

SIMFONIA

Building the modular trust layer for digital finance

Vision paper by a multi-stakeholder working group

OLIVER WYMAN
A MARSH BUSINESS

GLEIF
Enabling global identity
Protecting digital trust

Contents

About SIMFONIA 3

Preface 5

Executive summary 7

Digital financial innovation is outgrowing today's institutional trust model 11

Trust functions becoming modular, portable and verifiable 23

Pathways toward modular trust for financial markets 33

Hong Kong stablecoins regulatory framework paves the way to a modular trust layer 41

Requirements: What the trust layer must and must not do 45

Recommendations for enabling modular, portable and verifiable trust 49

Open questions 57

Glossary *65*

Reading list *67*

Appendix A. Developments in digital assets and agentic payments *72*

Appendix B. Digital identity *76*

Appendix C. Proof points for four scenarios *80*

Appendix D. Hong Kong case study *84*

Appendix E. Requirements *89*

About SIMFONIA

SIMFONIA is an open, collaborative initiative convened by the Global Legal Entity Identifier Foundation (GLEIF) and Oliver Wyman. It brings together more than 40 contributors from financial institutions, digital asset and identity providers, regulators, central banks, standards bodies, technology, and academia.

The working group aims to evolve conventional approaches to how trust is established and shared in financial markets. By bringing together perspectives from across the financial ecosystem, SIMFONIA seeks to build a shared understanding of emerging challenges and opportunities and inform the industry's future development.

This initiative was prepared with financial contribution from GLEIF and Oliver Wyman.

© Oliver Wyman and GLEIF

SIMFONIA coauthors

Please contact any of the authors to learn more, share insights, or contribute to further discussions on SIMFONIA.

Ivan Mortimer-Schutts
Ivan.Mortimer@gleif.org

Pieter Verhagen
Pieter.Verhagen@oliverwyman.com

Douwe Lycklama
Douwe.Lycklama@oliverwyman.com

Yekaterina Travkina
Yekaterina.Travkina@oliverwyman.com

Acknowledgments

We thank the following individuals, among the wider group of SIMFONIA contributors, for sharing their expertise and perspectives.

Alexandre Kech
GLEIF

Gerard van der Hoeven
iSHARE

Niels van den Bergh
mintBlue

Thomas Hardjono
MIT

Anthony Ralphs
novamodus.xyz

Italo Borssatto
BIS Innovation Hub

Oliver Naegele
Blockchain Bundesverband

Thomas Mayfield
Veridian

Benjamin Chodroff
Ethereum Institutional

James Zhibin Lei
Hong Kong University of Science & Technology

Olivier Rikken
DutchZeroHumanCompany

Tim Bailey
Red Date Technology

Chengyi Ong
Circle

Jelmer Koster
Qivalis

Rene Mijs
W3Alliance

Tom Barbereau
TNO

Erwin Voloder
LTIN

Khai Uy Pham
Banque de France

Rickard Israelsson
Global vLEI

Felix Laufenberg
Fireblocks

Mert Askaroglu
BIS Innovation Hub

Ryo Takahashi
Toppan

Gerard Hartsink
Independent expert

Miroslav Milenkovic
Independent expert

Steve Pannifer
Fime

The views expressed in this report are those of the authors and do not necessarily reflect the positions of the contributors or their respective organizations.

© Oliver Wyman and GLEIF

Preface

Digital assets and agentic AI transactions are transforming the financial system. The identity architecture underpinning every transaction must now provide faster, cheaper, more granular, and fully digital answers to two fundamental questions: Who are you, and are you authorized to act?

Digital assets — including tokenized bank deposits, stablecoins, tokenized real-world assets such as securities and funds, and central bank digital currency — are increasingly becoming part of mainstream finance. Settlement is becoming programmable, and AI agents are beginning to act on behalf of people and organizations. At the same time, regulators, financial institutions, and technology providers are each adapting — often at different speeds and from different starting points.

This raises important questions.

How can we benefit from financial innovation without undermining the trust, accountability, and control on which regulated markets depend? How can policymakers adapt existing frameworks and infrastructure to preserve market integrity while potentially improving outcomes and making market supervision more effective and efficient?

How will financial markets be shaped by digital trust arrangements being developed outside the financial system? In parallel with financial innovation, policymakers and market participants are adopting innovations that enable a new generation of digital identity and data networks. How will these developments shape the new actors and services on which the financial system itself relies, and the risks it must manage, to preserve integrity and stability?

If these questions are not addressed deliberately, answers will emerge by default. This could lead to new institutional silos, proprietary platforms, jurisdiction-specific solutions or parallel markets outside the traditional financial system. These outcomes would have consequences. There are no bystanders, as the architecture of tomorrow's financial markets is being shaped now.

© Oliver Wyman and GLEIF

SIMFONIA was initiated to contribute to this discussion. Convened by GLEIF and Oliver Wyman, it has brought together more than 40 contributors from financial services, digital assets, digital identity, regulation, central banking, standards, technology, and academia. Their perspectives differ, but a common theme has emerged: in a world of portable, interoperable assets, identity also needs to become portable, verifiable, and modular. Although most of the trust functions required for financial market stability and integrity remain valid, the way in which they are delivered will need to evolve.

This paper is not a blueprint for a particular technology, identity scheme, or regulatory model. Nor is it an argument for replacing financial institutions or existing controls. It starts instead from first principles: what must remain true for trusted financial markets and transactions when assets become mobile, contracts become smart, and participants in the ecosystem cross more and more boundaries? What changes when markets become wallet-based and programmable? How could emerging forms of portable and verifiable identity, data, and trust help us improve outcomes across the board?

Many questions remain — notably around reliance, liability, cross-border recognition, governance, and sustainable economics. This is to be expected in a market still taking shape. The purpose of SIMFONIA is therefore not to present a finished architecture, but to bring greater clarity and a common understanding to the potential outcomes of market innovation and their implications for different stakeholders. This vision paper outlines areas where regulators, financial institutions, and trust providers can make progress together.

The opportunity is immediate: to shape the trust architecture while the next generation of financial markets is still being built.

© Oliver Wyman and GLEIF

Executive summary

Digital financial innovation is outgrowing today's institutional trust model.

Tokenized assets, stablecoins, and AI agents are moving into mainstream finance, enabling faster, continuous transactions, including those involving amounts currently too small to process economically. The objectives of financial regulation and supervision[1] do not change. Markets still need legal certainty, accountability, market integrity, investor protection, resilience, and auditability, alongside anti-money laundering and countering the financing of terrorism (AML/CFT) and sanctions controls.

Today, the trust functions — the checks that establish who a party is, what it may do, and whether a transaction is permitted — are anchored in an account at one institution. In digital-asset markets, addresses are created and discarded, and agents act for a principal. Treating every address and agent as a new account to onboard adds friction and undermines the benefits of speed, cost, and programmability. It also risks drawing activity back within closed institutional boundaries or pushing it outside regulated markets. SIMFONIA explores the alternative: unbundling the trust functions so they work across institutions.

Compliance stays, the mechanism changes

The trust functions do not need to be reinvented. Instead, they need to become less dependent on the institution and account in which they were first established. Identity, authority, regulatory status, and mandates can be expressed as portable, cryptographically verifiable evidence, bound to a wallet, agent, or transaction.

This works through the issuer–holder–verifier triangle: a recognized issuer signs a fact, the holder presents it, and the relying party verifies it independently. Cryptography proves origin and integrity; legal certainty comes from the framework under which the issuer operates. Before value moves, the verified evidence is bound to the specific transaction and subsequently retained as a record of what was relied upon. This does not relieve relying parties of their responsibilities: each still decides what evidence it requires, which issuers it recognizes, and whether the transaction meets its own obligations.

1 "Regulation and supervision" is shorthand for all relevant authorities and objectives, including financial intelligence units and market oversight. Where a point concerns only specific authorities, policies or mandates, we name them.

© Oliver Wyman and GLEIF

Portable assurance supports every stage of the compliance lifecycle

The SIMFONIA working group considered how portable, provable evidence could support compliance throughout the lifecycle, rather than just at onboarding, once identity and related credentials are separated from the account. We modeled a transaction in five stages: licensing check, onboarding, pre-transaction, settlement, and post-transaction. In traditional finance, checks are concentrated at onboarding, when an institution establishes identity, beneficial ownership, authority, and permissions, and after the transaction, when monitoring, holds, recalls, and disputes address what earlier checks missed.

For digital assets, settlement is often final, and whether it can be reversed depends on the asset, the ledger, and the legal regime. Pre-transfer controls therefore become more important, while monitoring, reporting, and enforcement remain necessary afterward. Licensing requirements also change: a bank proves its standing to its supervisor and a small number of bilateral counterparties, while a custodial wallet provider must demonstrate its standing to any party relying on it, for every transaction.

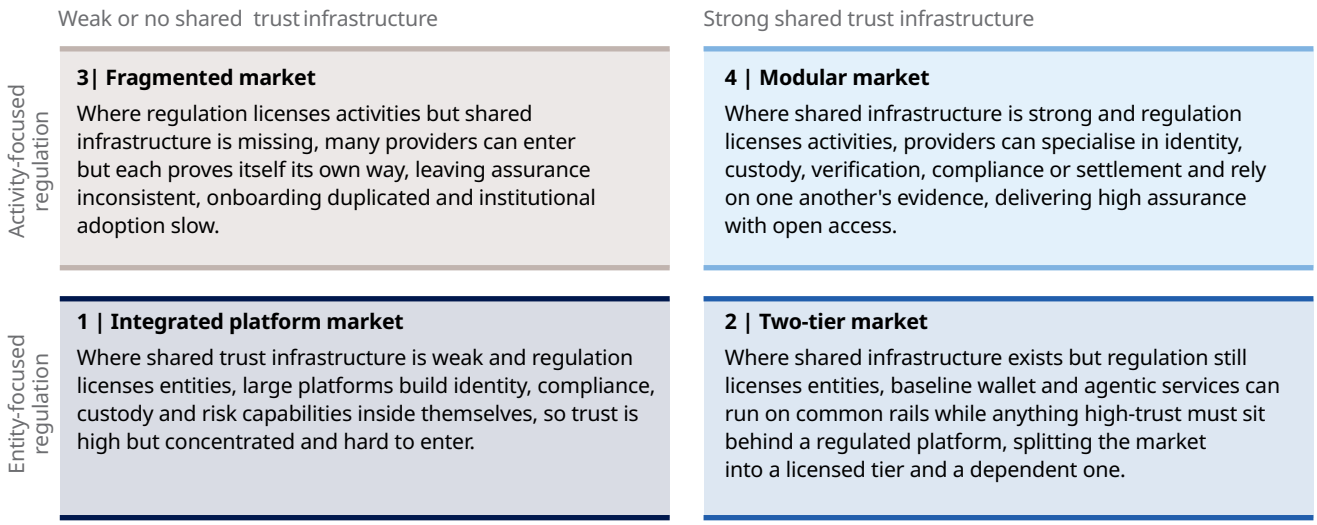
Where markets are heading: Industry and policy choices will shape market structure

Digital assets highlight the bottlenecks created by account-based custody. Identity can now be embedded in the control of an asset and travel with it. But if asset custodians play a smaller role, what will replace them as trusted gatekeepers protecting market integrity?

Markets differ on two dimensions: whether regulation licenses entities (the institution holds the obligations) or activities (whoever performs the function holds them), and whether shared trust infrastructure is weak or strong. Market participants and regulators shape these markets through three choices: how far regulators support shared trust infrastructure, whether they license institutions or activities, and whether banks, custodians and other relying parties are prepared to accept and reuse evidence issued outside their own institution. Together with market investment in infrastructure, these choices produce four scenarios: integrated platform, two-tier, fragmented, and modular as depicted in the framework below.

Elements of all four exist today, with the mix varying by jurisdiction, asset class, and system maturity. Each involves trade-offs. The working group argues that industry and policy makers should aim for a more modular market. Enabling new service providers to enter safely, supported by limited but efficient digital infrastructure, can increase choice and efficiency while supporting compliance and market integrity. Alternative scenarios are more likely to concentrate market power or create fragmentation, making important policy objectives harder to achieve.

© Oliver Wyman and GLEIF



The scenarios are not equally desirable. The modular market is our North Star because it offers the strongest potential for cheaper, faster, better-evidenced transactions that benefit end customers and the market as a whole, rather than whoever owns the infrastructure.

Four levers move markets between scenarios. Technology and economics enable the development of shared infrastructure, while liability and governance shape the regulatory framework. Where shared infrastructure develops first, markets can move toward broader reliance on portable evidence. Where activity-based licensing comes first, more providers can enter, but assurance remains fragmented.

Hong Kong illustrates one route toward modularity. Electronic transactions gained legal recognition in 2000, iAM Smart launched in 2020, data-sharing infrastructure followed from 2022, and stablecoin issuance became a licensed activity in 2025. Regulation arrived on infrastructure that already existed.

What the trust infrastructure must do, and must not do

The report sets out what the trust infrastructure must enable at each stage and where responsibility remains with participants. These boundaries prevent the trust layer from becoming a central authority. It carries and verifies evidence and links it to a transaction, but the participants in that transaction retain responsibility for deciding who can access a market, holding keys or assets, applying their own policies, settling transactions, and determining liability.

We identify 16 requirement families and a set of cross-cutting requirements that apply across the stages of compliant transactions. Seven appear twice: first to establish a fact from an authoritative source, then to verify that fact against a specific transaction. This distinction enables unbundling by separating responsibilities: credential issuers establish trust, while relying parties verify and rely on the evidence.

© Oliver Wyman and GLEIF

What each group of market actors can do to move toward the modular market

SIMFONIA identifies recommendations that three stakeholder groups can act on today, without waiting for one another:

- **Financial and transaction service providers** can integrate these capabilities into transaction flows by separating persistent identity from changing wallets and agents, using trusted external evidence, and issuing reusable evidence where they are the authoritative source.
- **Digital identity and authoritative-data providers** need to move beyond generic identification toward machine-verifiable evidence of identity, authority, delegation, status, and eligibility that financial counterparties can act on.
- **Regulators and policymakers** can preserve regulatory outcomes while allowing new ways to achieve them by recognizing governed portable evidence, clarifying when regulated firms may rely on it, and defining assurance and accountability requirements.

Some aspects of a more modular market require all three groups to act together, particularly on common semantics for authority and delegation, assurance mappings, issuer recognition and cross-border interoperability.

Three steps that can be taken now

The components of a modular trust infrastructure already exist in many advanced jurisdictions. What is missing is coordination. Three targeted steps could be taken now to move in the proposed direction:

1. **An industry request for supervisory clarity** on reliance upon verified evidence for a narrowly defined set of claims relating to one asset class in one jurisdiction.
2. **A cross-border pilot** between two financial centers with different trust frameworks to test whether assurance levels can be mapped and establish where liability sits.
3. **A demand commitment** from financial relying parties to turn the issuance of legally grounded evidence from a speculative cost into a funded one.

We welcome further dialogue with regulators, financial institutions, and trust providers interested in exploring this direction.

© Oliver Wyman and GLEIF

Digital financial innovation is *outgrowing* today's institutional trust model

Chapter 01



Transactions increasingly execute through temporary wallets, addresses and agents, while the trust functions behind them remain anchored where they were first established: in an institutional account.

Digital assets are moving from crypto-native markets into mainstream financial infrastructure.

Tokenized deposits, stablecoins, and tokenized real-world assets (RWAs), such as securities, funds, commodities, and real estate, are increasingly being issued, held, and settled through blockchain- and wallet-based infrastructure. Meanwhile, regulated financial institutions, central banks, and market infrastructures are developing capabilities to support them. The trend is toward tokenization as an extension of regulated finance rather than a separate financial system.

Agentic payments are at an earlier stage but are developing rapidly. AI agents are beginning to move beyond recommending and preparing transactions toward initiating them on behalf of people and organizations. AI developers and platform companies are driving this shift, while banks, card networks, and payment providers are responding. New mechanisms for agent identity, delegated authority, customer intent, authentication, and transaction limits are emerging.

© Oliver Wyman and GLEIF

Evidence of these developments is set out in detail in Appendix A.2 and provides a few examples highlighting the growth in adoption of wallet-based[2] digital asset and agentic[3] transactions.

These developments share an important characteristic: the endpoints through which financial activity takes place are becoming more dynamic. A legal person may use multiple wallets and addresses, while an individual or organization may authorize different software agents to act on its behalf. These wallets, addresses, and agents may be temporary, even though the underlying person, organization, and authority remain persistent.

This creates opportunities for faster settlement, 24/7 availability, programmability, automation, and transactions at lower economic values. It also presents a challenge for existing control models (see Exhibit 6 at the end of the chapter for more detail.

The policy objectives remain unchanged. Financial markets still require legal certainty, accountability, AML/CFT and sanctions controls, market integrity, investor and consumer protection, resilience, and auditability. The question is how to continue achieving these outcomes as transactions increasingly take place through infrastructure in which an account, wallet address, or software agent is no longer the persistent anchor of the relationship.

SIMFONIA therefore starts with a simple question: How can regulated finance capture the benefits of wallet-based and agentic transactions while preserving the trust, compliance and accountability on which institutional markets depend?

2 In SIMFONIA, "wallet-based finance" is used as a blanket term for financial exchanges where digital wallets are involved to facilitate transactions and manage assets (for example, any type of tokenized digital asset).

3 In SIMFONIA, "agentic transactions" and/or "agentic finance" is used to refer to transactions facilitated via AI agents.

Exhibit 1: Highlights of developments and growth in digital assets and agentic payments

Adoption of wallet-based and agentic transactions is growing

Global value of tokenized assets on public blockchains by February 2026, up from €7.4 billion at the start of 2024	€38 billion
Stablecoin market as of April 2026 having expanded to 3.73 times its 2021 size	$315 billion
Value of payments settled by agents in 2026, with four competing agentic payment architectures launched, backed by Coinbase, Stripe, Google, Visa, and American Express[1]	> $73 million
Volume processed via the x402 machine-payment protocol between its launch in May 2025 and April 21, 2026[2]	~109.6 million transactions

1. This metric serves as a signal of adoption, rather than as evidence of an economic transaction volume. 2. This is an adjusted metric from Visa excluding identified wash and test activity.

Source: 1. European Central Bank (ECB); 2. Bank of International Settlements (BIS); 3. Keyrock; 4. Visa and Artemis.

