Cleanverse

INSTITUTIONAL TRUST

The Foundation for On-Chain Finance



WHITEPAPER | NOVEMBER 2026

Institutional trust as a shared foundation for regulated on-chain finance

Publication Information & Disclaimer

INSTITUTIONAL TRUST | THE FOUNDATION FOR ON-CHAIN FINANCE

PUBLISHER	Cleanverse International Pte Ltd
PUBLICATION	Whitepaper | November 2026
WEBSITE	www.cleanverse.com
ENQUIRIES	contact@cleanverse.com
CONTRIBUTIONS	See Acknowledgements for contributors recognized in this paper

Disclaimer

This publication is provided for information and industry discussion. It proposes principles and a potential validation pathway for institutional trust in on-chain finance; it does not constitute legal, financial or regulatory advice, or prescribe a binding industry standard.
The views, proposals and illustrative architectures described in this paper should not be taken to represent the official position, approval or endorsement of any financial institution, regulatory authority or other contributing party, except where expressly stated. Institutions remain responsible for their own applicable legal, regulatory, governance and risk-management obligations.

Attribution And Contributions

This whitepaper is developed and published by Cleanverse International Pte Ltd. Contributors are recognised in the Acknowledgements section. Attribution reflects their contributions to industry discussion and does not, by itself, imply co-authorship of, or endorsement of every proposal or implementation in, this publication.

Copyright And Permissions

Copyright © 2026 Cleanverse International Pte Ltd. All rights reserved, except where separately attributed. For permission requests and other correspondence, please contact contact@cleanverse.com.

Executive summary

Finance is moving onto programmable infrastructure. Stablecoins, tokenised deposits, tokenised securities, real-world assets and autonomous agents expand the ways in which value can be issued, held and transferred. Yet institutional participation depends on something that execution infrastructure alone does not provide: a consistent basis for trusting the participants, the assets and the conditions governing a transaction.

This paper proposes Institutional Trust as that common foundation. Institutional Trust is the ability to rely on accountable, sufficiently current evidence about identity and authority, the asset or claim being transacted, and the policy applicable to the proposed action - before value moves. It does not replace an institution's legal, regulatory or risk responsibilities; it provides a common structure through which those responsibilities can be expressed and applied across institutional boundaries.

The paper proposes **Five Principles for Institutional Trust**: *Verified Identity, Verified Assets, Programmed Policy, Institutional Accountability and Interoperable Trust.* They describe outcomes that different infrastructures may implement while allowing institutions to preserve their own customer relationships, acceptance decisions and governance obligations.

From those Principles follows the proposition for an **Institutional Trust Network (ITN).** ITN is not defined here as one proprietary platform or ledger. It is the network effect that arises when institutions can issue, recognise and rely on common trust evidence, and apply policy consistently enough for value to move across participating institutions and approved infrastructure. As participation grows, the value of reusable trust evidence and common semantics increases, while the need to recreate bespoke bilateral trust arrangements can fall.

The longer-term objective is a **Common Trust Standard**: a minimum specification for identity evidence, asset information, policy decisions, execution binding, records and operational governance. The Standard should support multiple technologies, assets and ledgers.

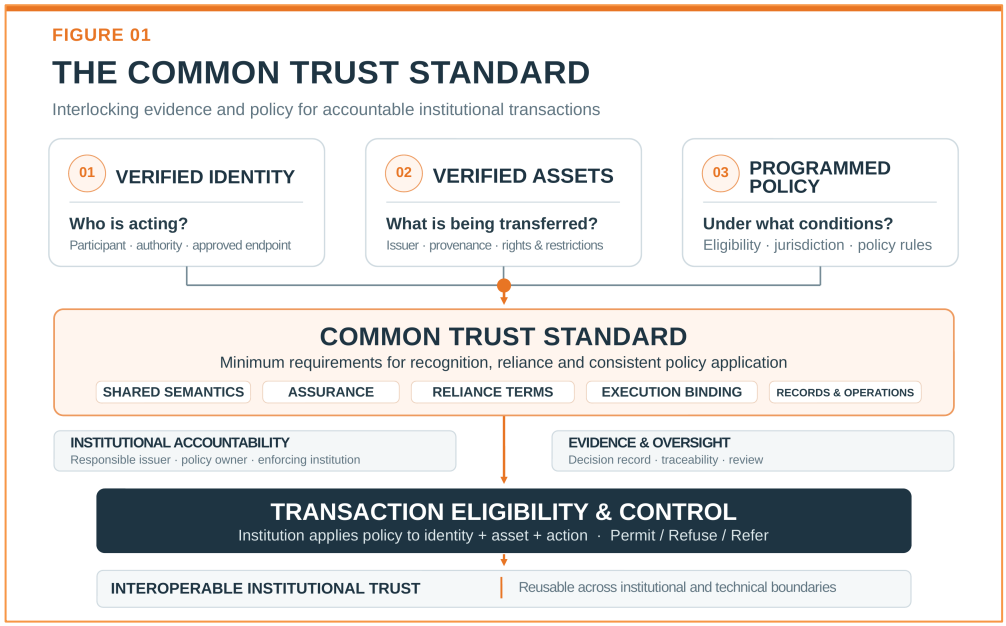


Fig 1: The proposed Common Trust Standard integrates verified identity, verified assets and programmed policy through shared semantics and assurance conditions. It supports accountable transaction decisions and interoperable institutional trust.

