Distributed Ledger Technology in Financial Transactions: A Mechanism-Oriented Review of Architecture, Risk, and Governance

Distributed Ledger Technology in Financial Transactions

Juan Wang[1,2,*], Li Wang[3]

[1]School of Economics and Management, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[2]Blockchain and Digital Finance Committee, Beijing Computer Federation, Beijing 100083, China
[3]School of Electronic Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

*Corresponding author's email: jane@xupt.edu.cn

Abstract. Distributed ledger technology (DLT) is increasingly being considered for payment, settlement, asset registration, and compliance processes. However, much of the existing discussion remains project-centred and offers limited explanation of why similar technologies produce different outcomes across public, consortium, and permissioned systems. This review develops a mechanism-oriented framework that connects ledger architecture with financial function, risk transmission, and governance design. A structured review and comparative case analysis are used to examine consensus, smart contracts, oracles, zero-knowledge proofs, and cross-ledger interoperability. The findings show that consensus design shapes settlement finality and accountability; programmable execution can reduce reconciliation but also converts specification and oracle errors into immediate operational losses; privacy-enhancing proofs can support selective compliance; and interoperability may widen liquidity access while introducing bridge, finality, and legal-mapping risks. DLT creates value when a shared record is tied to enforceable off-chain rights, custody duties, validator responsibilities, and workable intervention procedures. It should therefore be understood less as a substitute for financial intermediaries than as a coordination infrastructure for regulated multi-party transactions.

Keywords: distributed ledger technology, blockchain, financial transactions, tokenisation, smart contracts, zero-knowledge proofs, interoperability

1 Introduction

Financial transactions are not merely messages transmitted between accounts. They are institutional processes through which obligations are created, verified, transferred, and

© The Author(s) 2026
V. Erokhin et al. (eds.), *Proceedings of the 6th International Conference on Internet Finance and Digital Economy (ICIFDE 2026)*, Advances in Economics, Business and Management Research 412,
https://doi.org/10.2991/978-94-6239-830-6_9

discharged. A securities transfer, collateral pledge, token redemption, or cross-border payment becomes reliable only when the relevant parties recognise the same transaction state. Conventional infrastructures achieve this through banks, clearing houses, custodians, registrars, and regulators. These arrangements provide legal certainty, but they also require repeated reconciliation because multiple institutions maintain separate records of the same economic event.

DLT offers a different coordination model. Rather than requiring every participant to update a private ledger and reconcile discrepancies after the event, authorised participants can validate and update a shared record under agreed technical and governance rules. This does not remove the need for financial intermediaries. In regulated markets, intermediaries also perform identity verification, custody, liquidity management, dispute resolution, and regulatory reporting. The relevant question is therefore narrower: which transaction states can be produced more efficiently through a shared ledger, and which functions still depend on legal and institutional support [1, 2]?

Previous reviews frequently discuss public blockchains, wholesale central bank money, stablecoin regulation, and tokenised securities as separate developments. That mapping is useful, but it does not explain why the same technological vocabulary leads to different outcomes in public chains, consortium networks, permissioned ledgers, and unified-ledger proposals. Public chains prioritise open participation and composability; institutional networks prioritise identity, confidentiality, and accountable validation; unified-ledger proposals emphasise atomic settlement among regulated entities. Their mechanisms, benefits, and failure modes are therefore not interchangeable [3–6].

This paper adopts a mechanism-oriented perspective organised around four linked dimensions: transaction-state production, trust generation, risk transmission, and governance embedding. Its contribution is threefold. First, it replaces a catalogue of projects with a common framework for evaluating transaction mechanisms. Second, it explains core technologies at the level required to understand their financial consequences. Third, it traces how technical and legal defects can propagate into liquidity, ownership, compliance, and confidence risks.

2 Research Design and Review Method

The study combines a structured literature review with comparative case interpretation. The evidence base covers four groups of sources: standards and policy materials from international organisations and regulators; technical documentation from blockchain foundations and open-source communities; peer-reviewed research on blockchain, privacy, and financial market infrastructure; and publicly documented institutional cases involving tokenised assets, settlement, stablecoins, or regulatory technology [2–6].

Search terms combined technical concepts with financial applications. The technical terms included distributed ledger technology, blockchain, consensus, proof-of-stake, Byzantine fault tolerance, smart contract, oracle, zero-knowledge proof, rollup, bridge, and interoperability. The application terms included clearing, settlement, cross-border payment, stablecoin, tokenised deposit, tokenised securities, real-world assets, custody, compliance, and regulatory technology. Priority was given to materials published from

2021 to 2026, a period in which the policy debate shifted from isolated blockchain experiments towards infrastructure-oriented tokenisation and stablecoin regulation.