© Oliver Wyman and GLEIF

1.1 The paradigm shift: from account-bound trust to portable assurance

In traditional financial markets, many trust functions are organized around a persistent institutional relationship. A regulated institution establishes the customer's identity, opens and administers an account, verifies who may act, applies compliance controls, and retains the evidence. The account therefore becomes more than an addressing mechanism: over time, it acts as a persistent anchor linking the institution, identity, authority, and transactions.

Digital assets weaken this linkage. Wallets and addresses can be created, replaced, and used for specific purposes at very low cost. AI agents introduce another dynamic endpoint through which an underlying principal can act. Identity and authority are comparatively persistent; accounts, addresses, and agents increasingly are not.

Exhibit 2: SIMFONIA derives four principles from this change:

	Today's assumption	Emerging principle
01	Identity is tied to an account/address which is largely persistent over time.	Identity is persistent, accounts/addresses can be temporary.
02	Trust sits with the institution that onboarded the customer.	Trust can be portable, provided its source, assurance and validity are verifiable.
03	Compliance is established mainly at onboarding.	Assurance increasingly needs to be verified at transaction time.
04	The intermediary provides the trust.	Trust functions can be unbundled from the intermediary, but not from governance, accountability and liability.

Source: Oliver Wyman analysis

© Oliver Wyman and GLEIF

The implication is that banks, custodians, and other regulated intermediaries will remain important and, in many cases, will continue to be the most efficient providers of trust. What changes is that identity and authority should not have to remain permanently bound to the account or institution that first established them. Accounts and institutional relationships may change or be temporary, while the underlying holder's identity (that is, a natural or legal person) persists. Where appropriate, evidence of identity, authority, and other relevant attributes should therefore be capable of being presented and independently verified across wallets, institutions, transactions, and potentially jurisdictions.

If the model does not evolve: Digital assets can still develop without this change, but much of their activity is likely to be pulled back inside closed institutional perimeters. The likely consequences include re-intermediation and closed ecosystems, repeated onboarding and address whitelisting, reduced interoperability between custodial and self-hosted environments, and limits on programmability where every new counterparty, address, or machine interaction first requires bilateral institutional setup.

Fragmentation is another possible outcome: each institution, platform, or jurisdiction creates its own trusted perimeter and standards. Innovation that depends on direct interaction and composability would then have stronger incentives to develop outside those perimeters, including in less regulated environments.

Agentic payments amplify the need for a shift in the trust paradigm. A future in which machines transact dynamically across different accounts, wallets, jurisdictions, and payment instruments is difficult to reconcile with a model in which each technical endpoint must first be treated as a separate, persistent customer relationship.

The challenge is to make regulated trust sufficiently portable and machine-verifiable to operate across more dynamic transaction environments.

© Oliver Wyman and GLEIF

1.2 The control model changes, while compliance remains

The trust and compliance functions embedded in financial markets do not disappear when transaction infrastructure changes. Throughout the financial transaction lifecycle, participants still need to establish a sequence of facts and make decisions. Exhibit 3 shows generalized end-to-end compliance lifecycles for payments and value transfers, including traditional fiat, wallet-based digital asset, and agentic transactions. Where a transaction has two legs, such as the cash and securities legs of delivery versus payment or the two currency legs of a foreign exchange (FX) trade, the stages apply to each leg.

SIMFONIA refers to this as the **transaction trust handshake**. This is a generalized depiction; formal models may include additional steps depending on a financial organization's role, asset classes, and specific jurisdictions.

The following two cases illustrate this:

Digital assets: A regulated participant may need to establish the relationship between a verified natural or legal person and a particular wallet, assess the counterparty behind another address, determine authority and eligibility, perform anti-money laundering (AML), sanctions, and other controls, and retain the evidence required for monitoring and audit. Ongoing know your customer (KYC) and customer due diligence (CDD) scrutiny must also be conducted periodically or in response to external compliance events, such as changes to jurisdictional sanctions, rather than being triggered by individual transactions.

Agentic payments: An additional delegation relationship arises. The institution needs to distinguish the underlying principal from the software agent, establish what authority has been delegated, verify that it remains valid, and determine whether the proposed transaction falls within its scope. The distinction with legal significance is between subjects and objects, as defined in ISO/TR 6039: a subject is an entity with rights and obligations, while an object is an entity without them. Natural and legal persons are subjects; wallets, addresses, smart contracts, and software agents are objects. Rights, obligations, and liability attach only to the subject behind an object, however autonomous the object may appear.

This highlights the distinction between technical control and legal authority and accountability. Possession of a private key can prove the ability to sign a blockchain transaction. Authentication can establish control over a device or account. Neither, on its own, establishes the legal identity of the actor, the principal represented, the mandate under which it acts or whether the proposed transaction is permitted.

These are precisely the functions that need to become more portable and machine-verifiable if regulated financial activity is to operate efficiently across dynamic wallets, addresses and agents.

© Oliver Wyman and GLEIF

The trust handshake pattern has long existed in financial markets. In wallet-based and agentic transaction models, what changes is where the evidence comes from, who performs the individual functions, and how those functions are linked to the transaction.

Exhibit 3: Transaction trust handshake model as an end-to-end compliance lifecycle for payments

Financial organization lifecycle	**i. Licensing and regulatory classification** — setting up operations as a financial institution/custodian/issuer • Obtain license • Establish compliant custody safeguarding arrangements (reserves) • Continuously conduct audits and risk management
Customer lifecycle	**ii. Onboarding** — setting up an account/wallet for the principal (including registration of authorized humans/agents) • Identity (natural/legal persons) and jurisdiction check (part of AML/CFT, KYC, CDD) • Beneficial ownership checks — sanctions list and PEP checks (part of AML/CFT, KYC, CDD) • Establish authority, mandates to act and delegations (company-person-agent relations) • Establish transaction permissions (amount and frequency thresholds/policies) • Continuously conduct checks: ongoing KYC, CDD scrutiny that is event-driven and/or from a periodically required refresh
Transaction lifecycle	**iii. Transacting** — facilitating a compliant transaction from start to finish **1. Pre-transaction phase** • Counterparty check (counterparty due diligence screening) • Principal check (identity and jurisdiction) • Beneficial ownership checks (sanctions list and PEPs) • Control checks (authentication, consent, authority, delegated-mandate and policy-limit checks) • AML/CFT pattern checks (risk-based financial-crime and fraud decisioning) • Recorded authorization outcome (tamper-evident and timestamped record) **2. Settlement and reconciliation phase** • Execute settlement or route • Clear where applicable • Conduct reconciliation **3. Post-transaction phase** • Monitor • Report • Protective actions (Risk-based hold/block/freeze/quarantine) • Recall/cancellation (Stop or revoke before rail-specific finality; after finality: initiate return, recall or recovery (where legally and technically possible)) • Disputes

Source: Oliver Wyman analysis

1.3 Three broad responses emerge from the markets and regulators

Markets and regulators can respond to these developments in different ways (see Exhibit 4 for a visual summary).

The first response is to allow technology-led markets to develop with limited equivalent safeguards. This characterized parts of the early cryptocurrency market, which showed what direct wallet interaction makes possible, first on public permissionless ledgers and later on other ledgers. It also showed the risks of relying predominantly on technical rather than institutional trust.

The second response is re-intermediation: bringing activity within licensed exchanges, custodians, stablecoin issuers, CASPs/VASPs, banks and other regulated platforms. This restores familiar accountability and control mechanisms and will remain appropriate for many activities. However, if applied as the only model, it risks reproducing the existing institutional architecture on new technical rails and limiting the benefits of portability, direct interaction and programmability.

SIMFONIA examines a third response: to unbundle and reassemble selected trust functions. Identity, authority, regulatory status and other forms of assurance can be expressed as independently verifiable evidence and made available across institutional boundaries.

Custodial, hybrid and direct wallet models can then coexist, including on public permissionless ledgers, while regulated participants apply their own policies at the asset level and remain accountable for their decisions.

This model can develop when market participants are confident that appropriately governed digital evidence may be used within regulated compliance processes, provided the necessary legal, assurance, and accountability conditions are met.

© Oliver Wyman and GLEIF

In practice, regulators can define the required outcomes and assurance levels, clarify when recognized third-party evidence may be relied upon, and signal that portable, cryptographically verifiable credentials can be used in regulated finance.

Industry can then undertake the implementation work: developing credentials, issuer frameworks, trust lists, verification services, transaction protocols, and viable operating models.

The remainder of this report explores how such a model could work: how trust functions can become modular and portable; how cryptographically verifiable credentials make this possible; what market structures could emerge; and what requirements institutions must meet to rely on these mechanisms safely.

Global standards already cover every stage of this lifecycle (see Exhibit 5). FATF sets the AML/CFT baseline, FSB covers financial stability, IOSCO market integrity and DeFi, CPMI-IOSCO settlement infrastructure, and BCBS the prudential treatment for banks. None of these is directly binding law: they set the common baseline, and local legislation and supervisory decisions make them binding. The implication for SIMFONIA is that the obligations for compliant transactions already exist at every stage; what is still being built are the mechanisms to meet them at transaction time.

How these standards translate into concrete obligations differs by transaction model and by jurisdiction. Appendix A.2. maps the compliance actions per lifecycle stage for traditional fiat, wallet-based and agentic transactions, showing that agentic payments remain an overlay on the underlying regulated rail. Appendix A.3. sets out the local regulatory regimes of thirteen jurisdictions across Europe, Asia and the Americas. The pattern in both is the same: the requirements are in place or arriving, while the shared infrastructure to demonstrate compliance at transaction time is not or not yet.

Exhibit 4: Three responses to developments, with SIMFONIA focus on the third

First response
Allow technology-led markets to develop with limited equivalent safeguards

01

Second response
Re-intermediation to bring activity within licensed players and regulated platforms

02

SIMFONIA focus

Third response
Unbundle and reassemble selected trust functions as independently verifiable evidence across institutional boundaries

03

Source: Oliver Wyman analysis

Exhibit 5: Global standards cover every stage of the compliance lifecycle

These serve as the common baseline; obligations become binding through local legislation, rules and supervisory decisions

AML/CFT baseline

FATF recommendations

Risk assessment, CDD, sanctions and PEP controls, virtual assets, Travel Rule, records and suspicious-transaction reporting.

Lifecycle i ii 1 2 3

Financial stability

FSB crypto and GSC recommendations

Governance, risk management, data, disclosure, redemption, stabilisation and cross-border cooperation for crypto and global stablecoins.

Lifecycle i ii 1 2 3

Market integrity

IOSCO CDA recommendations

CASP conflicts, market abuse, custody and client assets, operational risk, disclosure, cross-border risk and retail distribution.

Lifecycle i ii 1 2 3

DeFi activities

IOSCO DeFi recommendations

Identify responsible persons and apply equivalent regulatory outcomes for conflicts, technology, data, market integrity and cross-border risk.

Lifecycle i ii 1 2 3

Settlement infrastructure

CPMI–IOSCO PFMI + stablecoin guidance

Governance, settlement finality, money settlement, custody and operational risk for FMIs and systemically important stablecoin arrangements.

Lifecycle i ii 1 2 3

Banks only

BCBS third-party + crypto prudential standards

Third-party, cloud and agent-provider risk across the service lifecycle; separate prudential capital treatment for bank crypto exposures.

Lifecycle i ii 1 2 3

● Applies in lifecycle stage ○ Does not apply in lifecycle stage

Scope rule

FATF, FSB, IOSCO, CPMI–IOSCO and BCBS materials are standards or guidance — not directly binding law. Apply the local regulation and the relevant institutional perimeter.

Source: Oliver Wyman analysis

© Oliver Wyman and GLEIF

1.4 The SIMFONIA core question

Digital assets and agentic payments are rapidly moving into mainstream institutional finance, reshaping how value is held, transferred, and initiated. As adoption grows, they also challenge existing control models, making identity, delegated authority, transaction traceability, and regulatory accountability increasingly important.

SIMFONIA raises the question:
How can wallet-based finance and agentic payments meet the same expectations that underpin traditional financial markets — legal certainty, accountability, AML/CFT, market integrity, investor protection, reporting, privacy, and resilience — without undermining the potential benefits of digital market infrastructure and tokenization?

Exhibit 6 summarizes key developments and considerations for the trust layer needed to facilitate compliant wallet-based digital asset and agentic payment transactions. It sets the context for SIMFONIA's exploration.

Exhibit 6: Key developments and considerations for wallet-based and agentic transactions

	Digital assets	Agentic payments
Developments summary	Digital assets are shifting from predominantly crypto-native markets toward tokenized deposits, tokenized real-world assets (RWAs), stablecoins, central bank settlement, and institutional cross-border payments integrated with regulated financial infrastructure.	Agentic payments are at an early stage but are beginning to gain financial volume. Major card networks, banks, payment service providers (PSPs), and technology platforms are developing the infrastructure to enable them.
Ways to transact	• Self-hosted Wallets (self-custody) • Hybrid model • Custodial wallets (via banks, crypto-asset service providers (CASPs), and virtual asset service providers (VASPs))	• Credit cards • Bank accounts and instant-payment rails • Self-hosted and/or custodial wallets
Trust handshake compliance requirements	For digital assets, a custodian is responsible for linking a verified real-world customer to wallets, counterparties, and transaction information. • Custody and key-management risk. • AML, sanctions, and Travel Rule compliance. • Legal certainty of ownership and settlement finality. • Liability, capital, liquidity and balance-sheet treatment. • Interoperability with traditional payment and market infrastructure.	For agentic payments, the institution also needs to distinguish the customer's identity from the AI agent's identity and delegated authority.

Source: Oliver Wyman analysis

© Oliver Wyman and GLEIF

Trust functions becoming *modular*, *portable* and *verifiable*



Chapter 02

The trust functions described in the previous chapter remain necessary and are likely to become even more important as digital assets and agentic AI become mainstream.

To preserve the integrity, resilience, and efficiency of the financial system, the way these functions are organized also needs to evolve. In wallet-based and agentic markets, identity, authority, compliance, and accountability increasingly need to operate across providers, platforms, and transaction environments, including at transaction time, rather than being re-established within each provider.

The control perimeter is moving away from the permanent account relationship. Identity, authority, and policy still need to persist, but the endpoints through which transactions are executed — increasingly wallets and agents — may be temporary. Identity therefore needs to be separated from the account, with supporting evidence made portable. Compliance remains essential, but the mechanisms used to achieve it must evolve.

Trust that was built into the institution should become evidence that can travel with the transaction and be independently verified.

© Oliver Wyman and GLEIF

2.1 Compliance checks across the lifecycle, by transaction model

The trust handshake model described in Chapter 1 originates from traditional finance, where checks take place at three key stages: licensing, customer onboarding and post-transaction.

In the **licensing stage**, an institution obtains authorization, establishes custody and safeguarding arrangements, and becomes subject to ongoing audit and supervision.

The second stage is **customer onboarding**, when it establishes identity, beneficial ownership, authority, and permissions, then keeps them current through periodic reviews[4] and event-driven updates.

The third stage is **post-transaction**, when monitoring, holds, recalls, and disputes address issues that earlier checks may have missed.

Exhibit 7 shows, at a high level, where checks take place in each model. The licensing column reflects how often an institution must demonstrate its regulatory standing and to whom, rather than how demanding it is to obtain a license. A bank demonstrates its standing to its supervisor and to counterparties with which it has bilateral relationships, but rarely at transaction time. A custodial wallet provider must demonstrate its standing to any party relying on it, including parties with which it has no prior relationship, for every transaction.

For onboarding, banks and crypto-asset service providers are subject to the same AML/CFT regulatory requirements, although local implementation may differ. In practice, bank onboarding involves additional requirements because banks also offer services such as credit and trade finance, which require additional or different proof points.

4 Some periodic checks can be required to be performed on a daily basis over the entire customer base, such as sanctions screening.

In the pre-transaction phase, banks perform relatively few additional checks because onboarding has already identified both parties, schemes such as SEPA admit only regulated members, and payments can be corrected afterwards. The remaining checks are automated: sanctions screening, fraud scoring, and Verification of Payee. Crypto custodians perform more checks because the counterparty may be an unknown or self-hosted address, there is no common scheme, the address needs to be screened for links to sanctions or fraud, Travel Rule data must be exchanged, and settlement is often, though not always, final.

In traditional finance, settlement is generally easier to correct afterwards, although instant and real-time gross settlement (RTGS payments are also final. For digital assets, whether settlement can be reversed depends on the asset, the ledger, and the legal regime. A custodian can freeze an account, and the issuer of a permissioned token can freeze an address or force a transfer back, on a permissioned or a public permissionless ledger alike. However, where no such operator exists, the transfer stands.

Post-transaction activity follows the same pattern. In traditional finance, it is most extensive: banks monitor transactions, report suspicious activity, handle disputes, and correct errors through recalls and chargebacks. Custodians also monitor and report transactions and can freeze or quarantine assets, but have fewer options for reversing transfers. With self-hosted wallets, monitoring is generally limited to the regulated counterparty's provider, while the ability to reverse a transfer depends on whether an issuer has the authority and technical means to intervene.

Exhibit 7: Concentration of compliance checks by transaction model and lifecycle stage

	Licensing	On-boarding	Pre-transaction	Settlement	Post-transaction
Traditional finance	●	●●●	●	Often correctable	●●●
Custodial wallet-based finance	●●●	●●	●●●	Often final	●
Self-hosted wallet-based finance	n/a	n/a	● / ●●●*	Final, unless an operator can act	●

*with/without regulated counterparty. Additional controls may be enforced by the asset's own smart contract.
n/a = not available, although obligations could rest with a regulated counterparty

Source: Oliver Wyman analysis

2.2 Unbundling and reassembling trust functions

For digital-asset finance, this means the distribution of compliance activity can shift. Depending on the asset, ledger design, and applicable legal framework, settlement may become final more quickly, and opportunities for operational intervention after execution may be more limited. This increases the importance of pre-transfer controls, although post-transaction monitoring, reporting, investigation, dispute resolution, and enforcement remain necessary. The control model must also reflect the specific characteristics of the asset and settlement mechanism.

Where a self-hosted wallet transacts with a regulated institution, the institution remains responsible for meeting its own regulatory obligations. It may need to establish the identity of the counterparty, the relationship between that counterparty and the wallet, and any other information required by the transaction's risk profile and applicable law. These checks do not necessarily require the institution to establish a complete customer relationship. Relevant evidence may be provided by the wallet holder, a regulated intermediary, or another recognized source, provided the institution can assess its provenance, level of assurance, and current validity.

Where two self-hosted wallets transact directly, no regulated intermediary is necessarily present in the transaction flow to perform customer due diligence or pre-transfer controls. This does not remove any legal obligations that may apply to the parties, issuers, or other service providers. Nor does it prevent monitoring, investigation, or subsequent enforcement. However, the absence of an intermediary or central operator may limit the ability to block, suspend, or reverse the transfer.