Contents

Part I The institutional trust imperative

Ch 1: Why institutional trust must become portable

Ch 2: Industry Foundations

Ch 3: Policy and market developments

Part II Principles for Institutional Trust

Ch 4: The five Principles

Ch 5: From evidence to an enforceable decision

Part III From institutional adoption to a network

Ch 6: The Institutional Trust Network proposition

Ch 7: Common trust across financial applications

Ch 8: Toward a Common Trust Standard

Part IV Reference implementation

Ch 9: Cleanverse as a reference implementation

Ch 10: Validation pathway

Conclusion

References, definitions and acknowledgements

PART I THE INSTITUTIONAL TRUST IMPERATIVE

01 Why institutional trust must become portable

Tokenisation changes how financial claims are recorded and operated, but not the need to establish who is acting, what rights or value are involved, and which conditions govern the action. A valid blockchain instruction can establish that technical execution rules have been met; it does not by itself establish legal identity, authority, investor eligibility, asset provenance or the sufficiency of a compliance decision.

Within traditional finance, much of this trust is established inside regulated institutional relationships. Customer identity, authority, balances, entitlements and controls are connected through internal systems and operating processes. When value moves across wallets, applications, institutions and jurisdictions, that connection can fragment. Another institution may encounter a valid address or token without being able to recognise the evidence on which the originating institution relied.

This is not only an information problem. Two institutions can hold the same data yet interpret its assurance, scope or freshness differently. A credential may be authentic but no longer current; an asset may be legitimate but subject to transfer restrictions; a participant may be verified but not authorised for the proposed action. Institutional Trust therefore requires common semantics and defined conditions of reliance, not merely compatible messages.

02 Industry foundations

The proposition developed here is consistent with a wider body of work on tokenisation, technology-neutral regulation, digital credentials, policy automation and shared financial infrastructure. The references do not prescribe one architecture; together they indicate recurring requirements for accountable intermediaries, interoperable information, machine-verifiable evidence, explicit governance and controls that can operate at transaction time.