Screening proceeded in three stages. First, items concerned only with cryptocurrency prices, promotional claims, or corporate announcements lacking technical or regulatory detail were excluded. Second, retained sources had to address at least one infrastructure issue, such as ledger architecture, settlement finality, asset representation, privacy design, legal recognition, custody, or compliance. Third, the remaining materials were coded by technical architecture, financial function, asset form, risk mechanism, and governance requirement. Each case was then examined through the same questions: what state is recorded, who may update it, how finality is achieved, what off-chain claim is represented, how failure may spread, and what governance arrangement is required.

The comparative procedure focuses on mechanisms and boundary conditions rather than reproducing project descriptions. Public documents are treated as evidence for a shared analytical structure, allowing similarities and differences to be tested across cases. This approach also limits dependence on the language of individual reports and makes the paper's analytical claims easier to distinguish from source summaries.

3 Analytical Framework

Table 1. Mechanism-oriented framework for reviewing DLT in financial transactions [1, 2, 6]

Dimension	Core question	Observed variables	Financial implication
Transaction state	What is recorded and when is it final?	balance, ownership, pledge, obligation, redemption status	defines settlement certainty and enforceable claims
Trust generation	Why do participants accept the record?	consensus, identity, validator rules, custody, audit trails	reduces reconciliation while requiring accountability
Risk transmission	How can a local failure spread?	code defects, oracle error, bridge failure, liquidity stress, legal ambiguity	turns technical or legal defects into financial losses
Governance embedding	How are rules enforced?	permissions, compliance checks, reporting, dispute handling, emergency controls	aligns automation with regulation and resilience

Table 1 organises the review around the economic function of a ledger. Transaction state identifies the object produced by the system. Trust generation explains why participants accept that state. Risk transmission describes how a local defect becomes a financial loss. Governance embedding considers how automated processes remain aligned with compliance, supervision, and market stability. The framework therefore avoids treating decentralisation as the sole evaluation criterion. In financial transactions, an architecture is useful only when it supports finality, confidentiality, accountability, legal recognition, and resilience in the relevant setting [1, 2, 6].

DLT applications also differ in the type of state they seek to stabilise. A cross-border payment platform coordinates payment, compliance, and settlement states; a tokenised-

securities platform coordinates ownership, transfer, and redemption states; and a supply-chain-finance platform coordinates trade-document and collateral states. Treating these cases as equivalent would conceal the distinct legal and operational assumptions on which each system depends.

4 Technical Mechanisms of Financial DLT

Consensus is the process through which distributed nodes agree on transaction validity and ordering. In finance, it is directly connected to settlement finality. Proof-of-work supports open participation and strong resistance to unilateral alteration, but its finality is probabilistic: confidence rises as additional blocks are added. That property may be acceptable for some open digital-asset markets, but it is less suitable for high-value regulated settlement, where participants require predictable confirmation and clear responsibility allocation [1].

Proof-of-stake reduces energy use by replacing computation-intensive mining with validator stake and penalties. It can support faster confirmation and modern settlement-layer designs, but it also raises questions about validator concentration, governance influence, and the legal meaning of protocol finality. Permissioned consensus, ordering services, and notary-based validation are common in institutional finance because validators are identified and can be governed by contract and regulation. In such systems, trust rests less on open competition and more on admission rules, contractual accountability, and supervisory oversight [7].

Smart contracts express transaction conditions as executable code. In delivery-versus-payment or payment-versus-payment arrangements, they can lock assets, test predefined conditions, and execute both legs atomically. Their benefit lies in reducing manual reconciliation where conditions are precise and observable. The same precision creates risk: legal and economic judgement may be compressed into code that cannot accommodate exceptional circumstances. Vulnerabilities, excessive privileges, or unsafe upgrade procedures can therefore convert an operational error into an immediate asset loss [1].

Oracles are the principal channel through which smart contracts obtain information that is external to the ledger. Prices, interest rates, shipping records, credit events, investor eligibility, and sanctions lists are not generated by the ledger itself. Incorrect, delayed, or manipulated oracle data may cause a contract to execute a technically valid but economically incorrect transaction. Financial-grade oracle arrangements consequently require multiple data sources, accountable providers, auditable records, fallback procedures, and a controlled method for suspending execution when an external fact is disputed [1].