The scope for intervention depends on the asset's architecture, not solely on the ledger it runs on. A permissioned instrument may allow an issuer or administrator to apply transfer restrictions, freeze an address, or force a transfer back, including where it runs on a public permissionless ledger. A permissionless instrument may lack a central operator with equivalent technical powers, although regulated participants, analytics providers, and public authorities may still monitor activity and take action against identifiable persons or assets through legal and operational channels.

A modular trust infrastructure can support these different models by making relevant evidence available when and where it is needed. Information about a participant's identity, regulatory status, authority, and permissions can be established by recognized sources and presented for verification in the context of a specific transaction. Freshness, status, and revocation checks can then be performed at or immediately before authorization.

© Oliver Wyman and GLEIF

The trust infrastructure does not itself determine whether a transaction should proceed. Its role is to carry and verify evidence, link that evidence to the transaction context, and record the resulting authorization outcome. Accountable participants, or systems expressly acting under their authority, remain responsible for applying policy, making decisions, and enforcing outcomes. Settlement continues to be performed by the relevant payment, ledger, or market infrastructure.

Agentic payments add a further layer. The acting software must be linked to an identifiable principal and a verifiable chain of delegated authority. The transaction must fall within the mandate's scope, limits, and conditions, and the mandate must remain valid at the time of use. Some controls, such as transaction amount or counterparty limits, can be applied deterministically. Assessing whether an agent's actions are consistent with the broader purpose for which authority was granted may require additional risk-based or probabilistic controls.

SIMFONIA's working thesis is therefore: The functions of the trust layer do not need to be reinvented. They need to be made portable where appropriate and reassembled within a governed, interoperable, and accountable ecosystem.

This evolution may change the roles of market infrastructures, regulated institutions, and specialist service providers. Financial institutions already establish trust through identity documents, KYC records, corporate mandates, board resolutions, and contractual arrangements. Regulated stablecoin issuers are a natural addition: a licensed issuer that has verified its holders is an authoritative source for holder and wallet status, and its license itself is verifiable evidence. The challenge is to express and govern equivalent evidence in a form that can be verified and relied upon across digital transaction environments.

Governed digital credentials and recognized reliance frameworks are important enablers. Their effectiveness will also depend on common semantics, authoritative identifiers, assurance standards, liability allocation, privacy protections, and clear accountability. Together, these elements can reduce unnecessary duplication and the need for bilateral integration while preserving the responsibilities of regulated participants.

© Oliver Wyman and GLEIF

2.3 Cryptographically verifiable credentials as a highly versatile foundation of modular trust

Cryptographically verifiable credentials[5] provide the technical mechanism for making trusted information portable and independently verifiable. Legal certainty comes from the framework under which the issuer operates, not from the cryptography.

A recognized issuer can express a trusted fact as digitally signed evidence that a holder can present and a relying party can verify independently. The fact can concern a subject (a legal identity, a regulatory license, authority to act, or a transaction mandate) or an object (an instrument and its register entry, a smart contract and its administrator, a wallet and its provider, or an AI agent and its principal). The origin and integrity of that evidence can be proven cryptographically, while its current validity can be checked at the time of use and audited historically. This relationship is commonly described through the **issuer–holder–verifier trust triangle** (see Exhibit 8).

Several concepts underpin this model and are essential to establishing trust:

- **Issuer recognition**: Establishing that a credential issuer is recognized by an authoritative trust source as one that can be relied upon for a particular credential.
- **Credential authenticity and integrity**: Cryptographic evidence that the credential comes from the stated issuer and has not been altered.
- **Holder binding**: Establishing, to a defined level of assurance, that the presenter is the person or entity to whom the credential was issued.
- **Level of assurance**: The degree of confidence in how strongly an identity or claim has been established.
- **Selective presentation**: Revealing only the specific credential attributes needed for a transaction without disclosing all the underlying data.
- **Revocation**: Withdrawing a credential's validity before its stated expiry because it is compromised, incorrect, outdated, or no longer applicable.
- **Auditability**: Preserving sufficient tamper-evident records to reconstruct which credential or proof was presented, verified, and relied upon, including its issuer, assurance, and validity status at the time of the decision, without retaining unnecessary underlying data.

These concepts are explained in more detail in Appendix B.1.

5 By "cryptographically verifiable credentials" the authors mean the general concept of digitally signed, independently verifiable evidence, not the specific W3C Verifiable Credentials standard. Other formats follow the same issuer–holder–verifier model, including SD-JWT VC, ISO/IEC 18013-5 mdoc, ACDC (used for the vLEI), and X.509 certificates.

© Oliver Wyman and GLEIF

Cryptographically verifiable credentials are increasingly being used in real-world applications, supported by developments in public digital identity, technical standards, and market adoption:

- Governments are putting digital identity infrastructure in place, increasingly supporting reusable digital credentials for individuals, organizations, attributes, and authority.
- The technology is proven, and standards are converging, with common approaches emerging for credential formats, issuance, presentation, and verification.
- Adoption is extending into financial services, with banks, exchanges, wallet providers, and technology platforms beginning to issue, store, and verify reusable credentials.

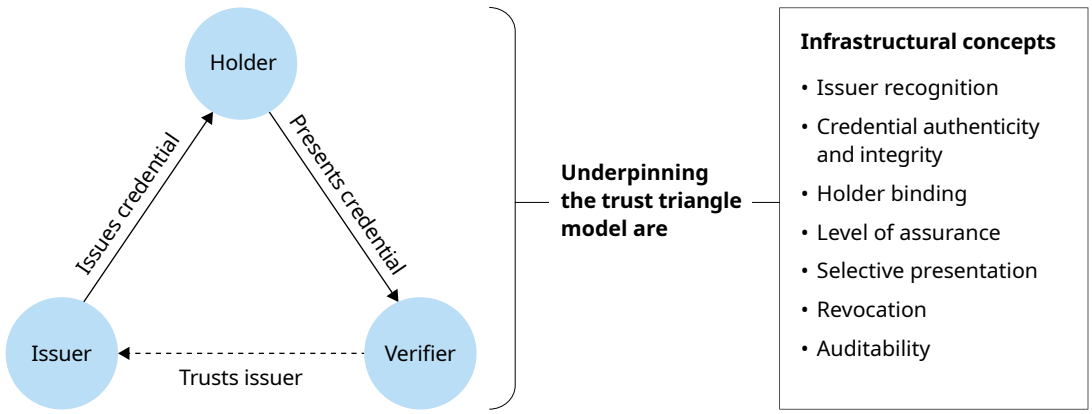
Further evidence of this increasing maturity can be found in Appendix B.2.

Cryptographically verifiable credentials change how trust can be established and reused in digital transactions. They enable five important shifts:

1. **Portable evidence instead of institution-bound records.** Credentials can be presented across institutions, platforms, and transaction contexts rather than remaining with the organization that first established the information.
2. **Independent verification instead of bilateral validation.** Once a credential is presented, the recipient can independently verify its issuer, origin, integrity, and status.
3. **Reusable evidence instead of repeated re-establishment.** The same credential can be used multiple times without the underlying fact having to be established again for each transaction or counterparty.
4. **Transaction-time assurance instead of onboarding and periodic assurance.** Relevant identity, authority, and authorization attributes, along with their validity status, can be checked at transaction time, immediately before value moves.
5. **Selective proof instead of full-data sharing.** Only the information required for a transaction needs to be disclosed.

Together, these shifts make assurance more portable, reusable, provable, current, and transaction-specific, which is particularly important for wallet-based and agentic payments.

Exhibit 8: The trust triangle (simplified)



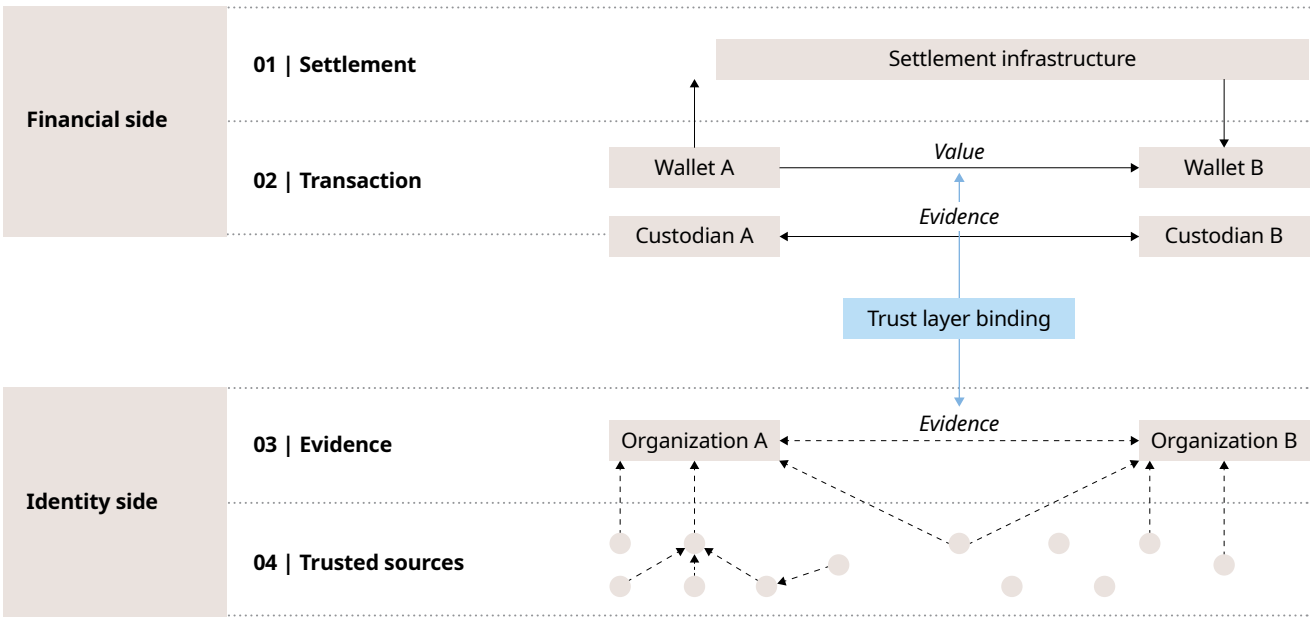
Source: Oliver Wyman analysis, based on concepts popularised in the Self-Sovereign Identity community (e.g. Drummond Reed)

2.4
From verified evidence to transaction authorization

The next step is to bind the verified evidence to the specific transaction being initiated. A valid credential or mandate may be subject to limits on amount, asset type, counterparty, jurisdiction, or approval threshold. The verifier therefore checks whether the evidence relating to both parties covers the transaction intent and whether all applicable policy conditions are satisfied. If these conditions are met, an authorization outcome is created and linked to the transaction before value moves.

The transaction can then be executed and, in a wallet-based payment, settle almost immediately. A transaction trust record retains the evidence needed to reconstruct the decision afterwards: the credentials or proofs relating to both parties, cryptographic signatures, their status at the time, relevant policy outcomes, the authorization decision, and its link to the resulting transaction. These digital records provide evidence of what was established, verified, and relied upon when the transaction was authorized (see Exhibit 9).

Exhibit 9: Trust layer role in binding evidence for transactions



Source: Oliver Wyman analysis

The flow shown in Exhibit 9 is as follows:

A transaction starts with an intent between two organizations, Organization A and Organization B (layer 3). They may already share some evidence: a contract, an invoice, or a handshake. This rarely suffices for a financial transaction because each custodian must be able to demonstrate to its supervisor who it is dealing with, that the signatory is authorized to act, and that the transfer is permitted.

Organizations A and B therefore each collect evidence from trusted sources (layer 4), such as a company register, a notary, or a licensing authority, about their legal identity, license status, and the authority of the person acting. Some sources serve both organizations, for example when both use a vLEI to prove their signatory's mandate.

Each organization passes this evidence to its custodian (layer 2). Custodian A checks its own customer and requests the proofs it needs from Custodian B, such as sanctions and AML screening results. The trust layer binds the evidence to the intended transaction and checks it against the applicable policy conditions. When all checks pass, an authorization outcome is linked to the transaction, which then proceeds.

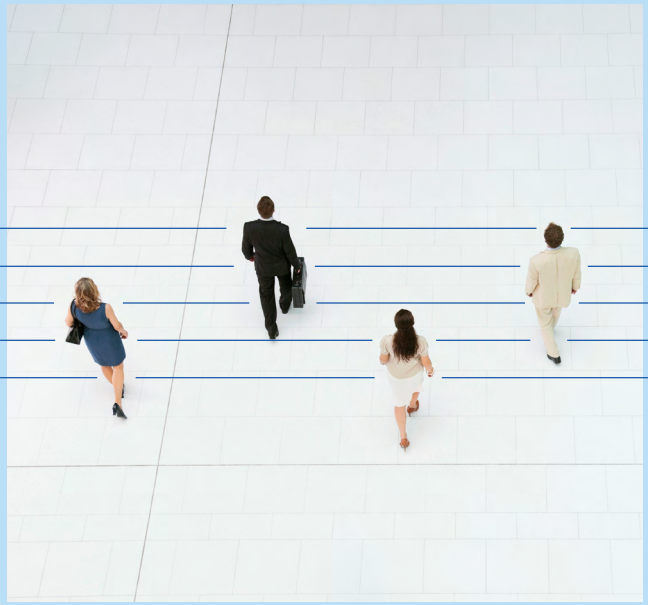
Settlement follows (layer 1). The settlement infrastructure debits Wallet A and credits Wallet B. Corrections after settlement are limited and depend on the asset and the ledger (see Section 2.1), which is why the checks need to take place beforehand.[6]

The file cabinets of financial institutions will not disappear. Where they once contained copies of passports, company extracts, mandates, and signed forms, they will now contain verifiable credential presentations, cryptographic proofs and signatures, status checks, authorisation decisions, and timestamps.

6 The settlement infrastructure can be any type of ledger, public permissionless ledgers included. Where the token contract checks eligibility itself, as in some permissioned tokens, this is an additional check before the transfer takes effect: a non-eligible transfer fails and no debit or credit takes place.

Pathways toward *modular trust* for financial markets

Chapter 03



Two forces that shape how institutional markets for digital assets and agentic payments develop: regulatory dynamics and the availability of shared trust infrastructure.

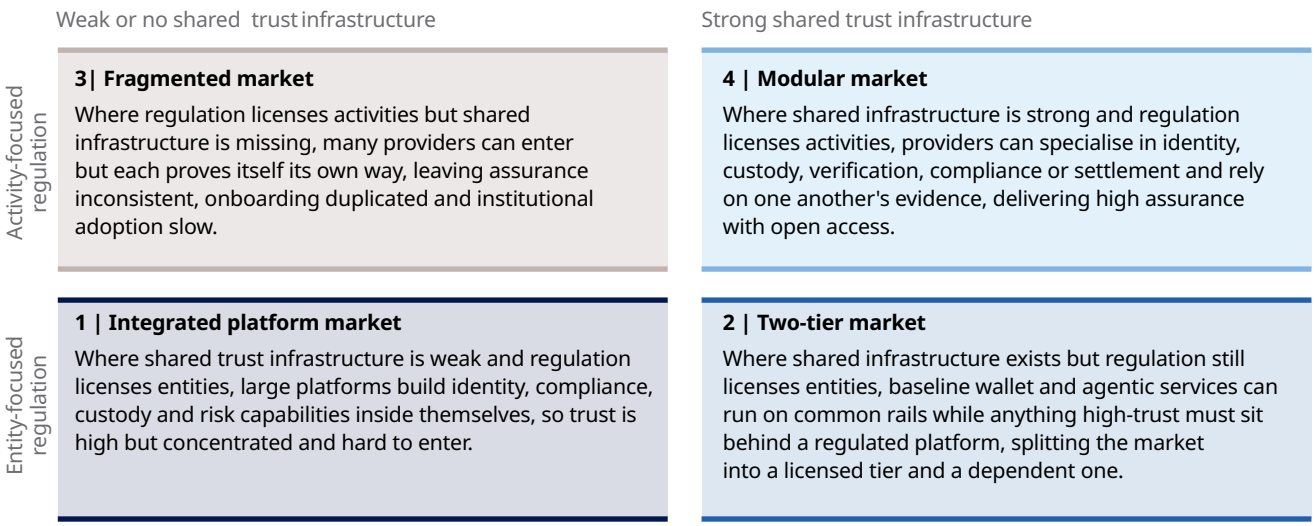
The SIMFONIA expert group, workshops, and review process identified two forces that shape how institutional markets for digital assets and agentic payments develop: regulatory dynamics and the availability of shared trust infrastructure. Their interaction determines whether trust functions remain concentrated within institutions, become fragmented across providers, or evolve toward more interoperable and modular arrangements. The scenarios below capture the main market structures identified through that work (see Exhibit 10).

Force 1: Strength of shared trust infrastructure. The trust functions described in the previous chapters — establishing identity, authority, compliance, and accountability — no longer have to be performed within each institution. As these functions are unbundled, they can be provided as services by technology firms, identity providers, auditors, and specialist compliance firms alongside regulated financial institutions. Where those services are widely available, mutually recognized and relied upon, and their evidence can be verified independently, the market has strong shared trust infrastructure.

Force 2: Regulatory focus: entity- or activity-based. Regulation is also moving from authorizing institutions toward authorizing activities: licensing and requirements attach to the specific functions needed to complete a compliant transaction, whether traditional, wallet-based, or agentic. Accountability and liability then rest with whoever performs the function rather than whichever licensed entity happens to hold the customer relationship. This makes specialization possible: a relying party can use a third party's identity check, credential, or compliance service and remain accountable for the transaction because the terms of that reliance are defined in regulation and rulebooks rather than negotiated bilaterally. Where regulation is activity-focused, trust functions can be sourced from whoever performs them best. Where it remains entity-focused, they can still be sourced externally, but under a licensed institution's retained responsibility.

Together, these two forces form four development scenarios for the trust services market.

Exhibit 10: Four development scenarios of market dynamics for wallet-based and agentic transactions



Source: Oliver Wyman analysis

3.1 Four development scenarios coexist in practice

In practice, four scenarios coexist, with the mix varying by jurisdiction and asset class. Exhibit 11 provides a non-exhaustive overview of market initiatives, projects, and regulatory frameworks plotted in their respective quadrants. SIMFONIA uses this model to consider the consequences of different market approaches for providers of digital asset wallets, agentic payments, and digital identity services, as well as regulators.