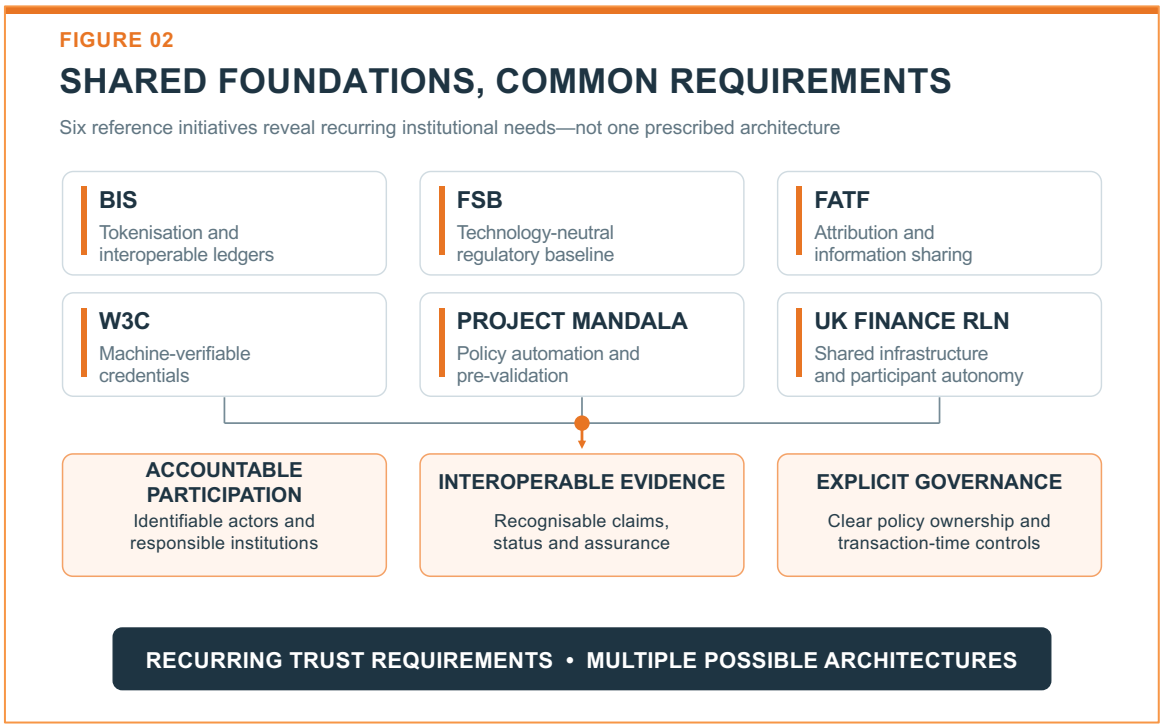


Fig 2. Selected industry and standards initiatives point to recurring needs for accountable participation, interoperable evidence and explicit governance, without prescribing a single architecture. Sources: BIS [1], FSB [2], FATF [3], W3C [4], Project Mandala [5] and UK Finance RLN [6].

The BIS has noted both the potential of tokenisation and the possibility of multiple ledgers connected through APIs rather than a single universal platform. The FSB frames its crypto-asset recommendations as a technology-neutral global baseline. FATF requirements emphasise attribution and information exchange for virtual-asset transfers. W3C Verifiable Credentials provide a standard model for machine-verifiable claims. Project Mandala demonstrates how jurisdiction-specific policy can be represented and checked through a common protocol while preserving institutional responsibility. UK Finance's RLN experimentation highlights the trade-off between shared infrastructure and participant autonomy. [1-6]

MAS Global Layer One is relevant as one example of institutional work on shared infrastructure and interoperability, but the Institutional Trust proposition is not dependent on a single ledger architecture or on GL1 adoption. [7]

03 Policy and market developments

Recent policy and industry developments point towards a common set of requirements for institutional on-chain finance: interoperability, accountable participation, programmable controls and the ability to maintain appropriate oversight as digital value moves across institutional and technical boundaries.

Singapore's BLOOM programme expanded in October 2026 with Bank Negara Malaysia and the Bank of Thailand to explore cross-border acceptance and settlement of digital money, including interoperability and programmable controls. MAS has separately identified market infrastructure and programmable compliance as important components of trusted digital financial infrastructure. [7; 8]

Regulatory attention is also extending beyond issuance towards the continuing circulation of digital value. MAS's September 2026 stablecoin consultation, for example, considers capabilities relating to tracing, freezing and burning, alongside further measures for holder identification and circulation

monitoring. These remain consultation proposals, but illustrate the growing policy focus on maintaining identity, accountability and control throughout an asset's lifecycle. [9, paragraphs 3.21-3.23 and Question 14]

Market experimentation is progressing in parallel. DBS, OCBC and UOB have completed live tokenised-deposit transactions through Swift's ledger, OCBC's GOLDX initiative uses public blockchains for tokenised investment exposure while its work with Ant International addresses treasury use of tokenised deposits.

Taken together, these developments suggest that the next phase of institutional adoption is not solely a question of enabling digital value to move. It is increasingly a question of how identity, assets and applicable policy remain trustworthy and actionable as value moves across institutional boundaries.

PART II PRINCIPLES FOR INSTITUTIONAL TRUST

04 The five Principles

The Principles define the minimum trust outcomes that should remain recognisable as financial activity crosses institutional and technical boundaries. They are intentionally independent of any single implementation.

