. In *Annual economic report 2025*. <https://www.bis.org/publications/aer-2025/next-generation-monetary-financial-system>
- [6] BlockEden. (2026, March 9). *Agentic commerce revolution: When AI agents start spending your money*. <https://blockeden.xyz/blog/2026/03/09/agentic-commerce-revolution-ai-agents-payments/>
- [7] Caldarelli, G. (2020). Understanding the blockchain oracle problem: A call for action. *Information*, 11(11), Article 509. <https://doi.org/10.3390/info11110509>
- [8] Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. *Communications of the ACM*, 63(7), 80–90. <https://doi.org/10.1145/3359552>
- [9] Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13, Article e00151. <https://doi.org/10.1016/j.jbvi.2019.e00151>
- [10] Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, 32(5), 1754–1797. <https://doi.org/10.1093/rfs/hhz007>
- [11] de Vries, A. (2018). Bitcoin's growing energy problem. *Joule*, 2(5), 801–805. <https://doi.org/10.1016/j.joule.2018.04.016>
- [12] Dinh, T. N., & Thai, M. T. (2018). AI and blockchain: A disruptive integration. *Computer*, 51(9), 48–53. <https://doi.org/10.1109/MC.2018.3620971>
- [13] Ethereum Foundation. (n.d.). *The Merge*. [ethereum.org](https://ethereum.org/en/upgrades/merge/). Retrieved October 14, 2026, from <https://ethereum.org/en/upgrades/merge/>
- [14] European Parliament & Council. (2023). Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets. *Official Journal of the European Union*, L 150, 40–205.
- [15] European Parliament & Council. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence. *Official Journal of the European Union*, L, 2024/1689.
- [16] Financial Stability Board. (2025a, October 16). *Thematic review on FSB global regulatory framework for crypto-asset activities*. <https://www.fsb.org/2025/10/thematic-review-on-fsb-global-regulatory-framework-for-crypto-asset-activities/>
- [17] Financial Stability Board. (2025b, October 10). *Monitoring adoption of artificial intelligence and related vulnerabilities in the financial sector*. <https://www.fsb.org/uploads/P101025.pdf>
- [18] Foley, S., Karlsen, J. R., & Putnıř, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798–1853. <https://doi.org/10.1093/rfs/hhz015>
- [19] ForkLog. (2026). *European Parliament committee backs digital euro bill*. <https://forklog.com/en/?p=99083>
- [20] Fortune. (2025, December 18). *North Korea stole a record amount of crypto—again: Report estimates its hackers' 2025 haul at \$2 billion*. <https://fortune.com/2025/12/18/north-korea-stole-a-record-amount-of-crypto/>

- [21] Fuster, A., Goldsmith-Pinkham, P., Ramadorai, T., & Walther, A. (2022). Predictably unequal? The effects of machine learning on credit markets. *The Journal of Finance*, 77(1), 5–47. <https://doi.org/10.1111/jofi.13090>
- [22] FXStreet. (2026, July 6). *Reality of RWA tokenization in 2026: Only one asset class is ready for prime time*. <https://www.fxstreet.com/cryptocurrencies/news/reality-of-rwa-tokenization-in-2026-only-one-asset-class-is-ready-for-prime-time-202607061400>
- [23] Gibson, Dunn & Crutcher LLP. (2026). *EU AI Act omnibus agreement: Postponed high-risk deadlines and other key changes* [Client alert]. <https://www.gibsondunn.com/eu-ai-act-omnibus-agreement-postponed-high-risk-deadlines-and-other-key-changes/>
- [24] Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), Pub. L. No. 119-27 (2025).
- [25] KuCoin News. (2026). *Tokenized assets reach \$346B across 47 asset types*. <https://www.kucoin.com/news/flash/tokenized-assets-reach-346b-across-47-asset-types>
- [26] Markets Media. (2026, August 17). *US Treasury seeks comment on GENIUS Act rulemaking*. <https://www.marketsmedia.com/us-treasury-seeks-comment-on-genius-act-rulemaking/>
- [27] Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM Computing Surveys*, 54(6), 1–35. <https://doi.org/10.1145/3457607>
- [28] Mishra, D., Mishra, R. K., & Agarwal, R. (2026a). *AI-driven smart systems in business management*, In Book: *Artificial Intelligence and Beyond: Data, Computing and Smart Systems*. Bhumi Publishing. ISBN: 978-81-69967-09-9, ISBN: 978-81-69967-09-9, 64-75.
- [29] Mishra, D., Mishra, R. K., & Agarwal, R. (2026b). The alignment problem and the architecture of trust, In Book: *Co-Intelligence: Human-AI Coexistence in the Age of Thinking Machines*. Deep Science Publishing. E-Book ISBN-13 (15)- 978-93-7185-166-4, Book (Paperback) ISBN-13 (15), 978-93-7185-178-7, <https://doi.org/10.70593/978-93-7185-166-4>, 45-50.
- [30] Mishra, D., Mishra, R. K., & Agarwal, R. (2026c). Artificial Intelligence and Management: Rethinking Strategy, Decision-Making and Organizational Design in the Age of Intelligent Systems, *International Journal of Science Architecture Technology and Environment* 3(9):675-695, DOI: 10.63680/ijstate092652.44.