In Exhibit 11, the examples are plotted according to the market structures they produce, rather than their maturity[7]. The list brings together regulations, schemes, initiatives, prototypes, and commercial platforms because each example represents and shapes a market structure in its own way. Appendix C provides details of all the examples listed and their effects on the respective quadrants in which they are positioned.

The placement of these examples leads to two key conclusions:

(a) **The modular market is a direction with working analogs**. The live examples in quadrant 4 come from adjacent domains, such as open banking, cross-sectoral data sharing (data spaces), and legal entity identity. Meanwhile, the digital asset and agentic examples are mostly early deployments, prototypes or standards still under development.

(b) **The same governance questions will produce different answers depending on the market structure**. PFMI Principle 2 requires governance that protects the public interest and raises the following questions for market infrastructures: Who sets the rules? Who recognizes trust providers? Who carries the loss when evidence fails? Who can change the rules? And how are end users represented?

The answers differ by scenario, mainly according to where control sits:

- Platform operators in the integrated scenario.
- Licensed institutions in the two-tier scenario.
- Bilateral agreements in the fragmented scenario.
- Schemes under recognized trust frameworks in the modular scenario.

7 The same firm can appear in several quadrants because a quadrant describes the project or product arrangement, not the company itself. For example, Anchorage appears twice (in quadrants 1 and 4). This is because Anchorage Digital operates as an integrated institutional custody platform, while its Atlas project, which unbundles custody, matching, credit, and settlement across separate regulated actors, best fits in quadrant 4.

© Oliver Wyman and GLEIF

Exhibit 11: Proof points for four scenarios at a glance

	Weak or no shared trust infrastructure	Strong shared trust infrastructure
Activity-focused regulation	**3| Fragmented market** **Typical use case:** Two VASPs exchange Travel Rule data, each using a different protocol and negotiating bilaterally before a transfer can proceed. Agentic payments show the same pattern: each framework defines its own agent identity and mandate format. **Real-life examples:** • Travel Rule networks: Sygna Bridge, VerifyVASP, TRISA, OpenVASP/TRP, Global Travel Rule • Agentic protocols: AP2, ACP, Visa TAP, x401, x402 • Access and payment: Cloudflare Monetization Gateway • Abandoned: AOPP	**4 | Modular market** **Typical use case:** A company is onboarded using a legal-entity credential from an official register and a mandate credential from a separate authoritative source, neither of which has a contract with the relying party. Verification runs against a published trust list. **Real-life examples:** • Public identity frameworks: EUDI Wallet and eIDAS trust services, UK Digital Verification Services Trust Framework, Singpass and Corppass • Entity identity: GLEIF vLEI • Credential standards: ISO 18013-5 mobile driving license • Cross-sector analogs: UK Open Banking, iSHARE Trust Framework, India Account Aggregator • Prototypes: BIS Tamga, BIS Mandala • Standards in development: FIDO agentic authentication and delegation • Boundary cases*: Anchorage Atlas; Coinbase Bitcoin Yield Fund tokenized share class (ERC-3643 on Base)
Entity-focused regulation	**1 | Integrated platform market** **Typical use case:** An institutional customer trades and settles digital assets within a single platform that has onboarded both sides, holds the keys, and runs its own compliance stack. Nothing has to be proven to anyone outside the platform. **Real-life examples:** • Bank platforms: J.P. Morgan Kinexys, Citi Token Services • Institutional crypto platforms: Coinbase Prime, Anchorage Digital, Fidelity Digital Assets • Stablecoin issuers: Circle Mint	**2 | Two-tier market** **Typical use case:** A consumer wallet payment runs on shared rails, while the regulated acquirer or bank behind it carries the compliance obligation. Baseline services scale, while anything requiring high assurance remains within the licensed tier. **Real-life examples:** • Wholesale settlement: J.P. Morgan JPMD deposit token (live on Base and Ethereum), Swift tokenized-deposit ledger, BIS Project Agora, Pontes, Fnality, Partior, HKMA Ensemble TX, Canton Network, Regulated Liability Network • Retail shared rails: UPI • Card and agent rails: Visa Intelligent Commerce, Mastercard Agent Pay, Adyen Agentic • Compliance utilities: Notabene SafeGateway

*Boundary cases: examples that meet the quadrant's verification model but not its shared control of trust.

Source: Oliver Wyman analysis

3.2 Market developments point to increasing modularity

The scenarios coexist, but markets can transition toward a modular state. Not all scenarios are equally desirable for end customers or most other participants in digital wallet services and agentic payments. The market structure that emerges and persists varies by jurisdiction and asset class. However, these choices compound: as technology, standards, and reliance practices are reused across markets, early adoption in one place makes the same structure more likely to be adopted elsewhere.

In light of this, the modular market is our North Star for wallet-based and agentic markets, offering the most scalable way to extend trusted financial infrastructure to them without requiring every participant to rebuild the full trust stack. Other models will coexist for good reasons, but the modular market offers the strongest potential for cheaper, faster and better-evidenced financial services without depending on a single gatekeeper for access, price, continuity and innovation.

In the modular market scenario, specialized and certified service providers help financial players reduce duplicated onboarding and control stacks, lower integration and operating costs, reduce user friction, and improve market access.

The move toward modularity is consistent with four major developments:

- FATF rules and recommendations that allow regulated institutions to rely on qualified third parties for customer identification while retaining ultimate regulatory responsibility.
- FSB's functional principle of "same activity, same risk, same regulation," which shifts the regulatory focus from the type of institution or technology being used to the economic function performed and the associated risk.
- BIS work identifying interoperability, verifiability, and modularity as building blocks for a more accessible, reliable, and lower-cost financial system (see Projects Agora, Mandala and Tamga).
- The emergence of local regulatory frameworks for digital finance and digital identity markets that support each other and lead toward modularity. Two examples are:
- The European EUDI regulation, which is driving mandatory acceptance of qualified trust services by financial institutions.
- Hong Kong Stablecoin Ordinance and Electronic Transactions Ordinance, which set a precedent for legally recognized trusted identity for holders and public trust lists for issuers (see Chapter 4 for more on Hong Kong).

Taken together, these developments suggest that modularity is not an immediate or inevitable outcome, but a credible end state if common standards, interoperable credentials, reliance frameworks, and clear accountability mature across jurisdictions, and digital wallet services and agents gain further traction.

© Oliver Wyman and GLEIF

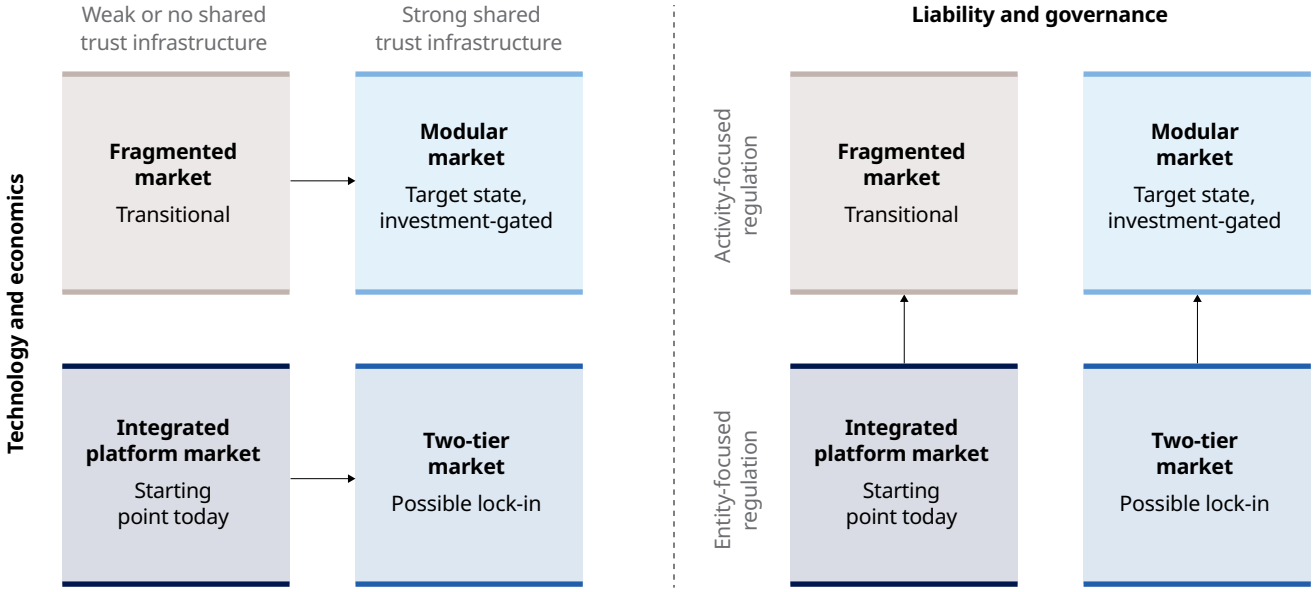
3.3 Four levers move markets toward modularity

Movement between the quadrants is driven by four interrelated levers: technology, economics, liability, and governance. Technology and economics build shared infrastructure and move a market to the right; liability and governance change the regulatory basis and move it upward. Exhibit 12 illustrates these movements, followed by further details on how the four levers operate in practice.

1. **The technology state determines whether interoperability is attainable for global deployment.** Credential formats, issuance, and verification are converging around common standards, and the technology can support transaction-time verification. The remaining challenge is scale: issuers, wallets, and verifiers need to be deployed within the same market and connected through interoperable infrastructure.
2. **Economics determine whether the model works at transaction scale.** Reusable credentials only displace repeated onboarding if verification costs a small fraction of the transaction it supports. Verification involves checking a cryptographic signature against a recognized issuer, so its marginal cost falls toward the cost of computing once the infrastructure is in place and reaches scale. Getting there presents a catch-22: no issuer invests without verifiers, and no verifier invests without credentials in circulation. Public schemes can break this barrier: governments bear the cost of initial citizen identity issuance and mandate its acceptance for government services, creating an installed base that private credentials can then build on.
3. **Liability determines whether participants can truly rely on evidence established elsewhere.** Today, a party that relies on another's evidence carries the full consequences if that evidence is wrong. This makes bilateral contracts the only safe route and limits the market to the number of pairs willing to negotiate. Liability must be distributed so that each party is responsible for its own part: the issuer for the fact asserted, the verifier for the check performed, and the relying party for the decision taken. This is typically settled through a scheme rulebook rather than by waiting for case law. Qualified trust services under the EU Digital Identity Regulation (eIDAS) already show that statutory reliance and allocated liability can work at scale because liability follows the assurance level, and qualified certification status carries the legal effect. Without this, activity-based licensing creates providers that nobody can safely rely on.
4. **Governance provides the framework for recognized reliance.** A relying party will only accept someone else's evidence if it knows who is entitled to issue it, at what assurance level, and how revocation is handled. This requires organized recognition: admission criteria, published trust lists, and lists of trusted lists so that recognition itself can extend across schemes. The aim is to make cryptographic evidence something a party can rely on as a matter of law rather than judgment. This requires a legal basis for each step: the issuer's attestation, the verifier's check, and the relying party's decision each need a statute, rulebook, or contract that holds in every jurisdiction the transaction touches. Recognition is best established one jurisdiction at a time, starting where an authoritative source already exists, and extended across borders once it is established. Pursuing cross-border recognition first leaves nothing solid to be recognized.

© Oliver Wyman and GLEIF

Exhibit 12: Four levers of change: Technology, economics, liability, and governance move markets



Source: Oliver Wyman analysis

The sequence of changes affects the transition path: one is viable, another fragile. As described above, the four change levers create opportunities for markets to move between scenarios. However, these levers do not act in isolation. Depending on the sequence in which they are activated, the transitions between scenarios can unfold in different ways. Exhibit 13 illustrates these transitions and highlights two main paths.

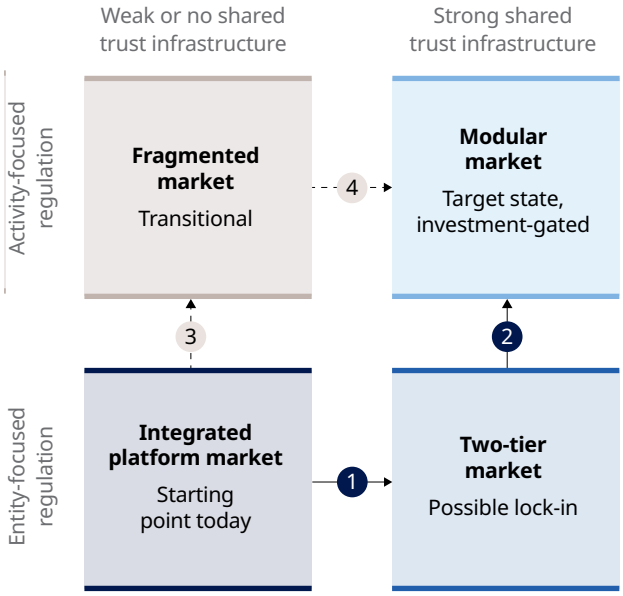
The fragile path is the "regulation-alone path," where market access and activity-based regulation develop faster than the underlying trust infrastructure. As a result, more providers enter the market, but assurance remains fragmented, and bilateral arrangements continue to be necessary.

The more viable path is the "assurance-backed path," where shared infrastructure develops ahead of, or alongside, legal and governance arrangements, allowing markets to move progressively toward broader reliance on portable evidence.

Notably, irrespective of the path, markets can reach a standstill without adequate development of the four change levers. In particular, the two-tier scenario can become a point of lock-in when the levers do not provide sufficient impetus for major incumbents in the financial market to change and regulation does not develop in an activity-based direction. The market then reaches a state that satisfies enough players that the pressure to move disappears. This can result in lackluster innovation and stagnation in the adoption of wallet-based and agentic payments.

© Oliver Wyman and GLEIF

Exhibit 13: Two paths toward modularity



Two transition paths enabled by regulatory and market forces:

Assurance-backed path (viable)

1. Governed assurance is created by the market players, alongside regulation*
2. Overtime supervision shifts from entities to activities**

Regulation-alone path (fragile)

3. Regulation shifts before efficient assurance means exist
4. Assurance means and trust infrastructure catches up

*Trust infrastructure developments: e.g., service providers from identity side join the market, stronger and cheaper assurance means are developed.

**Regulatory shifts: Growth of activity-based regulations (e.g., in EU PSD3/PSR; eIDAS; in Hong Kong — stablecoins regulatory framework).

Source: Oliver Wyman analysis

© Oliver Wyman and GLEIF

Hong Kong stablecoins regulatory framework paves the way to a *modular trust layer*

Chapter 04



Hong Kong built legal recognition, public digital identity and governed data exchange first, and then licensed stablecoin issuance on top of them, showing how regulation and trust infrastructure can reinforce each other.

The Hong Kong stablecoins regulatory framework is an example of activity-based regulation that ensures trust and moves the market toward a more modular state.

Hong Kong's Stablecoins Ordinance, a regulatory framework in force since August 1, 2025, makes the issuance of fiat-referenced stablecoins a regulated activity, requiring issuers to obtain licenses from the Hong Kong Monetary Authority (HKMA). Licensed issuers are expected to:

1. Meet requirements on capital, full reserve backing and redemption, risk management, disclosure, and AML/CFT compliance.
2. Conduct mandatory risk-based know-your-customer (KYC) checks and customer due diligence (CDD), identify beneficial owners, and carry out ongoing transaction monitoring and wallet ownership and control checks.
3. Conduct enhanced screening for self-hosted wallets. Unless effective alternative controls are demonstrated, the HKMA expects individual holders to be identified by the issuer or an appropriately supervised intermediary.[8]

The framework aims to protect holders and enable responsible innovation by preserving monetary and financial stability and deterring illicit finance through a common assurance layer on which different market participants can rely. It creates assurance that can be reused by wallets, custodians, distributors, and payment providers, providing a foundation for a more modular digital-asset and payments market.

Hong Kong is not a stand-alone example. The EU is assembling the same building blocks by another route: eIDAS 2 provides reusable identity and qualified trust services, MiCAR licenses issuance, the Transfer of Funds Regulation extends the Travel Rule, and the EU's new AML framework moves toward harmonised rules and central supervision. The sequence differs, but the pattern is the same: regulation arriving on trust infrastructure.

8 The HKMA prohibits customer relationships and transactions under fictitious names but does not prohibit self-hosted wallets, instead subjecting them to enhanced screening.

The four levers that were discussed in chapter 3 are activated in Hong Kong's stablecoins framework to enable this:

Change lever	Hong Kong enablement of a modular market
Technology	Sets common rules for transaction screening and extends assurance into issuance without prescribing a single technology platform. This creates a common technical assurance baseline while allowing issuers and specialist technology providers to use different systems.
Economy	Full backing, disclosures, and independent assurance reduce the need for market participants to reassess stablecoins. Standardized KYC/CDD and controlled reliance on supervised intermediaries (iAM Smart service) reduce duplicated onboarding and verification while preserving risk controls.
Liability	The issuer remains accountable for reserve integrity, redemption, and AML/CFT compliance, including when activities are outsourced or CDD is performed by the iAM Smart service offered by the Digital Policy Office. This places responsibility with the party controlling each function and gives holders clearer legal rights against the issuer and reserve pool.
Governance	Establishes an HKMA public register of licensed issuers, AML/CFT controls, ongoing supervision, reporting, and audits. The register and common rules act as an authoritative trust layer that can be recognized across the market. The prohibition of fictitious-name customer relationships and identity controls for wallets strengthen recognized reliance across the ecosystem.