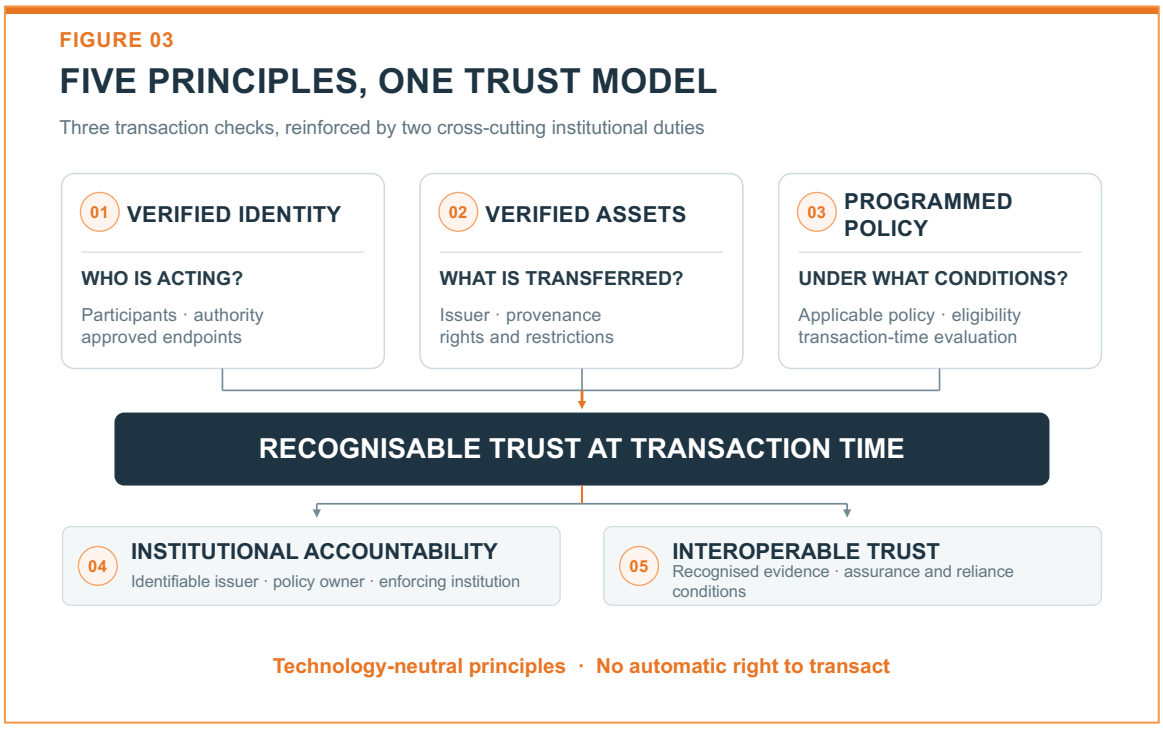


Fig 3. Verified Identity, Verified Assets and Programmed Policy establish transaction-specific trust conditions; Institutional Accountability and Interoperable Trust provide the cross-cutting obligations needed for responsible institutional reliance.

Principle	Institutional meaning
Verified Identity	Relevant participants, authority and approved transaction endpoints can be established through recognised evidence. Identity alone does not create a universal entitlement to transact.
Verified Assets	The instrument, issuer or origin, relevant provenance, rights and restrictions can be established. Recognition does not guarantee market value, creditworthiness or the legitimacy of every past holding.
Programmed Policy	Applicable requirements can be evaluated against the specific parties, asset and action before execution. A technical decision cannot exceed the legal authority of the responsible policy owner.
Institutional Accountability	The issuer of evidence, owner of policy, institution making an acceptance decision and operator enforcing it remain identifiable and responsible for their respective roles.
Interoperable Trust	Evidence and decisions can be recognised across institutional boundaries under explicit assurance and reliance conditions, without requiring common ownership of every technology component.

05 From evidence to an enforceable decision

A proposed instruction identifies the participants, asset and action. Recognised evidence establishes the relevant facts; applicable policy evaluates those facts; institutional approval is applied where required; and execution is permitted, refused or referred. Missing mandatory evidence must not silently become approval.

The approval should bind the relevant transaction context, including sender, recipient, instrument, amount, network, authority and validity window. Evidence should link the claims used, policy version, decision and execution result so that the outcome can be reconciled and reviewed. Status changes, revocation, policy updates and service outages require defined treatment.

Where restrictions are intended to continue throughout an asset's lifecycle, controls must remain effective across the supported routes by which that asset can move. The control may sit in an asset contract, a mandatory policy interface, custody arrangement or institutional admission process; the important requirement is that the stated control boundary is explicit and cannot be bypassed through another route that is represented as supported.

PART III FROM INSTITUTIONAL ADOPTION TO A NETWORK

06 The Institutional Trust Network proposition

The Institutional Trust Network (ITN) is proposed as a neutral network model created by institutional adoption of common trust semantics. It exists when multiple accountable institutions can issue and recognise trust evidence, apply their own policies using agreed meanings, and rely on transaction evidence produced through supported interfaces. No single participant needs to surrender its customer relationship, regulatory obligations or internal risk appetite.

The network effect is central. In a purely bilateral model, each new institutional relationship may require new definitions, integrations and reliance arrangements. Under a common trust model, participants can reuse agreed evidence structures and policy semantics across multiple counterparties. The objective is not universal acceptance of every credential or asset; it is a common way to express what is being asserted, by whom, at what assurance level, for how long, and under what conditions another institution may rely on it.

This makes ITN distinct from a settlement network. Settlement interoperability concerns how value moves between ledgers or liabilities. Institutional Trust concerns whether the parties can establish sufficient confidence in the participant, asset and transaction conditions before using whatever settlement mechanism is appropriate. The two can coexist but should not be conflated.