Zero-knowledge proofs can reconcile verification with confidentiality by allowing a participant to prove that a statement is true without disclosing all underlying data. In finance, a proof may attest to completed know-your-customer checks, investor eligibility, transaction-limit compliance, or reserve sufficiency while limiting disclosure to other participants. The technique is not a complete regulatory solution: proof circuits

may be incorrectly specified, generation costs may be material, and supervisors must understand both what the proof establishes and what remains outside its scope [2].

Cross-ledger interoperability transfers assets, messages, or proofs between otherwise separate systems. It can support multi-currency settlement and interaction between public and permissioned networks, but it also creates new points of concentration in bridges, relayers, and message layers. Where an asset is locked on one ledger and represented on another, failure of the locking contract or validator set may sever the link between the representation and the underlying asset. Differences in finality rules add further ambiguity unless finality mapping, reserve verification, and emergency controls are designed explicitly [3, 4].

5 Application Scenarios and Comparative Evaluation

Cross-border payments are a natural field for DLT experimentation because conventional processes may involve correspondent banks, repeated compliance checks, time-zone delays, and reconciliation across multiple ledgers. A shared programmable platform can coordinate payment, compliance, and settlement states. Its central mechanism is atomic settlement: the linked legs of a transaction are completed together or not at all. Implementation nevertheless depends on compatibility among legal systems, anti-money-laundering requirements, sanctions regimes, and cross-border data rules [3, 4].

Asset tokenisation represents a financial claim, instrument, or right as a programmable ledger record. Bonds, fund units, receivables, deposits, warehouse receipts, and other assets may then be issued, transferred, pledged, or redeemed through digital records. The token has economic value only when the on-chain record is connected to an enforceable off-chain claim. Whether it represents legal title, evidence of title, or a claim against an issuer or custodian must therefore be specified in the governing documentation [5, 6].

Stablecoins, tokenised deposits, and central bank digital currency can each provide the cash leg of a tokenised transaction, but their balance-sheet structures differ. Stablecoins depend on the issuer's reserves and redemption credibility. Tokenised deposits preserve a claim on a commercial bank but may alter deposit mobility and liquidity management. Central bank money offers the safest settlement asset, while raising design questions about access, privacy, and the role of commercial banks. Similar wallet interfaces should not obscure these different legal and risk structures [2, 8–10].

Supply-chain finance illustrates the boundary between ledger integrity and real-world integrity. A ledger may make an invoice, receivable, or warehouse receipt difficult to alter after entry, yet it cannot establish that the original document was genuine or that the goods existed. This is an institutional form of the oracle problem. Reliable implementation therefore depends on trusted data entry, warehouse inspection, electronic signatures, tax-invoice systems, logistics verification, and explicit liability for false information [1, 5].

Regulatory technology is another relevant application. Smart contracts and regulator-readable ledgers may improve audit trails and reporting timeliness, but the appropriate objective is selective rather than universal visibility. Supervisors need access to

evidence relevant to compliance, while market participants require protection for trading strategies, client relationships, and commercially sensitive flows. Privacy-preserving compliance is therefore a core architectural requirement rather than an optional feature [2, 11]. As shown in Table 2, the five application scenarios create value through different mechanisms and therefore require distinct governance priorities.

Table 2. Scenario comparison by value mechanism, risk mechanism, and governance focus [3–6, 8–11]

Scenario	Value mechanism	Main risk mechanism	Governance focus
Cross-border payment	synchronises payment, compliance and settlement states	jurisdictional conflict, inconsistent finality, duplicated or missing checks	cross-border rules, supervisory coordination and embedded compliance
Asset tokenisation	maps financial claims to programmable records	unclear title, custody disputes and redemption uncertainty	legal recognition, custody segregation and investor protection
Stablecoin or tokenised deposit	provides the cash leg for on-chain settlement	reserve opacity, run pressure, deposit mobility and operational concentration	issuer licensing, reserve disclosure, settlement limits and bank supervision
Supply chain finance	shares trade documents and financing status	false off-chain data, duplicate financing and weak oracle accountability	trusted data entry, warehouse audits, e-signatures and liability rules
Regulatory technology	makes reporting and audit trails programmable	privacy leakage, excessive visibility or incomplete supervisory access	selective disclosure, regulator-readable views and audit governance

6 Risk Transmission and Governance Logic

DLT risks are often classified as technical, legal, compliance, operational, and systemic. Classification alone does not explain how a local failure becomes financially material. A smart-contract defect matters when it controls assets that cannot be paused or recovered. A privacy failure matters when competitors can infer positions or client relationships. A bridge failure becomes systemic when many represented assets depend on the same verification layer. Legal ambiguity becomes costly when courts, custodians, and ledger records disagree about ownership [1, 6, 8–10].