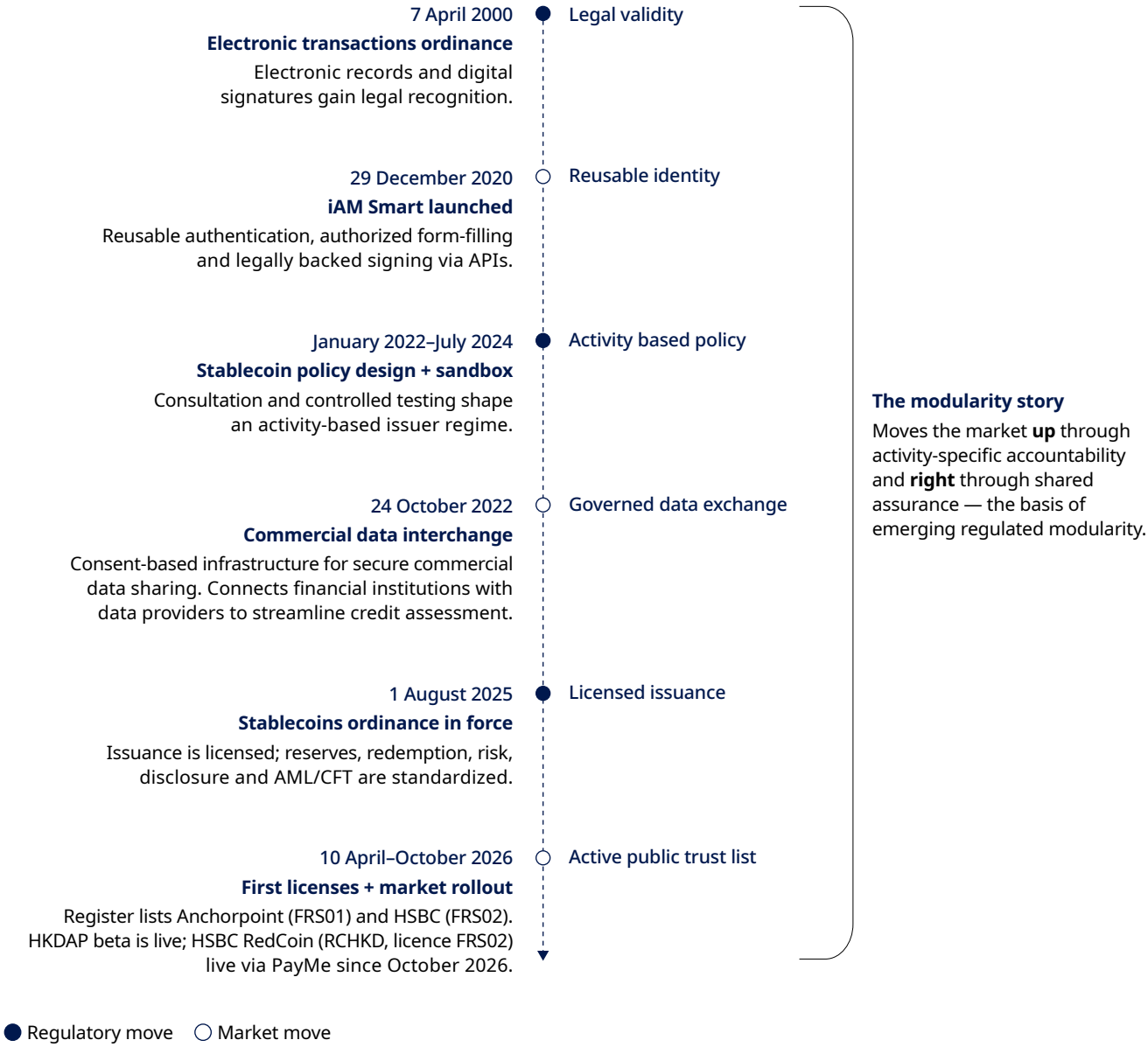
Overall, the stablecoins framework moves Hong Kong toward regulated modularity. Different providers can specialize in issuance, custody, distribution, and verification while relying on a shared regulatory assurance layer. The framework does not yet create a single technical interoperability rail, but it establishes the legal and supervisory foundation on which one can develop.

Exhibit 14 summarizes the timeline of regulatory developments and market implementations in Hong Kong that have together encouraged movement toward modularity. In this case, the right transition path is unlocked in both directions: upward, toward activity-specific accountability, and to the right, toward shared infrastructure on which multiple participants can rely.

This should nevertheless be understood as an emerging form of regulated modularity rather than a completed end state. Participants cannot yet rely on portable, independently verifiable evidence across all institutions; cross-border liability rules and recognition also remain to be developed. (Further details from HKChain technical reports and research by Prof. James Zhibin Lei (Hong Kong University of Science and Technology) are covered in Appendix D.)

© Oliver Wyman and GLEIF

Exhibit 14: Hong Kong timeline path to regulated modularity



Source: Oliver Wyman analysis

© Oliver Wyman and GLEIF

Requirements: What the trust layer *must and must not do*

Chapter 05



Sixteen requirement families define what the trust layer must enable, and the boundaries that keep it a neutral carrier of evidence.

The requirements presented below derive from the transaction and regulatory analysis in the previous chapters and from discussions within the SIMFONIA working group. They represent an initial articulation intended for market testing and are expected to be added to, consolidated, and re-scoped as they are tested in practice.

They apply wherever trust functions are performed across multiple parties rather than within a single institution, whether because those functions have been unbundled from a bank or other regulated institution or because the market developed without one. This covers wallet-based payments, agentic transactions, tokenized deposits and securities, stablecoin settlement, and the traditional systems with which these interact.

They describe what an ecosystem must deliver collectively. No single provider is expected to satisfy the full set. The test is whether each requirement is met by an identifiable party on terms on which others can rely.

The requirements follow the trust handshake set out in Chapter 1. Each stage is stated in two parts: what the trust layer must enable and the boundary beyond which responsibility remains with participants. The boundaries are as important as the capabilities because they keep the trust layer a means of carrying and verifying evidence rather than a central authority over market access, custody, or transaction outcomes (see Exhibit 15).

Exhibit 15: what the trust layer must enable at each stage and what it must not do
Within these stages, the requirements are organized into 16 families. Each family contains a set of related functional and non-functional requirements covering a particular topic (see Exhibit 16).

Stage	Must enable	Must not
Licensing	Verify that a party is licensed or recognized in a jurisdiction, in which role, under which scheme, and whether that status remains valid. Establish the custody model, asset terms, and rules on which others may rely.	Determine who may access a market, admit or exclude participants, or substitute for a supervisor.
Onboarding	Establish identity, jurisdiction, beneficial ownership, authority and mandates, wallet control, and permissions from authoritative sources,[9] and keep them current through periodic and event-driven review.	Act as the identity register, grant or administer mandates, hold keys, or replace the relying party's own onboarding and compliance review.
Pre-transaction	Present and verify that evidence against the transaction: revocation and freshness checks, counterparty screening, proof of control, purpose and limit checks, and an authorization outcome bound to the transfer.	Decide whether the transaction is acceptable, apply a participant's policy, or enforce an outcome.
Settlement	Reference the settlement outcome from the authorization record.	Settle, clear, or hold value.
Post-transaction	Reconstruct what was relied upon and that it held at authorization. Support monitoring, reporting, market-integrity links, protective action where a party can still act, and routes to recourse.	Serve as the central record store, determine whether conduct is abusive, or determine liability.

Source: Oliver Wyman analysis

9 An authoritative source is a party whose statement the relying party accepts without repeating the check. Self-issued statements can also qualify as authoritative, but only for facts under the control of the issuer, such as internal mandate.

Exhibit 16: Requirement families mapped to the trust handshake

	Requirement family	Licensing	On-boarding	Pre-transaction	Settlement	Post-transaction
1	Issuer, instrument and asset governance	●		▲		
2	Safeguarding, custody and asset control	●	●	▲		
3	Legal identity and jurisdictional anchoring	●	●	▲		
4	Authority, mandate and delegation		●	▲		
5	Counterparty and participant due diligence		●	▲		
6	Account, wallet, address and control attribution		●	▲		
7	Transaction permissioning and policy enforcement		●	▲		
8	Governance, and accountability of the trust layer	■				
9	Participation and access	■	■			
10	Reliance, liability and dispute resolution	■	■			■
11	Client, investor and user protection	■	■	■		■
12	Market conduct and market integrity	■	■	■	■	■
13	Information exchange and data minimization	■	■	■	■	■
14	Recordkeeping, auditability and supervisory visibility	■	■	■	■	■
15	Interoperability	■	■	■	■	■
16	Operational resilience and security	■	■	■	■	■

● Establish the fact ▲ Verify and reuse it ■ Applies

Source: Oliver Wyman analysis

© Oliver Wyman and GLEIF

The last five rows are not bound to a specific stage. Market conduct and integrity are expected from any party engaged at any stage of the financial flow. Information exchange and data minimization apply wherever parties request and present evidence. Recordkeeping also applies across all stages because each stage produces evidence on which someone relies later. Interoperability and operational resilience are properties of the shared infrastructure rather than steps in a transaction.

Three families appear at both the licensing and pre-transaction stage, and six at both the onboarding and pre-transaction stage. These represent different requirements: establishing a fact from an authoritative source (for example, a mandate to transfer up to $100,000 exists) and verifying that same fact against the context of a specific transaction (a transaction of $125,000 exceeds that mandate). This distinction is what makes unbundling possible: issuers establish the facts, while relying parties verify and rely on them.

The full set of functional and non-functional requirements, organized by family within these stages, is set out in Appendix E.

Taken together, these requirements describe what would have to be true for trust functions to be sourced from whoever performs them best. They also provide a test of the market scenarios set out in Chapter 3.

- In an **integrated platform market**, most requirements are satisfied within a single institution, where they are met but not shared.
- In a **two-tier market**, the baseline requirements are met through shared infrastructure, while those requiring higher assurance remain within the licensed tier.
- In a **fragmented market**, the requirements are met inconsistently or not at all because no party can rely on another's evidence.
- The **modular market** is the only structure in which the full set of SIMFONIA requirements can be met across providers on terms on which others can rely.

Coverage of these requirements, rather than the adoption of any particular technology, is therefore the practical measure of progress toward a modular market. No combination of jurisdiction and asset class meets the full set today. Chapter 6 sets out what would have to change, and Chapter 7 discusses the questions that remain open.

© Oliver Wyman and GLEIF

Recommendations for enabling *modular, portable and verifiable trust*

Chapter 06



Modular trust takes coordination: identity providers turn trusted data into verifiable evidence, financial service providers put it to work in transactions, and regulators can give both the confidence to invest.

Realizing this model requires coordinated action across the ecosystem. SIMFONIA therefore sets out practical recommendations for three groups of stakeholders, each playing a distinct role in enabling portable, verifiable trust in digital and agentic transactions:

1. **Financial and transaction service providers**, ranging from traditional banks and payment providers to wallet, blockchain infrastructure, and agentic payment providers, which need to integrate these capabilities into their transaction and control processes.
2. **Digital identity and authoritative data providers**, which need to make trusted information available as scalable, interoperable, and machine-verifiable evidence.
3. **Regulators and public authorities**, which need to provide the regulatory, legal, and supervisory conditions for trusted information and controls to be used across new transaction models.

The recommendations broadly follow the development of the market. Financial and transaction service providers hold the customer relationships and the transaction volumes, so their adoption is what turns portable trust into market reality; identity and data providers develop the capabilities they consume; and regulators create the conditions for adoption. Standards-setting and ecosystem development are continuous, joint efforts involving all three groups (see Exhibit 17 for a summary of the recommendations)

Exhibit 17: SIMFONIA recommendations by actor group (summarized)

Financial service providers	Identity service providers	Regulators
Build shared understanding and ownership across business, technology, risk and compliance.	Design digital identity services for digital assets and agentic transactions.	Build regulatory understanding and coordination on digital assets, agentic AI and digital identity
Define what must be established for each transaction.	Extend digital identity from proving identity to proving the right to act.	Follow and interact with regulated firms who rely on portable, independently verifiable evidence
Separate persistent identity from changing transaction identifiers.	Turn authoritative data into portable, provenance-rich evidence rather than proprietary data moats.	Encourage regulated firms to rewrite internal policies that demand paper where the rules accept verifiable digital evidence.
Consume reusable external evidence and machine-readable authority.	Make credentials independently understandable and verifiable across ecosystems.	Support establishing a tiered, interoperable trust framework with recognized issuer lists.
Embed verification and policy controls into transaction execution.	Integrate verification directly into transaction execution.	Provide regulatory clarity that creates confidence to invest in modular trust.
Act as an issuer as well as a verifier.	Design for financial-market scale and prove it in production.	Acknowledge that verifiable control mechanisms extend from digital assets to agentic AI.
Extend the same control model to agentic payments.		
Joint actions		
Agree on common semantics for machine-verifiable authority and authorization.	Align service, product and transaction taxonomies.	Map assurance frameworks to transaction requirements.
Make trust discovery interoperable across sectors and jurisdictions.	Standardize how authority is bound to a transaction.	Standardize machine-verifiable delegation chains.

Source: Oliver Wyman analysis

6.1 Recommendations for financial service providers

Financial and transaction service providers can move first: they integrate portable evidence and transaction-time verification into their control models, systems and transaction flows, and work with regulators to advance the mutual understanding about what may be relied upon.

1. **Build shared understanding and ownership across business, technology, risk and compliance.** Digital assets and agentic payments increasingly raise similar questions around identity, authority, transaction rights and accountability, while many organizations manage them in separate silos.
2. **Define what must be established for each transaction.** Specify the required identity, authority, wallet or device control, mandate and compliance evidence, the sources that can be relied upon, and the level of assurance required for different transaction types and risks.
3. **Separate persistent identity from changing transaction identifiers.** Enable a verified person or organization to prove control over changing wallets, addresses, devices and agents without repeating the underlying identity process each time.
4. **Consume reusable external evidence and machine-readable authority.** Redesign onboarding, KYC and mandate processes to accept trusted external credentials where appropriate, and move from broad role-based mandates toward granular authorizations covering scope, limits, conditions, validity and delegation.
5. **Embed verification and policy controls into transaction execution.** Verify identity, authority, wallet or device control, mandate scope, credential status and applicable policies before value moves, and retain sufficient evidence to reconstruct the decision afterwards.
6. **Act as an issuer as well as a verifier.** Make appropriate facts for which the provider is itself an authoritative source — such as account or customer status, wallet control, entitlements, mandates or transaction permissions — available as reusable credentials beyond its own environment.
7. **Extend the same control model to agentic payments.** Use machine-readable delegation and transaction permissions to define who an agent acts for, what it may do and within which limits, rather than creating a separate identity and control architecture for AI agents.

© Oliver Wyman and GLEIF

6.2 Recommendations for identity service providers

Digital identity and data providers need to turn trusted information into portable, interoperable, and machine-verifiable evidence that can be used across transaction contexts.

1. **Design digital identity services for digital assets and agentic transactions.** Understand how wallets, direct settlement, smart contracts, and AI agents change requirements for identity, authority, authorization and accountability, and design services around those transaction flows.
2. **Extend digital identity from proving identity to proving the right to act.** Develop cryptographically verifiable credentials covering organizational role, authority, authorization, and delegation, including granular scope, limits, conditions, validity and revocation.
3. **Turn authoritative data into portable, provenance-rich evidence rather than proprietary data moats.** Enable users to trace claims back to their authoritative source and independently prove their provenance and integrity, while developing business models that incentivize authoritative data providers to issue and maintain reusable credentials.
4. **Make credentials independently understandable and verifiable across ecosystems.** Use common standards and machine-readable semantics for credential meaning, issuer identity, assurance, governance, and status, and support interoperable issuer discovery and assurance mapping across sectors and jurisdictions.
5. **Integrate verification directly into transaction execution.** Make identity, authority, authorization, credential status, and mandate scope consumable at machine speed by wallets, payment systems, smart contracts, and AI agents, and enable the resulting authority to be linked to the transaction being executed.
6. **Design for financial-market scale and prove it in production.** Verification must be fast, reliable, and inexpensive enough for routine high-volume and low-value transactions; develop real-world implementations with financial and technology providers to mature the economics, governance, and operating models.

© Oliver Wyman and GLEIF

6.3 Recommendations for regulators

Regulators and policymakers are following these developments closely and contributing to how they are understood.

1. **Build regulatory understanding and coordination on digital assets, agentic AI and digital identity, within and across jurisdictions.** Payments, digital assets, AI, AML, cyber, operational resilience and digital identity now meet at the point of transaction. Engage directly with the authorities and their financial institutions by helping to shape digital identity architectures and their governance, and keep aligning with regulators in other jurisdictions so that rules and supervisory expectations stay interoperable.
2. **Follow and interact with regulated firms who rely on portable, independently verifiable evidence at transaction time.** Align supervisory expectations, legal conditions for reliance, responsibilities and liability accordingly, including where issuer and relying party are in different jurisdictions.
3. **Encourage regulated firms to rewrite internal policies that demand paper where the rules accept verifiable digital evidence.** Regulation often already allows digital evidence, but firms translate it into internal policies that permit only one process, such as a paper mandate with a wet signature where the law accepts any verifiable form. Make clear in supervisory dialogue that such self-imposed constraints are not regulatory requirements, and that cryptographically verifiable evidence meets the same outcome.
4. **Support establishing a tiered, interoperable trust framework with recognized issuer lists.** Define proportionate criteria for different assurance levels, maintain or recognize interoperable trust lists, and support cross-border and cross-sector recognition of equivalent frameworks, so that Financial Institutions can decide which issuers and credentials they trust for a given purpose.
5. **Provide regulatory clarity that creates confidence to invest in modular trust.** Where needed, clarify the conditions under which reusable, cryptographically verifiable evidence is acceptable within existing regulatory frameworks, reducing uncertainty that may otherwise deter investment by financial institutions and identity service providers.
6. **Acknowledge that verifiable controls extend from digital assets to agentic AI.** Reuse the same identity, authority, delegation and transaction-permission mechanisms to determine an agent's right to act, and add the specific controls needed for probabilistic AI behavior.

© Oliver Wyman and GLEIF

6.4 Recommendations requiring joint action

Some of the remaining building blocks cannot be developed by any single actor. While credentials can be technically portable, trust only becomes scalable across organizations, sectors and jurisdictions when parties share enough common semantics, assurance mappings, issuer-recognition mechanisms and transaction conventions to interpret and rely on them consistently. The recommendations below therefore focus on areas requiring joint standardization and ecosystem alignment.

1. **Agree on common semantics for machine-verifiable authority and authorization.** Define how roles, mandates and permissions express scope, limits, conditions, validity and revocation so that people and machines interpret them consistently across systems and organizations. Across jurisdictions, agree how national terms map to a shared core of functional roles, rather than aligning the terms themselves.
2. **Align service, product and transaction taxonomies.** Develop common classifications and mappings so authorizations defined in one organization or sector can be understood and applied in another.
3. **Map assurance frameworks to transaction requirements.** Develop common mappings between existing assurance frameworks and use-case requirements so relying parties can determine whether a credential provides sufficient assurance for a particular service or transaction.
4. **Make trust discovery interoperable across sectors and jurisdictions.** Connect recognized issuer and scheme lists so relying parties can determine whether an issuer is trusted for a particular type of information without establishing bilateral arrangements.
5. **Standardize how authority is bound to a transaction.** Develop common mechanisms to cryptographically link mandates and authorizations to the specific transaction being initiated, so transaction systems can verify that the proposed action falls within the permitted scope before value moves.
6. **Standardize machine-verifiable delegation chains.** Define how authority can pass between organizations, individuals and software systems, including AI agents, while preserving upstream scope, limits, conditions, validity and revocation.