07 Common trust across financial applications

The same trust structure can support different financial activities even though their legal rights, settlement arrangements and detailed policy requirements remain distinct

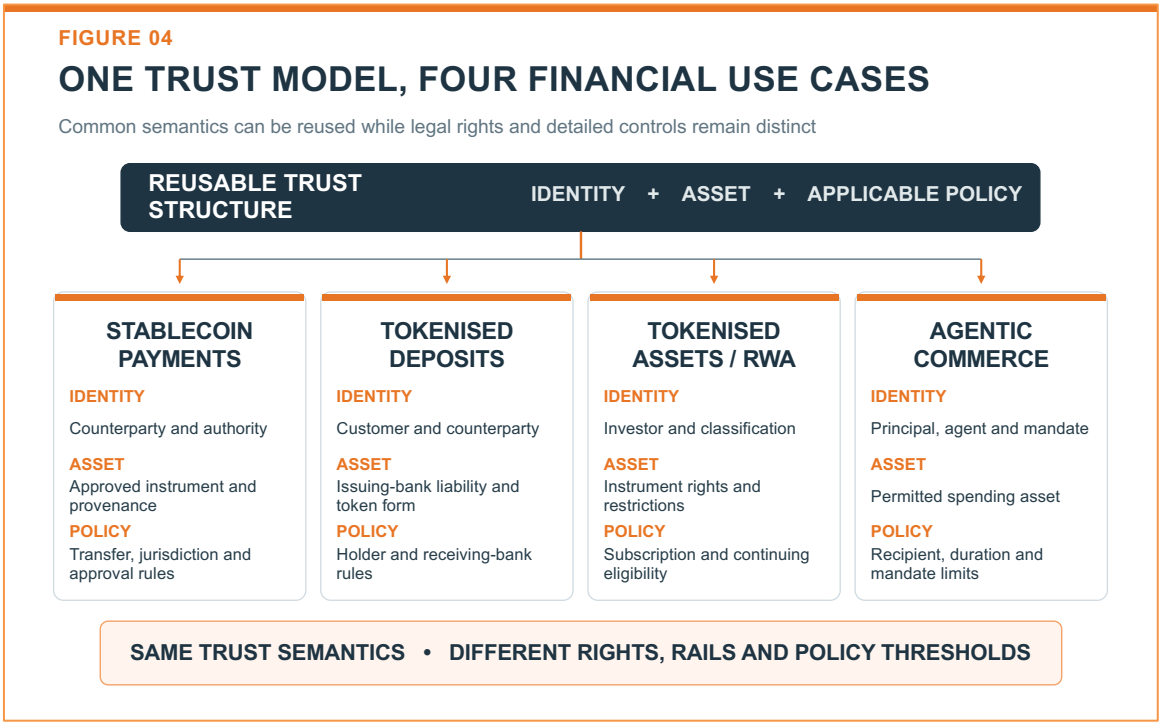


Fig 4. A reusable identity, asset and policy structure can support stablecoin payments, tokenised deposits, tokenised assets and agentic commerce, while preserving each activity's distinct legal rights, policy rules and settlement arrangements.

Activity	Identity	Asset	Policy
Stablecoin payments	Counterparty identity and authority	Approved instrument and relevant provenance	Transfer, jurisdiction, information-sharing and institutional approval rules
Tokenised deposits	Customer and permitted counterparty	Issuing-bank liability and permitted token form	Holder, transfer and receiving-institution acceptance rules
Tokenised assets / RWA	Investor, representative and classification	Instrument, legal rights and distribution restrictions	Subscription, transfer, jurisdiction and continuing eligibility
Agentic commerce	Principal, agent and current mandate	Permitted payment or spending asset	Recipient, purpose, amount, duration and aggregate mandate limits

08 Toward a Common Trust Standard

A common network requires more than compatible data formats. Institutions need to understand what a claim establishes, who is permitted to issue it, how current it must be, what supporting records exist and which party remains accountable if the claim, policy or enforcement fails. The same discipline applies to asset information and transaction decisions.