Technical risk may propagate through code execution, validator governance, key management, data availability, oracle feeds, and cross-ledger bridges. Financial risk may propagate through liquidity concentration, redemption pressure, leverage, collateral valuation, and confidence effects. Legal and compliance risk may propagate through uncertain title, unclear custody responsibility, cross-border data transfer, and inconsistent supervisory treatment. These channels interact: a code exploit may trigger withdrawals, liquidity stress, and disputes over loss allocation.

Governance should therefore be designed at the level of transaction mechanisms. Identity and admission rules determine who may participate and who can be held accountable. Transaction controls—including code audits, permission management, upgrade procedures, and pause functions—limit uncontrolled automation. Privacy controls balance confidentiality with regulatory visibility. Asset controls define custody, segregation, recovery, and redemption. Interoperability controls map finality across

ledgers and verify represented assets. Crisis-response controls establish escalation, reporting, and resolution procedures [1, 2, 6, 11].

A workable governance model also requires responsibility mapping. Each critical function should have an accountable operator or clearly defined accountable group. Developers, validators, custodians, bridge operators, data providers, and compliance gateways are not interchangeable technical components. Their duties should be specified through contracts, regulatory obligations, audit trails, and emergency procedures, so that participants know how losses will be allocated after key compromise, oracle error, validator failure, or erroneous code execution. As shown in Table 3, these responsibilities can be organised into six control layers covering identity, transactions, privacy, assets, interoperability, and crisis response.

Table 3. Governance controls for financial-grade DLT systems [1, 2, 6, 11]

Layer	Control measure	Problem addressed	Expected result
Identity and admission	licensed participants, KYC, validator qualification	anonymous or unsuitable participation	clear accountability and compliance base
Transaction control	smart-contract audit, permission rules, pause function	code error and unauthorised operation	safe automation and recoverability
Data and privacy	selective disclosure, ZKP, encrypted channels	privacy leakage or excessive opacity	balanced confidentiality and verifiability
Asset and custody	legal mapping, key custody, segregation, recovery rules	uncertain title and loss allocation	enforceable asset rights
Interoperability	bridge audit, finality mapping, message authentication	cross-chain contagion and settlement ambiguity	controlled connectivity
Supervision and crisis response	regulatory nodes, reporting, emergency procedures	delayed detection and disorderly resolution	resilience under stress

7 Discussion

The analysis suggests that DLT adoption should not be framed as a binary choice between decentralisation and centralisation. Public chains enable open participation and composability but present challenges for confidentiality, compliance, and accountable intervention. Permissioned ledgers provide identity and control but may reproduce conventional coordination problems when governance is too closed. Unified-ledger and hybrid architectures seek to combine shared state with institutional safeguards, although they require demanding legal and regulatory coordination [2, 3, 7, 10].

A more useful standard is fitness for transaction purpose. A retail payment system, wholesale settlement platform, tokenised bond registry, and supply-chain-finance ledger should not be judged by a single decentralisation metric. They should be assessed by whether they produce a reliable transaction state, reduce reconciliation without concealing concentration risk, protect confidentiality while permitting supervision, and assign responsibility when failure occurs.

Adoption should consequently be incremental. The strongest candidates are not necessarily projects that seek to rebuild the financial system at once, but processes in which reconciliation costs are high, several institutions require a shared view of the same state,

and legal rights can be mapped clearly to digital records. Wholesale settlement, tokenised fund administration, collateral management, audit trails, and selected supply-chain-finance processes are plausible starting points [3–6, 10, 12, 13].

Implementation should also proceed through staged testing. An initial pilot can verify data standards, access permissions, and legal documentation. A second stage can test settlement logic, exception handling, and reporting interfaces with a limited group of participants. Connection to larger market processes should occur only after the system has demonstrated how it handles failed transactions, incorrect data, key loss, participant default, and emergency intervention. This sequence prevents a technically successful prototype from being mistaken for production-ready financial infrastructure.

Standardisation is a further condition for scale. Token definitions, data schemas, wallet controls, finality rules, custody duties, and proof formats must be intelligible across institutions and jurisdictions. Without shared standards, each platform may become a closed ledger, replacing one reconciliation problem with another. Interoperability should therefore be treated as a legal and governance problem as well as a protocol-design problem [5, 6, 11–13].