© Oliver Wyman and GLEIF

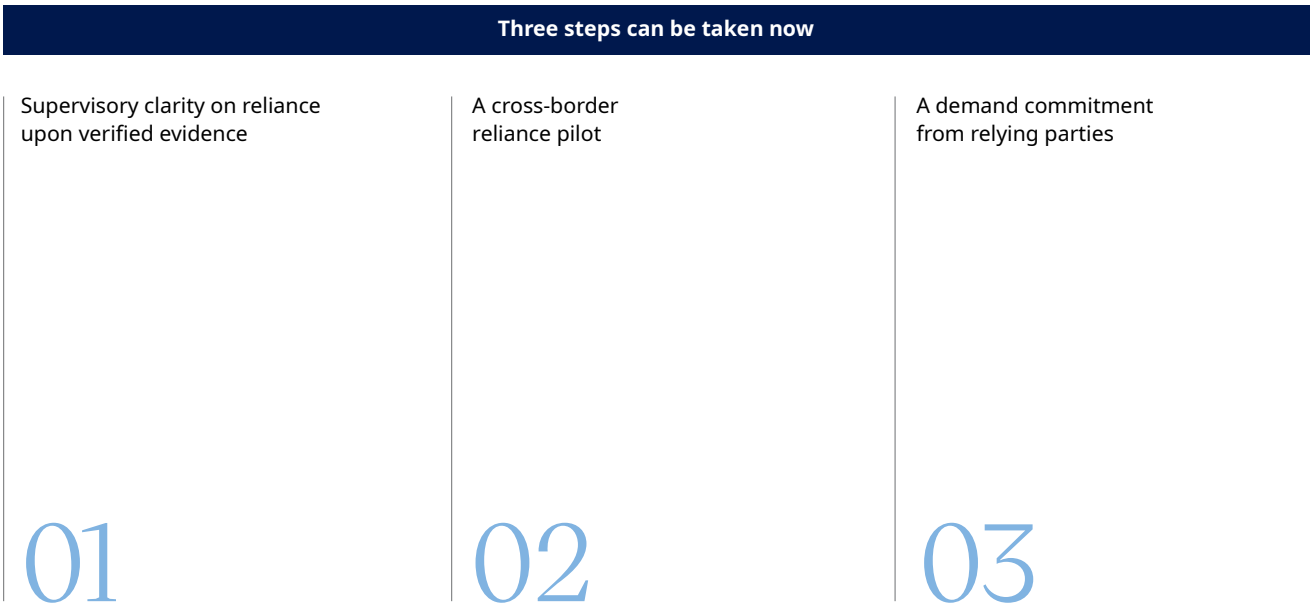
6.5 Where to start

The recommendations above describe what the transition requires. Three steps can be taken now, without new legislation or waiting for the rest of the ecosystem to be in place (see Exhibit 18).

1. **Supervisory clarity on reliance upon verified evidence.** A relying party cannot yet be sure what a verified credential entitles it to conclude. Supervisors can help reduce uncertainty by clarifying how existing regulatory requirements apply to the use of verified evidence. Where a recognised issuer attests to the accuracy of a claim under a governed framework and a relying party verifies that attestation before the transaction, the evidence may provide a basis for reliance, subject to applicable requirements. Industry can write the rulebook covering assurance levels, reliance conditions, and contractual liability. Supervisors can then provide guidance on how such arrangements fit within existing regulatory frameworks. Existing routes, such as a no-objection letter, supervisory guidance on an existing reliance regime, or a sandbox finding, may help provide clarity without new rulemaking, depending on the jurisdiction. Start with a narrow set of claims, such as legal entity identity and signatory authority, in a single jurisdiction and for a single asset class, and widen the scope once the model holds.
2. **A cross-border reliance pilot.** One rulebook in one jurisdiction shows that reliance works. It does not show that reliance crosses borders, and no single supervisor can settle that. Two financial centers with different trust frameworks should put credentials through a live transaction: a company identified and its signatory verified in one center, with that evidence relied on in the other. Each needs an operating source of entity identity and mandate data and a supervisor willing to state a position. The pilot answers whether assurance levels map, whether each supervisor accepts the other's recognized issuers, and who bears the loss when the evidence turns out to be wrong. The pilot should also measure how long it takes for a revocation in one center to cause the relying party in the other to reject the evidence, whether for a signatory's mandate, a wallet binding or, if included, an AI agent acting under that mandate.
3. **A demand commitment from relying parties.** Authoritative sources are being asked to fund issuance and carry liability for revenue that does not yet exist, which is why so few have moved. The barrier is demand, not technology. A group of relying parties that commits to accepting defined credentials from recognized issuers, at stated assurance levels and within a stated timeframe, turns issuance from a speculative cost into a funded one. Of the three, this is the step most likely to get the ecosystem moving, and it needs no one's permission.

© Oliver Wyman and GLEIF

Exhibit 18: Three steps that can be taken now



Open questions



Chapter 07

The remaining questions share one root: unbundling distributes the work, but someone still has to decide who may be relied on, who answers when evidence fails, who pays, and who holds the power.

This paper sets out a direction and provisional requirements, not a finished design.

Trust functions can be unbundled from an institution, but governance, accountability, and liability cannot; they have to be rebuilt across the split. How to rebuild them raises eight questions that emerged from the SIMFONIA working group and remain open (see Exhibit 19).

Exhibit 19: Open questions from the SIMFONIA working group

01	What may a relying party actually rely on?
02	On what legal basis can reliance cross borders?
03	Who is trusted to issue what?
04	Garbage in, cryptographically verified garbage out?
05	How to avoid over-asking?
06	Who pays?
07	Who benefits from a modular market?
08	Who controls the control points?

© Oliver Wyman and GLEIF

7.1
What may a relying party actually rely on?

A credential from a company register is a register extract in digital form, and FATF Recommendation 10 has always allowed verification against reliable, independent sources. A credential from a bank attesting to its own checks is different: this falls under Recommendation 17, which requires the third party to be supervised, requires the underlying documents to be provided on request, and leaves ultimate responsibility where it was.

The question, then, is where to draw the line between an issuer that is the authoritative source of a fact and one that is merely attesting to a check it performed. Supervisors have answered this question for identity through FATF's digital ID guidance and regimes that accept electronic identification at high assurance. However, they typically have not answered it for credentials attesting to authority, mandate scope, or beneficial ownership, which is where the line still needs to be drawn.

7.2
On what legal basis can reliance cross borders?

A rulebook works because one supervisor can accept it and one body of law contains it. Those conditions also limit its reach. Unbundling adds further complexity: the evidence may be issued under the law of one country and relied on in another, while the value moves under the law of a third.

Cross-border reliance holds only if the relying party's supervisor accepts evidence issued under a foreign framework, and recourse against the issuer requires a claim that can be enforced where the issuer is based. Principle 1 of the Principles for Financial Market Infrastructures (PFMI) requires a clear and enforceable legal basis in every jurisdiction involved.

How do assurance levels in one framework map to those in another? Which law governs a dispute when the issuer and relying party are in different jurisdictions? Can a judgment be enforced against an issuer over which the deciding supervisor has no authority? Differences in assurance, privacy, and evidentiary rules reflect policy choices, not technical gaps, so engineering will not close them. We expect regional blocs that recognize each other at the boundaries.

© Oliver Wyman and GLEIF

7.3 Who is trusted to issue what?

Portable credentials remove bilateral arrangements. What remains is deciding which issuers are trustworthy, for what purpose, at what assurance level, and for which facts a holder may vouch for itself (self-issuing). Trust lists are an important yet often overlooked part of the trust infrastructure. Statutory trusted lists under eIDAS in the European market show a workable pattern: an existing supervisor anchors recognition, criteria are published, and lists recognize each other rather than reporting to a single root. Applying the same pattern in finance raises three additional questions.

First, can a market-run scheme prevent its operator from becoming a large issuer? eIDAS avoids this conflict because a public supervisor maintains the list but issues nothing; a scheme run by a consortium of banks or platforms would have to establish that separation itself.

Second, how should relying parties treat a “too big to fail” issuer that is no longer fully trusted? The Dutch government faced this in 2011, when it had to ask software vendors to delay removing the breached certificate authority DigiNotar because public services depended on it. This might suggest a possible approach: guidance from a supervisor could allow relying parties to continue accepting those credentials for a limited period, with additional checks, while holders move to another issuer.

Third, who supervises the supervisors of trust? Recognizing an issuer is one layer. Accrediting the bodies that recognize issuers, and recognizing those bodies across borders, is another. Who is responsible for the “trust list of trusted lists”?

© Oliver Wyman and GLEIF

7.4
Garbage in, cryptographically signed garbage out?

Cryptography shows who issued a statement and that nobody has altered it, not that the statement is correct. Registers may lag, and registration mistakes happen. This is often raised as an objection to portable evidence, but the opposite is true. Once an error is found, the issuer revokes the credential, and from then on, every relying party that checks its status will see that it is no longer valid. A paper copy of a claim proven wrong can continue circulating in files and attachments, with nothing to signal that it is no longer valid.

What does disappear is the second pair of eyes: today, someone rereading an extract occasionally spots that the named director is not the person across the table, while an automated check that returns a valid result prompts nobody to look twice. What needs to be designed works in two directions. **Forward**: Each credential carries clear information on its freshness, revocation status, and the grounds on which it can be revoked. **Back**: Holders and relying parties can report a suspected error to the issuer, and holders can appeal a revocation they believe is wrong.

7.5
How to avoid over-asking?

Friction has always limited how much evidence a party asks for, and cheap verification removes that limit. Data protection and AML rules provide a weak counterweight: whatever a firm receives, it must protect and act on. But the penalty for asking too little is considerable and immediate, while the cost of asking too much is diffuse and comes later.

Three commitments would help prevent over-asking. First, assurance can be tiered according to transaction risk, so a small payment needs less evidence than a large one. Second, requests can default to predicates rather than attributes: “Is this company registered in the EU?” instead of requesting the full national register extract. Third, below a set threshold, a relying party can verify that whoever acts is authorized by a verified company without learning who that person or agent is. Each mandate carries its own identifier, so the custodian can enforce its limits and spot unusual use, while only the company knows who holds it.

Over-asking also increases the risk of exclusion: every extra credential requested is one more that someone may lack.

© Oliver Wyman and GLEIF

Transparency is the simplest tool against over-asking. Presentation requests already tell the holder what a relying party asks for. Publishing these in a comparable form would show where one relying party asks for more than its peers. Over-asking is hard to regulate, but industry and NGOs can already start publishing without action from regulators.

Exclusion is harder. A false match or a missing credential can stop someone from transacting, and a mistaken revocation now reaches every relying party at once. Redress requires a deadline for the issuer to make corrections, an appeal route that does not run solely through the relying party, and a manual route for anyone without a credential.

Correlation is the third risk: even when no attributes are disclosed, the record of who checked what about whom builds a picture of a person's commercial life. Relying parties should publish what they ask for, at which transaction values, and at what assurance level, in machine-readable form. Over-asking is hard to regulate but easy to observe, and industry can do this without anyone's permission.

7.6 Who pays?

Costs and benefits fall on different parties. The relying party avoids the work of establishing the fact. The issuer bears the cost of issuing the credential, keeping its status current, and carrying part of the liability if the credential proves incorrect. A public register may absorb these costs as public infrastructure; a private issuer has multiple ways to recover them. Models exist for each side: the holder pays (as with the LEI annual fee), the relying party pays (as with credit bureaus), a scheme fee spreads the cost (as with card networks), or the state funds it (as with national public identity schemes). Each model can work on its own. The open question is how to combine them into a working business model across jurisdictions and credential types when a single transaction may rely on credentials funded in different ways.

Three costs are also easily overlooked. First, governance, certification, and liability provisioning cost the same at any volume, which affects small participants most. Second, evidence that a check took place must remain verifiable for as long as anyone can examine the transaction, which means storing the validation data and trust list state as they stood at authorization. Third, an issuer that answers each status check individually learns where a holder presents its credentials. That is cheaper than privacy-preserving revocation and yields data it can sell, so without a rule against it, the cheaper option wins. Who funds these costs, and how, is still largely unresolved.

© Oliver Wyman and GLEIF

7.7
Who benefits from a modular market?

Not everyone. A platform that has built identity, compliance, and custody within its own operations benefits from fragmentation because weak shared infrastructure keeps competitors at low assurance levels and directs high-trust business its way. A two-tier market suits incumbents for the same reason: the regulated tier retains its franchise while the baseline tier remains dependent. Both market structures are stable and sufficiently comfortable for those who benefit from them that there is little incentive to push further.

Modularity pays off for everyone else: mid-sized institutions that would rather buy assurance than build it, specialist providers that need a market to exist at all, and customers who gain access to cheaper and faster financial services without becoming dependent on a single gatekeeper. The question is whether the parties that gain can move before the parties that do not entrench their position.

7.8
Who controls the control points?

Shared infrastructure creates dependencies, and dependencies can fail or be misused. Cutting sanctioned banks out of international payment messaging showed how quickly a shared utility becomes an instrument of political power. A single root, or a single list of trusted lists, allows one operator to exclude a participant, which federation and multiple anchors would have prevented.

Market concentration reaches the same result, although more slowly, since identity providers, wallet platforms, and trust-list operators can each become control points themselves. High-assurance credentials on phones depend on key storage and attestation managed by a few device manufacturers outside financial supervision, threatening availability rather than control.

No design removes political power over infrastructure. Good design reduces the number of control points, but it cannot eliminate them all. The open question is which ones remain, who holds them, and what keeps the system running when one of them is misused or fails.

© Oliver Wyman and GLEIF

Where this leaves us

The way trust is established and shared will help shape the next generation of financial markets. Without greater coordination, digital finance risks developing into fragmented ecosystems that limit interoperability, competition, and innovation.

SIMFONIA outlines a different direction: a more modular financial system in which trust can extend across institutions while preserving existing safeguards and accountability. The building blocks are emerging, but important questions around reliance, liability, governance, and economics remain.

Addressing these questions will require collaboration across the financial ecosystem. The three practical steps outlined in this report offer a starting point: clarifying when verified information can be relied upon, testing recognition across borders, and building market demand.

The opportunity is to shape how trust evolves while the next generation of financial markets is still being built. We welcome further dialogue with financial institutions, trust providers and regulators interested in exploring this direction.

© Oliver Wyman and GLEIF

Glossary

Digital assets and wallets	
Transaction	A transfer of value or of an instrument between two parties, including the cash leg of securities and foreign exchange (FX) settlement. The five-stage handshake applies to each leg.
Blockchain/ DLT vs digital asset	Blockchain or DLT (Distributed Ledger Technology) is the shared record and transfer infrastructure; a digital asset is the value or right represented and moved using it.
Tokenization/ tokenized asset	Tokenization represents money, securities or real-world rights as programmable digital tokens; the legal claim depends on the underlying instrument.
Stablecoin	A digital token designed to maintain a stable value relative to a reference asset, commonly a sovereign currency.
Digital-asset wallet and account-address	A wallet manages public-private cryptographic keypairs and transaction instructions; an account-address is a technical transaction identifier, not a verified legal identity.
Wallet-based finance	A blanket term for financial exchanges where digital wallets are involved to facilitate transactions and manage assets (for example, any type of tokenized digital asset).
Custodial wallet	A bank, CASP, VASP or other provider holds or controls the private keys and safeguards assets on the user's behalf.
Self-hosted wallet	A wallet in which the owner controls the private keys and assets, without an intermediary custodian; also called self-custody or non-custodial.
Hybrid custody model	An arrangement in which control, recovery or approval responsibilities are divided between the user and one or more service providers.
Permissioned token	A token whose issuer or administrator controls who may hold or transfer it.
Permissionless token	A token issued on an open infrastructure so that anyone can hold and transfer it without central approval, such as most cryptocurrencies.

Agentic payments	
AI vs agentic AI/AI agent	Artificial Intelligence (AI) performs intelligent tasks, while agentic AI can interpret goals, make decisions and take actions across systems with a degree of autonomy.
Agentic payment/ transaction	A payment initiated or executed by an AI agent on behalf of a person or organization under delegated authority.
Principal	The person or legal entity on whose behalf a wallet, representative or AI agent acts.
Delegated authority/ mandate	Permission defining what an agent or representative may do, for whom, within which limits and for how long.
Agent identity and authorization	Evidence identifying the agent and proving that the specific transaction falls within the mandate of the agent given to it by its principal.

Digital identity	
Digital identity	Digitally represented evidence of a persistent person or legal entity, distinct from changing accounts, wallets, addresses or agents.
Identity wallet vs digital-asset wallet	An identity wallet stores and presents credentials or proofs; a digital-asset wallet manages cryptographic keys and value transfers.
Cryptographically verifiable credential	Digitally signed evidence of identity, status, role, control or authority that another party can independently verify. (This refers to a technologically neutral concept, not the specific VC standard)
Issuer-holder-verifier model	The issuer creates a credential, the holder presents it, and the verifier checks its source, integrity, status and suitability for the purpose.
Issuer recognition/ trust list	A governed mechanism identifying which issuers are recognized for particular credentials, purposes and assurance levels.
Holder binding/ level of assurance	Holder binding links the presenter to the credential, while the level of assurance expresses confidence in the proofing and issuance process.
Selective presentation/ revocation	Selective presentation reveals only necessary information, while revocation and status checks confirm that the credential remains valid.

Trust architecture	
Trust functions	The identity, authority, control, compliance, authorization, accountability, evidence and recourse capabilities needed to support safe transactions.
Trust infrastructure	The shared governance, standards, services and technical mechanisms that let parties establish, exchange, verify and rely on trust evidence.
Modular trust layer	An ecosystem in which specialized providers supply portable, reusable and independently verifiable trust functions across platforms and transactions.
Trust handshake	The sequence of establishing identity and jurisdiction, authority, control, transaction data, policy outcomes, authorization, settlement and retained evidence.
Transaction-time assurance/trust record	Verification immediately before value moves, followed by retention of the proofs, checks and decisions needed for audit, supervision or dispute handling.

Reading list

This reading list sets out the sources behind the paper, grouped by type. It is a starting point for readers who want to explore the subject further, rather than an exhaustive literature review. Links were checked in October 2026.