- [31] Mishra, D., Mishra, R. K., & Agarwal, R. (2026d). Data governance for intelligent systems, In book: *Computing Beyond Algorithms: AI, Data and Intelligent Systems*, Volume I, First Edition, July 2026, ISBN: 978-93-47587-47-4, 9-26.
- [32] Mishra, D., Mishra, R. K., & Agarwal, R. (2026e). Digital transformation and sustainable business models: An integrated framework for value creation in the digital economy, In Book: *Digital Business and Sustainable Management: Emerging Trends and Practices*. Edition: First, Chapter: 4, Bhumi Publishing. ISBN: 978-81-69967-09-9, ISBN: 978-93-47587-84-9, 29-50.
- [33] Mishra, D., Mishra, R. K., & Agarwal, R. (2026f). Fairness, bias, and justice in algorithmic systems, In Book: *Co-Intelligence: Human-AI Coexistence in the Age of Thinking Machines*. Deep Science Publishing. E-Book ISBN-13 (15)- 978-93-7185-166-4, Book (Paperback) ISBN-13 (15), 978-93-7185-178-7, <https://doi.org/10.70593/978-93-7185-166-4>, 51-55.
- [34] Mishra, D., Mishra, R. K., & Agarwal, R. (2026g). Governance frameworks for the age of AI, In Book: *Co-Intelligence: Human-AI Coexistence in the Age of Thinking Machines*. Deep Science Publishing. E-Book ISBN-13 (15)- 978-93-7185-166-4, Book (Paperback) ISBN-13 (15), 978-93-7185-178-7, <https://doi.org/10.70593/978-93-7185-166-4>, 69-75.
- [35] Mishra, D., Mishra, R. K., & Agarwal, R. (2026h). Power concentration and the political economy of AI, In Book: *Co-Intelligence: Human-AI Coexistence in the Age of Thinking Machines*. Deep Science Publishing. E-Book ISBN-13 (15)- 978-93-7185-166-4, Book (Paperback) ISBN-13 (15), 978-93-7185-178-7, <https://doi.org/10.70593/978-93-7185-166-4>, 96-99.
- [36] Mishra, D., Mishra, R. K., & Agarwal, R. (2026i). The Role of Artificial Intelligence in Socio-Economic Growth and Development, *International Journal of Science, Architecture, Technology, and Environment*, ISSN 3048-8222, Volume 3, Issue 07, July 2026, 846-859.
- [37] Mishra, R. K., Mishra, D., & Agarwal, R. (2026j). AI in law, finance, and environmental governance, In Book: *Co-Intelligence: Human-AI Coexistence in the Age of Thinking Machines*. Deep Science Publishing. E-Book ISBN-13

- (15)- 978-93-7185-166-4, Book (Paperback) ISBN-13 (15), 978-93-7185-178-7, <https://doi.org/10.70593/978-93-7185-166-4>, 103-106.
- [38] Mishra, R. K., Mishra, D., & Agarwal, R. (2026k). Institutional design for the co-intelligent society, In Book: Co-Intelligence: Human-AI Coexistence in the Age of Thinking Machines. Deep Science Publishing. E-Book ISBN-13 (15)- 978-93-7185-166-4, Book (Paperback) ISBN-13 (15), 978-93-7185-178-7, <https://doi.org/10.70593/978-93-7185-166-4>, 107-109.
- [39] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>
- [40] Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. *IEEE Access*, 7, 10127–10149. <https://doi.org/10.1109/ACCESS.2018.2890507>
- [41] Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, 103(2), 153–174. <https://doi.org/10.20955/r.103.153-74>
- [42] Secure Privacy. (2026). *EU AI Act Digital Omnibus: The new high-risk AI deadlines after Council approval*. <https://secureprivacy.ai/blog/eu-ai-act-digital-omnibus-the-new-high-risk-ai-deadlines-after-council-approval>
- [43] Stablecoin Insider. (2026a). *Coinbase opens USDC payments from AI agents to all business customers via x402*. <https://stablecoininsider.org/coinbase-usdc-payments-ai-agents-x402/>
- [44] Stablecoin Insider. (2026b, June 11). *Stablecoin developer ecosystem report 2026: Market size, APIs, SDKs & regulation*. <https://stablecoininsider.org/stablecoin-developer-ecosystem-report-2026/>
- [45] Stablecoin Insider. (2026c). *Stablecoin market report: July 2026*. <https://stablecoininsider.org/stablecoin-market-report-july-2026/>
- [46] Sumsub. (2026, July 13). *Digital euro proposal advances to final EU negotiations*. <https://sumsub.com/media/news/digital-euro-proposal-advances-to-final-eu-negotiations/>
- [47] The Block. (2026a, February 25). *Stripe co-founder predicts 'torrent' of AI agent commerce powered by stablecoins*. <https://www.theblock.co/post/391244/stripe-co-founder-predicts-torrent-of-ai-agent-commerce-powered-by-stablecoins>
- [48] The Block. (2026b, July 18). *US regulators miss GENIUS Act's one-year deadline for final stablecoin rules*. <https://www.theblock.co/post/408843/us-regulators-miss-genius-act-deadline>
- [49] Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.
- [50] Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, 21(1), 7–31. <https://doi.org/10.1093/rof/rfw074>
- [51] Zetsche, D. A., Buckley, R. P., & Arner, D. W. (2018). The distributed liability of distributed ledgers: Legal risks of blockchain. *University of Illinois Law Review*, 2018(4), 1361–1406.