8 Conclusion

This review has organised research on DLT in financial transactions around transaction-state production, trust generation, risk transmission, and governance embedding. Its central argument is that DLT is best understood as infrastructure for coordinating transaction state among regulated participants. Its value lies in shared records, programmable settlement, and auditability—not in the automatic elimination of intermediaries.

The technical comparison shows that consensus determines finality and accountability; smart contracts support conditional automation but depend on reliable external data and intervention procedures; zero-knowledge proofs can support selective compliance; and interoperability may widen liquidity access while creating bridge and finality risks. These technical defects become financial losses when they affect assets, liquidity, legal rights, or market confidence [1, 3, 7, 11, 13].

Large-scale adoption requires technical, legal, and institutional conditions to be satisfied together. Systems need robust finality, privacy, key security, data availability, and audited code. Tokenised claims must be mapped to enforceable ownership, custody, and redemption rights. Regulators and market operators must define participant admission, embedded compliance, selective disclosure, cross-border coordination, and crisis response. Without this joint design, DLT is likely to remain a collection of pilots rather than dependable financial market infrastructure [2, 5, 6, 8–13].

Future empirical work should test the framework against operational data from tokenised settlement, privacy-preserving supervision, and regulated interoperability projects. Particular attention should be paid to exception handling, concentration in validation and bridge services, and the legal treatment of ledger records when technical finality conflicts with off-chain rights.

References

1. People's Bank of China. 2020. Financial Distributed Ledger Technology Security Specification (JR/T 0184—2020). Financial Industry Standard of the People's Republic of China, Beijing, China. Published and effective 5 February 2020. https://www.biaozhun.org/hangye/153218.html
2. Bank for International Settlements. 2025. The next-generation monetary and financial system. In BIS Annual Economic Report 2025, Chapter III. Bank for International Settlements, Basel, Switzerland. https://www.bis.org/publ/arpdf/ar2025e3.htm
3. Bank for International Settlements and Institute of International Finance. 2026. Project Agorá: A Shared Programmable Platform for Wholesale Cross-Border Payments. BIS Innovation Hub Other, Bank for International Settlements, Basel, Switzerland, 97 pages. https://www.bis.org/publ/othp110.htm
4. Bank for International Settlements Innovation Hub. 2022. Project mBridge: Connecting Economies through CBDC. BIS Innovation Hub Other Papers No. 59, Bank for International Settlements, Basel, Switzerland. https://www.bis.org/publ/othp59.htm
5. OECD. 2025. Tokenisation of Assets and Distributed Ledger Technologies in Financial Markets: Potential Impediments to Market Development and Policy Implications. OECD Business and Finance Policy Papers, No. 75. OECD Publishing, Paris, France. https://doi.org/10.1787/40e7f217-en
6. International Organization of Securities Commissions. 2025. Tokenization of Financial Assets. Final Report FR/17/2025. IOSCO, Madrid, Spain, 73 pages. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD809.pdf
7. Ethereum Foundation. 2024. Cancun-Deneb (Dencun). Ethereum.org, activated on Ethereum mainnet 13 March 2024. https://ethereum.org/roadmap/dencun/
8. European Parliament and Council of the European Union. 2023. Regulation (EU) 2023/1114 of 31 May 2023 on Markets in Crypto-assets, and Amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. Official Journal of the European Union L 150 (9 June 2023), 40–205. http://data.europa.eu/eli/reg/2023/1114/oj
9. Hong Kong Monetary Authority. 2025. Regulatory Regime for Stablecoin Issuers. Hong Kong Monetary Authority, Hong Kong. Regime effective 1 August 2025. https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/stablecoin-issuers/
10. Monetary Authority of Singapore. 2025. Project Guardian. Monetary Authority of Singapore, Singapore. https://www.mas.gov.sg/schemes-and-initiatives/project-guardian
11. Bank for International Settlements Innovation Hub. 2024. Project Mandala: Streamlining Cross-Border Transaction Compliance. BIS Innovation Hub Other Papers No. 87, Bank for International Settlements, Basel, Switzerland. https://www.bis.org/publ/othp87.htm
12. Iota Kaousar Nassr. 2021. Understanding the Tokenisation of Assets in Financial Markets. OECD Going Digital Toolkit Notes, No. 19. OECD Publishing, Paris, France. https://doi.org/10.1787/c033401a-en
13. Tobias Adrian. 2026. Tokenized Finance. IMF Notes 2026/001. International Monetary Fund, Washington, DC. https://doi.org/10.5089/9798229042468.068

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