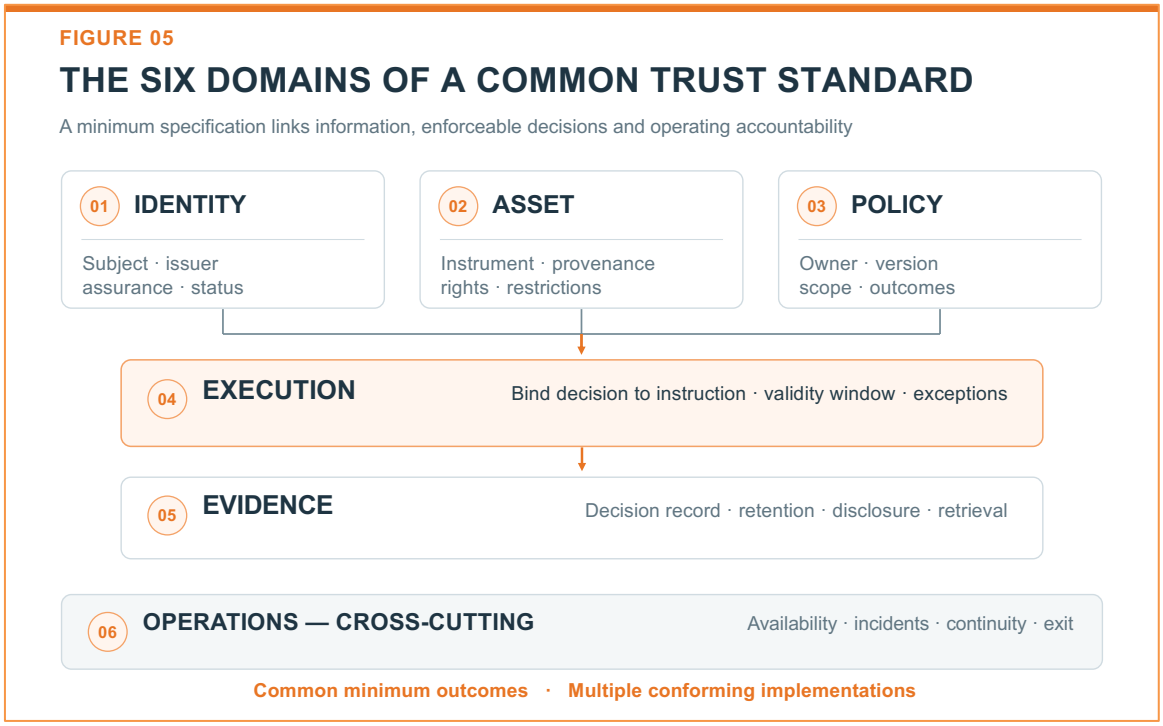


Fig 5. A proposed Common Trust Standard defines minimum requirements for identity, asset, policy, execution, evidence and operations. These requirements are intended to allow multiple technology implementations to demonstrate comparable trust outcomes

A Common Trust Standard should specify these minimum outcomes while allowing different implementations to demonstrate conformance. It should not require one blockchain, one stablecoin, one wallet architecture, one custodian or one technology provider. Institutions may impose stricter requirements where their obligations or risk appetite demand them.

The standard should therefore be judged by portability of trust, clarity of accountability, enforceability of policy and the quality of evidence - not by uniformity of technology.

PART IV REFERENCE IMPLEMENTATION

09 Cleanverse as a reference implementation

Cleanverse provides one implementation of the Institutional Trust model described in this paper. Its earlier Programmed Governance Playbook proposed an Operational Governance Framework for translating policy into controls that operate before value moves. The reference implementation applies that operating logic to institutional identity, governed assets and transaction policy.

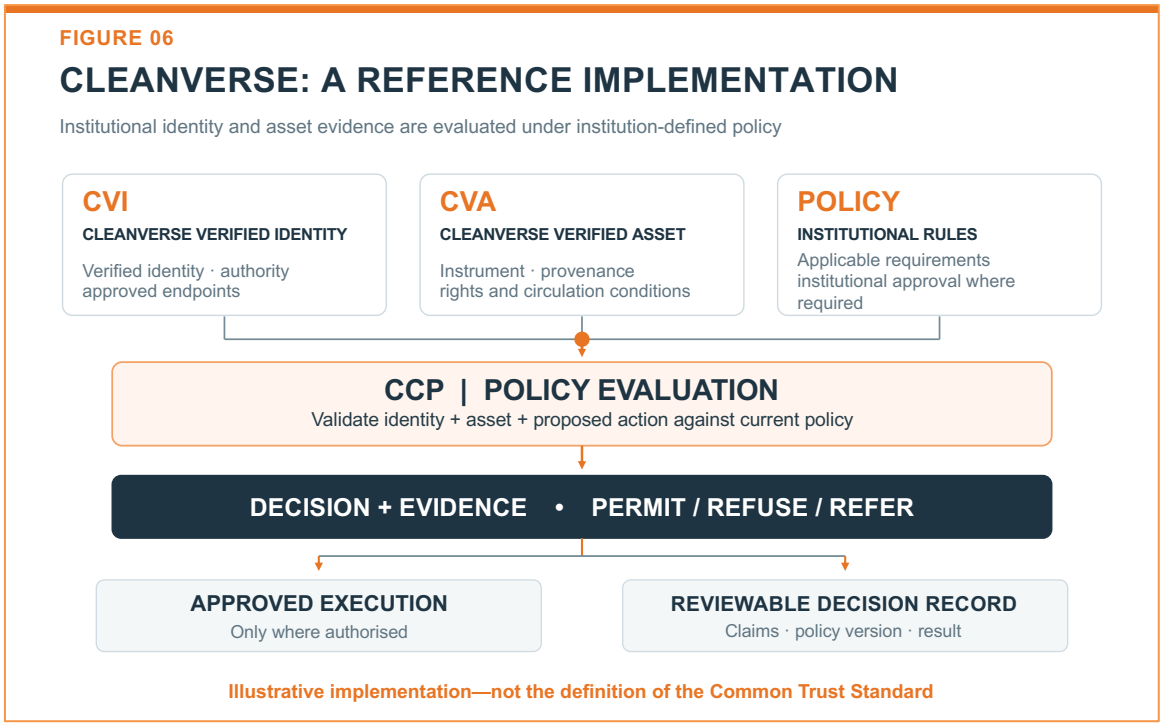


Fig 6. Cleanverse Verified Identity (CVI) and Cleanverse Verified Asset (CVA), together with institution-defined rules, are evaluated through the Cleanverse Compliance Protocol (CCP) to generate a transaction decision and reviewable evidence.