International standards and supervisory frameworks

Basel Committee on Banking Supervision (2022), Prudential treatment of cryptoasset exposures.
Basel Committee on Banking Supervision (2024), Cryptoasset standard amendments.
Basel Committee on Banking Supervision (2025), Guidelines: Principles for the sound management of third-party risk.
Basel Committee on Banking Supervision (2026), SCO60: Cryptoasset exposures, Basel Framework, in force 1 January 2026.
Published version: SCO60 as published 27 November 2024.
Committee on Payment and Settlement Systems and International Organization of Securities Commissions (2012), Principles for financial market infrastructures.
Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (2022), Application of the Principles for Financial Market Infrastructures to stablecoin arrangements.
Financial Action Task Force (2020), Guidance on Digital Identity.
Financial Action Task Force (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.
Financial Action Task Force (2024), Guidance on Beneficial Ownership and Transparency of Legal Arrangements.
Financial Action Task Force (2025), Interpretive Note to Recommendation 15: Regulation of virtual assets and virtual asset service providers.
Financial Action Task Force (2026), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations, adopted February 2012, as amended June 2026. Direct text: fatf-recommendations-2012.pdf.
Financial Action Task Force (2026), Public consultation on guidance to increase payment transparency.
Financial Action Task Force (2026), Targeted Report on Stablecoins and Unhosted Wallets: Peer-to-Peer Transactions.
Financial Action Task Force (2026), Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs.
Financial Stability Board (2023), FSB Global Regulatory Framework for Crypto-asset Activities.
Financial Stability Board (2023), High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-asset Activities and Markets: Final report.
Financial Stability Board (2023), High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements: Final report.
Financial Stability Board (2024), The Financial Stability Implications of Artificial Intelligence.
Financial Stability Board (2025), FSB finds significant gaps and inconsistencies in implementation of crypto and stablecoin recommendations.
Financial Stability Board (2025), Thematic Review on the FSB Global Regulatory Framework for Crypto-asset Activities.
International Organization of Securities Commissions (2023), Final Report with Policy Recommendations for Decentralized Finance (DeFi).
International Organization of Securities Commissions (2023), Policy Recommendations for Crypto and Digital Asset Markets: Final Report.
International Organization of Securities Commissions (2024), Media release on crypto and digital asset markets.
International Organization of Securities Commissions (2025), Information note to accompany FSB and IOSCO reports.

Legislation and regulation

Australian Government (2024), Digital ID Act 2024.
European Commission (2018), Commission Delegated Regulation (EU) 2018/389 on regulatory technical standards for strong customer authentication and common and secure open standards of communication.
European Parliament and Council of the European Union (2014), Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
European Parliament and Council of the European Union (2015), Directive (EU) 2015/2366 on payment services in the internal market (PSD2).
European Parliament and Council of the European Union (2022), Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA).
European Parliament and Council of the European Union (2023), Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (Transfer of Funds Regulation).
European Parliament and Council of the European Union (2023), Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA).
European Parliament and Council of the European Union (2024), Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
European Parliament and Council of the European Union (2024), Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
Government of the Hong Kong Special Administrative Region (2000), Electronic Transactions Ordinance, Chapter 553.
Government of the Hong Kong Special Administrative Region (2025), Stablecoins Ordinance, Chapter 656.
Legislative Council of the Hong Kong Special Administrative Region (1999), Electronic Transactions Bill. Chinese-language source.
Legislative Council of the Hong Kong Special Administrative Region (2025), Bills Committee on the Stablecoins Bill, agenda 18 March 2025. Chinese-language source.

Central bank, supervisory and official research

Bank for International Settlements & IOSCO (2012), Principles for Financial Market Infrastructures
Bank for International Settlements (2022), Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs
Bank for International Settlements (2025), Annual Economic Report 2025: The next-generation monetary and financial system.
Bank for International Settlements (2026), Annual Economic Report 2026: Anchoring trust in money.
Bank for International Settlements (2026), Stablecoins: framing the debate.
Bank for International Settlements (2026), The anatomy of stablecoin transactions, Working Paper No. 1359.
Bank for International Settlements Innovation Hub (2026), Project Agorá.
Bank for International Settlements Innovation Hub (2026), Project Mandala.
Bank for International Settlements Innovation Hub (2026), Project Tamga.
Bank of England and Financial Conduct Authority (2024), Artificial intelligence in UK financial services 2024.
European Banking Authority (2019), EBA clarifies application of strong customer authentication.
European Banking Authority (2019), EBA publishes opinion on the elements of strong customer authentication.
European Banking Authority (2019), Single Rulebook Q&A 2018_4031 on strong customer authentication.
European Central Bank (2025), Exploratory work on new technologies for wholesale central bank money settlement.
European Central Bank (2026), Eurosystem Brings Central Bank Money to Tokenised Finance. ECB Press release
European Central Bank (2026), Tokenisation and digital capital markets, Macroprudential Bulletin, April 2026.
European Central Bank (2026), Towards an efficient and integrated digital capital market in Europe: the role of tokenisation and the Eurosystem's policy response.
Hong Kong Monetary Authority (2021), Circular on the use of iAM Smart for remote customer onboarding.

Hong Kong Monetary Authority (2024), HKMA launches stablecoin issuer sandbox.
Hong Kong Monetary Authority (2025), HKMA publishes supervisory and AML/CFT guidelines for stablecoin issuers.
Hong Kong Monetary Authority (2026), First licences granted under the Stablecoins Ordinance. Chinese-language source.
Hong Kong Monetary Authority (2026), Register of Licensed Stablecoin Issuers.
Hong Kong Monetary Authority (2026), Stablecoin issuers.
International Monetary Fund (2026), The Rise of Tokenization: Deciphering New Trends in Payments and Asset Tokenization, Note 2026/006.
Keyrock (2026), Who Pays the Agent? The Race for Frictionless Machine Payments. Written in collaboration with Coinbase, Tempo and Virtuals
Standard Chartered Bank (Hong Kong) and Anchorpoint Financial Limited (2026), Standard Chartered becomes first bank distributor of HKDAP to unlock real-economy benefits of HKD stablecoins.
The Hong Kong and Shanghai Banking Corporation (HSBC) (2026), HSBC RedCoin launches today.
Visa and Artemis (2026), Agentic Payments from the Ground Up: What the Onchain Data Tells Us.

Technical standards and specifications

CPMI-IOSCO (2022), PFMI applied to stablecoin arrangements – Application of the Principles for Financial Market Infrastructures to stablecoin arrangements, final version.
International Organization for Standardization (2023) SO/TR 6039:2023, Blockchain and distributed ledger technologies — Identifiers of subjects and objects for the design of blockchain systems
FIDO Alliance (2026), FIDO Alliance to develop standards for trusted AI agent interactions.
Global Legal Entity Identifier Foundation (2026), Introducing the vLEI Ecosystem Governance Framework.
Global Legal Entity Identifier Foundation (2026), The verifiable LEI (vLEI).
International Organization for Standardization (2021), ISO/IEC 18013-5: Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application.
International Organization for Standardization (2025), ISO 17442: Legal Entity Identifier, including the verifiable LEI.
Internet Engineering Task Force, SD-JWT-based Verifiable Credentials (SD-JWT VC).
OpenID Foundation (2025), OpenID for Verifiable Credential Issuance 1.0.
OpenID Foundation (2026), OpenID for Verifiable Presentations. Specification index: openid.net/developers/specs.
Trust over IP Foundation, Governance Metamodel.
World Wide Web Consortium (2025), Verifiable Credentials Data Model v2.0.
World Wide Web Consortium, Digital Credentials API.
Hkchain (2026). Hkchain: A Layered Reference Architecture for Chain-Enforced Stablecoin Compliance. Technical Report, version 1.0.

Digital identity schemes and trust frameworks

Australian Government, Digital ID System Administrator (2026), The Australian Government Digital ID System (AGDIS), including the Relationship Authorisation Manager.
Digital Policy Office, Government of the Hong Kong Special Administrative Region (2026), iAM Smart use cases.
Digital Agency, Government of Japan, My Number Card and smartphone identity functionality.
European Commission, European Digital Identity Wallet and the List of Trusted Lists.
Government of India, Ministry of Electronics and Information Technology (2026), DigiLocker.
Government of Singapore (2026), Singpass.
Government of Singapore (2026), Corppass.
iSHARE Foundation (2026), iSHARE Trust Framework. Governance and scope: iSHARE Manifesto.

Logius (2026), eHerkenning.
Open Banking Limited, UK Open Banking standards and directory.
Reserve Bank of India, Account Aggregator framework.
United Arab Emirates Government (2026), UAE PASS.
United Arab Emirates Government (2026), UAE Verify.
United Kingdom Department for Science, Innovation and Technology (2026), UK digital verification services trust framework.
United States Transportation Security Administration, (2026) Mobile driver's license participating states and eligible digital IDs.

Digital asset infrastructure and platforms

Anchorage Digital, Anchorage Digital institutional platform.
Anchorage Digital, Atlas Coordinated Multiparty Settlement.
Anchorpoint Financial Limited (2026), Anchorpoint commences institutional rollout of HKDAP via Beta Access.
Canton Network, Canton Network.
Circle, Circle Mint.
Citi, Citi Token Services.
Chainalysis (2026), The New Rails: How Digital Assets Are Reshaping the Foundations of Finance.
Coinbase, Coinbase Prime.
Coinbase, Verified on-chain attestations.
Fidelity, Fidelity Digital Assets.
Fnality, Fnality Sterling Payment System.
Global Layer One (2026), GL1 Public Consultation Whitepaper.
Hong Kong Monetary Authority, Project Ensemble and Ensemble TX.
HSBC, HKD stablecoin plans and PayMe integration.
J.P. Morgan (2026), Kinexys by J.P. Morgan. Blockchain Deposit Accounts and JPM Coin: JPM Coin.
National Payments Corporation of India, Unified Payments Interface (UPI).
Partior, Partior network.
Regulated Liability Network, Regulated Liability Network.
Sparkasse, Reusable age credentials.
Standard Chartered, Authorized bank distributor of HKDAP.
Swift (2026), Swift's blockchain ledger ready for use: 17 banks set to pioneer tokenised cross-border payments on trusted global infrastructure.
Tom Barbereau, Balázs Bodó (2023), Beyond financial regulation of crypto-asset wallet software: In search of secondary liability, Computer Law & Security Review, Volume 49, ISSN 2212-473X, doi.org/10.1016/j.clsr.2023.105829.

Agentic payment protocols and services

Adyen, Adyen Agentic.
Apple, Wallet credential storage, presentation and verification.
Cloudflare, Cloudflare Monetization Gateway.
Chainalysis (2026), Agentic Payments Cross the Threshold: Inside x402's Path to Meaningful Adoption.
Google (2025), Announcing the Agent Payments Protocol (AP2).
Google, Credential storage, presentation and verification in wallets and browsers.
Mastercard (2026), Santander and Mastercard complete Europe's first live end-to-end payment executed by an AI agent.
Mastercard (2026), Worldline, ING and Mastercard complete a live end-to-end European agentic payment in production.

© Oliver Wyman and GLEIF

Mastercard, Mastercard Agent Pay.
Stripe and OpenAI (2026), Stripe and OpenAI launch Instant Checkout and the Agentic Commerce Protocol.
Visa (2025), Find and Buy with AI: Visa unveils new era of commerce.
Visa (2026), Visa Intelligent Commerce.
Visa, Trusted Agent Protocol (TAP).
Visa and Artemis (2026), Agentic Payments from the Ground Up.
x401, x401 identity proof protocol.
x402 Foundation (2026), x402 protocol.

Travel Rule networks and compliance utilities

Address Ownership Proof Protocol (AOPP), AOPP
Global Travel Rule, Global Travel Rule network.
Notabene (2026), Travel Rule messaging protocols and the Notabene Gateway.
OpenVASP Association (2026), Travel Rule Protocol (TRP).
Sygna (CoolBitX) (2026), Sygna Bridge.
Travel Rule Information Sharing Alliance (2026), TRISA and the Global Directory Service.
VerifyVASP, VerifyVASP network.
Zeb and DekaBank (2026), SWIFT-based travel rule solution: Establishing a scalable market standard for crypto transactions in European banking.

Appendix A
Developments in digital assets and agentic payments

A.1. Proof points: global adoption and institutionalization of digital assets and agentic payments

7 proof points	Digital assets	Agentic payments
01 **Adoption and growth trajectory**	Tokenization is scaling rapidly: tokenized assets on public blockchains grew from €7.4 billion at the start of 2024 to ~€38 billion by February 2026, more than a five-fold increase. (Source: European Central Bank, ECB — Tokenisation and digital capital markets)	AI is already deeply embedded in traditional finance: 75% of surveyed financial firms use AI, rising to 94% of international banks; 55% of reported use cases already involve some automated decision-making. This is broader AI adoption, but provides the foundation for agentic payments. (Sources: Bank of England, Bank of England/FCA — AI in financial services)
02 **Market/ ecosystem scaling**	Stablecoins have become a ~$320 billion market: BIS estimates global stablecoin market capitalization at approximately $320 billion at end-May 2026, demonstrating significant scale for tokenized forms of money. (Sources: Bank for International Settlements, BIS — Annual Economic Report 2026)	Agentic payments are being connected to existing global payment scale: Visa Intelligent Commerce is being built on a network with 4.8 billion payment credentials, 175 million+ merchant locations and 300 billion + transactions annually. These figures describe the underlying network — not current agentic-payment volumes — but show the infrastructure agents can potentially access. (Sources: Visa, Visa — Intelligent Commerce)
03 **Transaction activity**	On-chain transaction volumes are already enormous: BIS estimates stablecoins processed approximately $28 trillion of transaction volume in 2025; a separate BIS estimate puts payment-related flows at about $390 billion, highlighting both the scale of blockchain activity and the remaining runway for real-economy payments. (Sources: Bank for International Settlements, BIS — Stablecoins and the monetary system)	Machine-native payments now have measurable live activity: the x402 protocol processed approximately 109.6 million transactions and $15 million in adjusted volume between May 2025 and mid-2026; the newer Machine Payments Protocol recorded ~115,000 transactions in its first weeks. (Sources: Visa, Visa/Artemis — Agentic Payments from the Ground Up)
04 **Institutional participation**	Central banks and major FIs are actively building tokenized-finance infrastructure: BIS Project Agorá brings together 7 central banks and 43 regulated financial institutions to explore tokenized commercial-bank deposits and central-bank money for cross-border settlement. (Sources: Bank for International Settlements, BIS — Project Agorá/next-generation monetary system)	The major payments ecosystem is mobilizing: Visa has launched Intelligent Commerce with technology partners including OpenAI, Microsoft, Anthropic and Stripe; Mastercard has launched Agent Pay; and banks including Santander and ING have participated in live agentic transactions. (Sources: Visa Investor Relations, Visa — Intelligent Commerce launch)

7 proof points	Digital assets	Agentic payments
05 **Live/ production adoption**	Tokenized settlement has moved beyond laboratory experiments: the Eurosystem's DLT work involved 64 participants across nine jurisdictions and nearly €1.6 billion in central-bank-money settlement, including trials involving real transactions in production environments. (Sources: European Central Bank, ECB — DLT central-bank-money settlement trials)	Agentic payments have reached live banking infrastructure: Santander/Mastercard executed a live end-to-end AI-agent payment in March 2026, and in June ING, Worldline and Mastercard completed an end-to-end agentic payment in production between an ING cardholder and Dutch merchant. (Sources: Mastercard, Mastercard/ING/Worldline — production transaction)
06 **Standards and interoperability**	Traditional financial infrastructure is being adapted for tokenized money: Swift's blockchain ledger became ready for initial use in 2026, with 17 banks across six continents preparing to pilot live cross-border transactions using tokenized deposits. (Sources: Swift, Swift — tokenized cross-border payments ledger)	A standards ecosystem is emerging quickly: Google's Agent Payments Protocol (AP2) was developed with 60+ organizations and uses mandates to establish user intent and agent authority; Stripe/OpenAI separately released the open Agentic Commerce Protocol (ACP), already powering Instant Checkout in ChatGPT. (Sources: Google Cloud, Google — AP2; Stripe/ OpenAI — ACP)
07 **Increasing regulatory attention**	A dedicated global regulatory architecture now exists: the FSB has established a global crypto/stablecoin regulatory framework based on "same activity, same risk, same regulation," while FATF applies AML/CFT requirements to virtual assets/VASPs and continues to monitor implementation globally. Its 2026 review found progress but continuing jurisdictional gaps. (Sources: Financial Stability Board, FSB — Global Crypto Regulatory Framework; FATF — 2026 VA/VASP implementation review)	Regulation is earlier and largely technology-neutral: there is no dedicated global agentic-payments regime yet. The FSB has called on authorities to assess whether existing financial regulation adequately covers AI risks such as model governance, cyber risk and third-party concentration; regional regimes such as the EU AI Act add AI-specific requirements alongside existing payment, AML and consumer rules. (Sources: Financial Stability Board) [Sources: FSB — AI in financial services; EU — AI Act]

A.2. Current regulatory responses to create compliant transactions for traditional, wallet-based and agentic transactions

Lifecycle step	Compliance actions	FIAT **FIAT payments**	Wallet **Digital assets/wallets**	Agent **Agent-initiated overlay**
Organization				
i **Licensing and classification**	• License • Custody/ safeguarding • Audit and risk	• **Local banking/payment/ e-money laws** • **BCBS*** • **Resilience rules** Role-based license; client-fund protection; governance and audit	• **FATF R.15** • **FSB** • **IOSCO** • **Local CASP/issuer law** Perimeter; custody, reserves, governance and operational risk	• **Underlying rail** • **TPR/outsourcing** • **AI/technology rules*** Classify agent role; govern providers; regulated entity stays accountable
Customer				
ii **Onboarding**	• Identity and jurisdiction checks • BO • Sanctions/PEP checks • Mandates • Limits • Ongoing CDD	• **FATF R.10/12** • **Local AML/KYC** Principal and BO CDD; authority; periodic and event-driven refresh	• **FATF R.10/12/15** • **Local AML/CFT** Principal/BO KYC; wallet relationship; permissions, limits and refresh	• **Underlying AML/KYC** • **Mandate rules** Principal KYC; agent identity; mandate, delegation, limits and revocation
Transaction				
1 **Pre-transaction**	• Counterparty and principal • Authentication, consent, authority and limits • AML/fraud • Recorded outcome	• **Consent/SCA*** • **Sanctions** • **Payment transparency** Payer/payee validation; authority and limits; AML/ fraud; decision evidence	• **FATF R.6/7/16** • **Travel Rule** • **IOSCO conduct controls*** Wallet/CASP screening; transfer data; authorization and fraud evidence	• **Underlying rail** • **Mandate/auth** • **Fraud/payment transparency** Bind agent to principal; check scope, payee and limits; retain evidence
2 **Settlement and reconciliation**	• Execute or route • Clear where applicable • Reconcile	• **Scheme/finality law** • **PFMI*** • **Safeguarding rules** Execution/finality; rail controls; ledger and safeguarding reconciliation	• **Local rail/custody rules** • **PFMI*** • **Reserve and ledger controls** Finality; custody; on-chain, reserve and ledger reconciliation	• **Underlying rail/ finality rules** • **Operational resilience** Execute only within mandate; match instruction → execution → outcome
3 **Post-transaction**	• Monitor and report • Hold/block/freeze • Recall/return/recover • Disputes	• **AML reporting** • **Consumer liability** • **Incident/dispute rules** Monitoring/STR; protective actions; errors, liability and disputes	• **FATF R.11/20/21** • **IOSCO** • **Local conduct/ custody rules** Monitoring/reporting; freezes; custody records; recovery and disputes	• **Underlying rail** • **Incident/liability** • **AI/outsourcing controls*** Monitor agent; suspend mandate; report incidents; recovery and disputes

Global standards set the baseline; local law makes them binding. Agentic is an overlay on the underlying rail

* Role- and perimeter-dependent: IOSCO for market/intermediary activity; PFMI for FMIs or systemically important stablecoin arrangements; BCBS for banks; AI rules where in scope.