Cleanverse Verified Identity (CVI) represents verified institutional identity, relevant authority and approved endpoint relationships. Cleanverse Verified Asset (CVA) links value to instrument or origin, provenance and circulation conditions. The Cleanverse Compliance Protocol (CCP) interlocks identity and asset evidence with applicable policy so that the defined conditions can be evaluated before execution.

The implementation is designed so that source identity records remain with responsible institutions, while only the attributes required for a transaction are exposed or referenced. Policy versions, decisions and execution evidence can be retained for institutional review. The implementation can connect to institution-hosted wallets, custody arrangements, existing payment systems and approved blockchain environments; the precise control boundary depends on the use case.

This chapter is illustrative rather than normative. The Principles and proposed ITN model do not depend on the Cleanverse implementation, and alternative implementations should be able to demonstrate the same trust outcomes under comparable assurance, governance and testing requirements.

10 Validation pathway

The proposed model should be validated through bounded institutional testing rather than assumed from architecture alone. A first pilot can focus on stablecoin payments between institution-associated wallets because it creates a clear test of cross-institution identity, asset eligibility, policy evaluation and transaction evidence within a defined scope.

Scenario	Expected behaviour
Valid instruction	Correct eligibility outcome, required institutional approval and one authorised execution
Missing, stale or revoked evidence	Refusal or referral within the agreed status window
Ineligible participant or unsupported asset	Correct refusal with an interpretable reason
Changed or reused approval	No execution outside the authorised instruction
Service interruption	Controlled recovery, no duplicate execution and complete reconciliation
External or unsolicited receipt	Restricted admission until required evidence and institutional acceptance are established

Validation should measure decision accuracy, end-to-end completion and review time, revocation propagation, evidence completeness, information disclosure, reconciliation and recovery. It should also test whether common trust semantics reduce repeated integration or verification effort without weakening each institution's own control framework.

The purpose of the pilot is not to prove one product or network ready for universal deployment. It is to generate evidence about whether independently accountable institutions can recognise common trust information, apply their own policies consistently and preserve explainable decisions across an on-chain transaction.

Conclusion

The institutional challenge in on-chain finance is not simply whether a ledger can transfer value. It is whether trust can remain recognisable when value crosses institutional, application and jurisdictional boundaries. The proposed Principles for Institutional Trust provide a common foundation: Verified Identity, Verified Assets, Programmed Policy, Institutional Accountability and Interoperable Trust.

The Institutional Trust Network follows from the network effect of institutions adopting those common trust semantics. Its value grows when trust evidence can be reused and recognised across more participants without requiring those participants to standardise their entire technology stack. A Common Trust Standard is the longer-term objective through which different implementations can demonstrate the minimum behaviours required for institutional reliance.

The proposition is therefore deliberately simple: establish trust in the participant, the asset and the applicable policy before value moves; preserve accountable evidence of the decision; and make that trust portable across institutional boundaries.

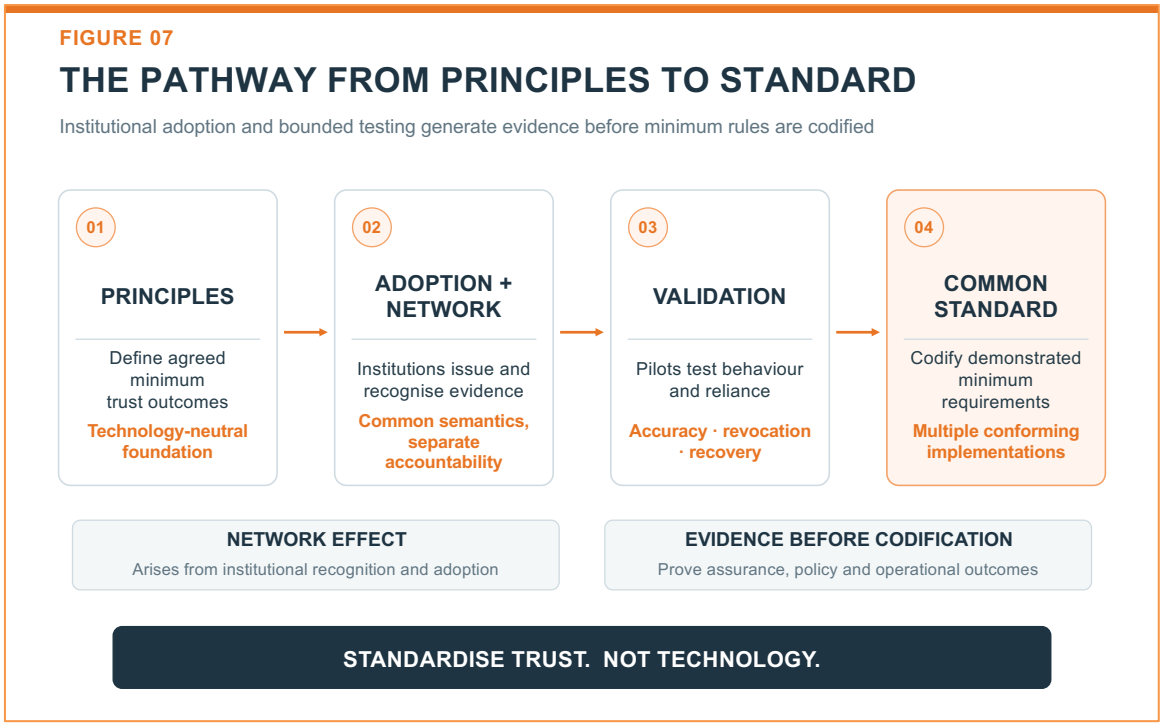


Fig 7. The proposed pathway moves from common principles to institutional adoption, bounded validation and evidence-informed standardization. The intended outcome is interoperability of trust without requiring uniform technology.

References

[1] Bank for International Settlements. Annual Economic Report 2023, Chapter III: Blueprint for the future monetary system - improving the old, enabling the new. Tokenisation, unified ledgers and interoperability through APIs.

[2] Financial Stability Board. Global Regulatory Framework for Crypto-asset Activities, July 2023. Technology-neutral, high-level recommendations and global regulatory baseline.

[3] Financial Action Task Force. Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs, October 2021; Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, July 2026.

[4] World Wide Web Consortium. Verifiable Credentials Data Model v2.0, W3C Recommendation, 15 May 2025.

[5] BIS Innovation Hub. Project Mandala: Streamlining cross-border transaction compliance, 2024; project materials updated through 2025.

[6] UK Finance. Regulated Liability Network Experimentation Phase - Summary, Technical, Business and Legal Reports, September 2024.

[7] Monetary Authority of Singapore. Global Layer One Whitepaper, May 2024

Definitions

Term	Meaning used in this paper
Institutional Trust	Justified reliance on accountable evidence about participants, assets and applicable policy for a financial action.
Institutional Trust Network (ITN)	A network model created when participating institutions can issue, recognise and rely on common trust evidence and apply policy under shared semantics.
Common Trust Standard	A technology-neutral minimum specification for the evidence, policy, execution and governance behaviours required for institutional trust interoperability.
Attestation	A claim issued by an identified party under stated assurance, validity and responsibility conditions.
Programmed Policy	Machine-evaluable expression of approved institutional or regulatory conditions applied to a defined action before execution.
Reference implementation	One technology implementation used to test whether the proposed principles and behaviours can be achieved.

Acknowledgements

This whitepaper is intended to provide a foundation for the development of institutional trust in on-chain finance and to contribute to the wider industry discussion on how trusted identity, trusted assets and applicable policy can be recognised and applied across institutional boundaries. Each institution remains responsible for determining and carrying out the due diligence and controls applicable to it under applicable laws, regulations and its own policies

Its development has benefited from contributions and perspectives from **OCBC, Paxos, Independent Reserve, DCS Group, Newrails and Prof. Zhu Feida (Chairman of Board of Directors, Blockchain Association of Singapore; Associate Dean and Associate Professor of Computer Science at Singapore Management University)** whose input has helped inform the institutional, operational and policy considerations reflected in this paper.

The co-authors recognize that the responsible development of digital asset markets requires both innovation and effective management of risks to financial stability and integrity. Progress in this area will depend on continued collaboration across the private and public sectors, including financial institutions, infrastructure providers, policymakers, regulators and other industry stakeholders.

This paper therefore seeks to provide a common starting point for further dialogue, testing and industry collaboration toward trusted and interoperable institutional participation in on-chain finance.

References to contributing organisations acknowledge their input to the development of this paper. Such participation does not constitute endorsement of any analysis, proposal, technology or implementation described herein, nor does it imply any commitment to adopt or implement the concepts or arrangements discussed, unless expressly stated otherwise.

Contributing organisations have not necessarily independently verified all information contained in this paper. The views and conclusions expressed herein are those of the authors and publisher and do not necessarily reflect the views, policies or positions of any contributing organisation. To the fullest extent permitted by applicable law, contributing organisations accept no responsibility or liability for the accuracy, completeness or reliance upon the contents of this paper, except where expressly agreed otherwise.