Source: Oliver Wyman analysis

A.3. Local regulatory overlays across regions and jurisdictions

Jurisdiction	i Licensing	ii Onboarding	1 Pre-transaction	2 Settlement	3 Post-transaction
Europe • UK • Switzerland					
European Union Current/transition	PSD2/EMDR MiCA, DORA	AMLD/AMLR CDD, BO, PEP	SCA RTS/TFR Sanctions, fraud	PSD2 execution TFR, PFMI	AML reporting DORA, disputes
United Kingdom Current + 2027	PSRs/EMRs MLRs, crypto 2027	MLRs registration CDD/BO	Consent/auth Travel Rule	PSRs, finality Scheme rules	MLR reporting Liability/disputes
Switzerland Classification-based	Banking Act/ AMLA/DLT FINMA classification	AMLA CDD/BO Issuer-holder controls	Transfer restrictions Sanctions/authority	Custody/settlement Ledger reconciliation	Reporting, complaints Recovery actions
Asia					
Singapore Current + proposed	PSA, FSMA DTSP MAS stablecoin rules	PSN02/AML-CFT CDD/BO	Auth, limits Travel Rule/screening	PSA safeguarding Execution/ reconciliation	Reporting, incidents Disputes/recovery
Japan Current	Payment Services Act FIEA where relevant	KYC/AML Asset segregation	Travel Rule Authority/screening	Transfer/custody rules Reconciliation	STRs, user protection Incident response
South Korea Current	VASP registration Virtual Asset User Protection Act	KYC/AML User-asset segregation	Travel Rule Authority/screening	Custody controls Reconciliation	Monitoring, reports Incident cover
Hong Kong Current	PSSVFO, AMLO/SFO Stablecoins ordinance	HKMA/SFC AML-CTF CDD/BO	Screening, transfer data Authority/limits	RPS/finality Reserves/ reconciliation	STRs, freezes Complaints/recovery
China (Mainland) Current	Non-bank Payment Regs./PBOC license VC, stablecoin and RWA restrictions	AML Law, real-name CDD BO registry, agent identity	Auth, active mandate/limits AML, fraud, traceable instructions	PBOC reserves/ clearing, SAFE FX e-CNY framework, no VC settlement	Large-tx + STR reporting Records, freezes, incidents/complaints
Americas and other selected jurisdictions					
Canada Federal + provincial	PCMLTFA/FINTRAC CSA registration	MSB/FMSB CDD BO/sanctions	VC Travel Rule Transaction screening	CSA platform/custody Settlement controls	STRs, client assets Complaints/recovery
United States Federal + state	State MTLs, BSA/MSB GENIUS Act	CIP/KYC BSA, OFAC	BSA/OFAC Reg E where covered	Federal/state Rail rules	SARs, Reg E OFAC actions
Brazil Current 2026	Law 14,478 BCB Res. 519–521	KYC/AML-CFT Governance	Traceability Self-custody checks	VASP/custody/FX Settlement records	Reporting/incidents Client protection
Australia Transition 2026–2027	Corporations Act/DAF AUSTRAC VASP rules	VASP enrolment CDD/governance	AML/CTF, transfer data Authority/fraud	AFSL/market rules Reconciliation	SMRs, safeguarding Disputes/incidents
United Arab Emirates Multi-perimeter	CBUAE PTSR VARA/ADGM by perimeter	AML/CFT Client-asset controls	Screening, Travel Rule Authority/limits	Custody/transfer Rail/reserve rules	Reporting, conduct Recovery/disputes

Applicability: Local perimeter depends on entity, activity, asset, customer/solicitation, geography and settlement nexus. Agentic payments remain an overlay on the underlying regulated rail.

Source: Oliver Wyman analysis

Appendix B
Digital identity

B.1. Digital verifiable credentials explained in more detail

The process of establishing and verifying an actor's identity, attributes, rights, and authorizations can be described through the issuer–holder–verifier model, also known as the trust triangle. Identity establishes who the actor is, while attestations establish relevant facts about that actor, such as regulatory status, wallet control, mandate, or authority to act.

The process starts with an issuer, typically an authoritative source, establishing a trusted fact about a person or legal entity. This may concern the subject's identity or an attribute linked to that identity, such as a person's date of birth, a company's legal representatives, or its regulatory status. Where required, the relevant person or legal entity first proves its identity to the issuer, which then issues a credential containing the relevant information and digitally signs it.

The holder presents the credential, or a proof derived from it, to a verifier. The verifier establishes whether it trusts the issuer as an authoritative source for that type of information and checks the credential's signature, validity, status, and contents before deciding whether it provides sufficient evidence for the intended purpose.

Today, this process often involves paper documents or digitized copies of them, manual inspection, bilateral checks, and local storage of evidence. Cryptographically verifiable credentials allow the same trust relationship to operate fully digitally.

Several concepts support this model:

1. Issuer recognition establishes whether the credential was issued by a source that is recognized as appropriate for the particular claim. For example, a company-register credential should come from an official register or another recognized issuer of legal-entity information. Often, recognized issuers or trust service providers (TSPs) are vetted and published on trust lists maintained by a higher-level authority or scheme operator, allowing verifiers to determine whether an issuer is recognized for a particular type of credential or service in a specific context.
2. Credential authenticity and integrity can be proven without a doubt because the issuer signs the credential with its private key, and the relying party checks that signature against the issuer's public key, obtained from a trust list or registry it recognizes. Any change to the credential after signing, even of a single character, makes the signature fail. Authenticity and integrity prove where the credential came from and that it is unchanged, not that its content is correct or still valid, which are separate checks.
3. Holder binding ensures that a credential cannot simply be copied and used by someone else. The verifier checks that the presenter controls the cryptographic key or device to which the credential is bound and, where relevant, is the person or legal entity entitled to exercise the associated rights or mandate.

4. Level of assurance indicates the degree of confidence that can be placed in the identity proofing and issuance process behind a credential. For example, a high-value transaction may require a credential issued at a higher level of assurance than a low-risk service interaction.
5. Selective presentation allows only the information required for a particular purpose to be shared. For example, a holder may prove that they are authorized to approve a payment without disclosing the full mandate or unrelated personal information.
6. Validity and revocation determine whether a credential may still be relied upon at the time of use. A credential has an issuance date and may have a predefined expiry date or lifespan. The verifier may also impose its own freshness requirement, for example by accepting only credentials issued or revalidated within a specified time period. In addition, the issuer can revoke a credential before expiry, for instance when the underlying license is withdrawn. These conditions are checked immediately before the transaction is executed.
7. Auditability is the requirement to enable independent reconstruction of who issued a credential, under which authority, its validity at the time of reliance and how it supported a decision, using tamper-evident records without centrally storing the underlying data.

B.2. Cryptographically verifiable credentials are becoming mainstream infrastructure

Digital identity and cryptographically verifiable credential concepts have existed for many years, but regulation, technical standardization and market adoption are now converging.

Regulation and public policy are driving adoption across jurisdictions worldwide for both personal and business-related credentials. The seven examples below are selected not only for their scale, but because each illustrates a different element of the emerging issuer–holder–verifier model relevant to SIMFONIA.

1. India's DigiLocker shows the model operating at exceptional scale, with more than 700 million registered users able to access and share legally recognized, digitally verifiable documents issued by government and other trusted organizations. It demonstrates that reusable, issuer-backed digital evidence can operate at population scale.
2. Australia's Government Digital ID System (AGDIS) supports around 15 million Digital IDs, while its Relationship Authorization Manager allows individuals to establish authority to act for businesses. It demonstrates how identity, organizational relationships and authority can be separated and verified as distinct trust components.
3. The UAE combines UAE PASS, with 12.5 million registered users, with digital signing and UAE Verify, through which 157 million trusted digital documents have been issued and can be independently verified for source, integrity and validity. It is a strong example of national digital identity being extended into reusable, cryptographically verifiable evidence across public and private-sector services.
4. More than 20 US states and territories now offer mobile driver's licenses, enabling millions of users to present attributes such as age, address, driver license or veteran status directly from their smartphones while selectively disclosing only the information required. It is a strong example of standards-based, cryptographically verifiable attributes and selective disclosure.

5. The Netherlands' eHerkenning provides more than one million business authentication means and supports fine-grained mandates to act on behalf of organizations across over 2500 distinct services at 600 public and private relying parties. It is particularly relevant to SIMFONIA because it shows authority can be granted at the level of individual services rather than only through broad organizational roles.
6. The EU's European Digital Identity Wallet will make interoperable digital identity and attribute wallets available across the EU, potentially reaching more than 450 million citizens as well as businesses, with mandatory acceptance in specified use cases. It is the clearest example of regulation, common standards and mandatory acceptance being combined to create an interoperable cross-border trust ecosystem.
7. Japan's My Number system reaches around 100 million card holders, with more than 7.5 million already carrying its cryptographically verifiable identity functionality on their smartphones. It illustrates how an established national identity infrastructure can evolve from card-based identification to smartphone-based attribute verification.

These examples are illustrative rather than exhaustive, with similar initiatives emerging across the globe.

Technology is also converging around common standards. Several interoperable credential models and formats are maturing in parallel, including W3C Verifiable Credentials, ISO mdoc and IETF SD-JWT VC, and ACDC credentials supported by KERI-based infrastructure, while OpenID4VCI and OpenID4VP increasingly standardize how credentials are issued and presented. These standards are already being incorporated into major public digital identity infrastructures, although different jurisdictions continue to use different combinations of technologies. In parallel, further standards are being developed to define how specific types of information and permissions should be expressed for different sectors and asset classes. The interoperability profile should remain open to additional credential families and presentation mechanisms where provenance, status and assurance can be verified.

Market adoption is developing on both sides of the trust triangle. On the issuance side, more reusable credentials are becoming available: the vLEI is one example for attesting organizational identity, roles and authority across borders. Financial players are also entering the issuing market. For example, Sparkasse is issuing reusable age credentials and Coinbase is issuing verified on-chain attestations. On the other side, Apple and Google are embedding credential storage, presentation and verification capabilities directly into wallets, smartphones and browsers, while verification capabilities are increasingly being integrated into financial-service infrastructure.

The EUDI Wallet illustrates both the opportunity and the current immaturity of the market: regulation sets the framework, common standards enable interoperability, and mandatory acceptance helps create a market where commercial use cases and adoption are still developing.

Taken together, these developments are creating the technical, regulatory and commercial foundations for cryptographically verifiable credentials to become increasingly reusable across organizations, sectors and jurisdictions.

B.3. Explanation of GLEIF and vLEI

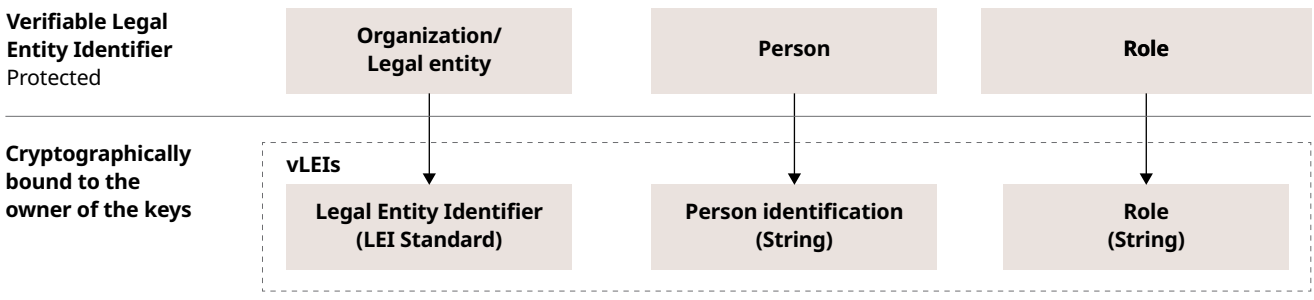
The LEI is a universal ISO standard identifier for legal entities (ISO 17442). It enables reliable identification and due diligence of counterparties worldwide and is widely mandated, endorsed, or referenced as an identifier in financial market and payments regulations worldwide. The LEI adheres to the ISO 17442 principles of (i) being a global standard, (ii) providing a single unique identifier for each legal entity, (iii) being supported by high-quality data, and (iv) operating as a public good, available free of charge to all users.

LEIs can be obtained by any type of legal entity in any jurisdiction worldwide. This includes not only corporations, private companies, and investment vehicles but also other economic actors, including government agencies, ministries, central banks, multilateral institutions, trusts, and associations. LEIs are issued through a trusted network of issuers accredited and monitored by GLEIF. These LEI issuers verify reference information, including an entity's ownership structure, against authoritative and authentic local sources.

The LEI register provides essential "Level 1" reference data. This is openly accessible via the GLEIF website and API and can also be used to access further information from other sources, including an entity's local or original registry and other data providers. This information helps "translate" other essential attributes of a company (also using ISO standards), for instance, by transliterating names, identifying legal forms, and identifying parent or related companies. An LEI can help link to information about an entity's license, credit rating, beneficial owners, or other details, such as legal officers and official organizational roles (OOR).

The Verifiable LEI (vLEI) is a system of high-assurance, granular digital credentials. These provide cryptographically secure "keys" that link an entity's LEI to a designated person acting on its behalf in an official role (e.g., CFO) or a context-specific, entity-defined role. From an anchor set of Legal Entity and OOR vLEI credentials, officers can issue, delegate, and revoke credentials autonomously, while enabling third parties to verify them against an open network of time-stamped and preserved "key event logs." vLEI can be used to sign and demonstrate control over assets and onchain addresses, be embedded in smart contracts, and verify control over beneficiary accounts or other rights, such as those assigned to an AI agent.

Exhibit 20: Illustration of components of a vLEI credential



Source: GLEIF

Appendix C
Proof points for four scenarios

This appendix describes the examples plotted in Exhibit 11 in Chapter 3.1, explaining what each one does and why it sits in its quadrant. The examples are positioned according to the market structure they produce, rather than their maturity or quality. They include regulations, schemes, prototypes, and commercial platforms, since each shapes market structure in its own way. The list is illustrative, not exhaustive, and reflects each example's status at the time of publication.

Exhibit 21: Scenario 4. Modular market examples

Example	What it does	Why it fits Q4
EUDI Wallet and eIDAS trust services — implementation	Creates common wallet specifications, interoperable credentials, legally defined trust-service roles and EU-wide mechanisms for recognizing trusted issuers and service providers.	Identity, signatures, attributes and other trust services can be issued by specialized regulated providers and reused by many relying parties. The Commission's List of Trusted Lists is a genuine federated trust-discovery mechanism.
UK Digital Verification Services Trust Framework — live framework	Sets role-specific rules and certification requirements for identity, attribute, holder, orchestration and component services, supported by a public register of certified services.	Multiple specialist providers can be recognized for defined trust functions and relied on through common rules and discovery, rather than through a bilateral contract with every relying party.
Singpass and Corppass — live public identity infrastructure	Provide reusable personal authentication through Singpass and organization-level authorization through Corppass, including managed employee permissions for digital services.	Identity and authority are separated into reusable public trust services that can support many government and private-sector relying parties.
GLEIF vLEI — live infrastructure	Provides cryptographically verifiable credentials linking a legal entity with the identity, authority and organizational role of a person acting for it.	It turns organizational identity and signing authority into a reusable, portable trust module that can support payments, reporting and counterparty verification across platforms.
ISO/IEC 18013-5 mobile driving license — published credential standard	Defines standard interfaces for an mDL to present data to a reader, bind it to the holder, authenticate its issuing source and verify data integrity.	It provides an interoperable credential format that specialized issuers, wallets and verifiers can use across services without one platform owning the full relationship.
UK Open Banking — live adjacent analog	Separately regulates account-information and payment-initiation activities and provides common APIs, security profiles, consent rules and a directory verifying authorized participants.	Specialist providers can perform defined activities across banks using a shared trust framework, rather than becoming the customer's full-service bank. This is one of the clearest live examples of modular, activity-level market design.
iSHARE Trust Framework — live cross-sector analog	Combines a shared legal and technical rulebook with participant, identity and authorization registries and supports federation across data spaces.	Identity, membership and permissions can be provided and verified by different specialist actors while remaining mutually recognized under one governance framework.

Example	What it does	Why it fits Q4
India Account Aggregator — live cross-sector analog	Creates a regulated, consent-based channel through which licensed Account Aggregators transmit financial information from providers to authorized users without retaining the data.	Data access is unbundled from the institution holding the account and delivered through shared rules, consent artifacts and specialist intermediaries.
BIS Project Tamga — prototype	Tests cross-border discovery and verification of licenses and regulatory attestations using existing web infrastructure and machine-readable trust metadata.	Regulatory status could be verified as a standalone service across jurisdictions and systems, without every institution maintaining bilateral registries or proprietary verification processes.
BIS Project Mandala — prototype moving to phase 2	Pre-validates jurisdiction-specific rules and generates privacy-preserving cryptographic compliance proofs that can accompany different payment instructions or digital settlement assets.	Compliance is separated from the payment rail and expressed as independently verifiable evidence, making it a particularly strong example of a reusable modular compliance component.
FIDO agentic authentication and delegation — under development	Develops standards for agent authentication, phishing-resistant user instructions, revocable delegation and verifiable authority for agent-initiated transactions.	It aims to make proof of customer intent and agent authority interoperable across agents, wallets, merchants and payment networks rather than proprietary to each platform.
Anchorage Atlas Coordinated Multiparty Settlement — emerging boundary example	Separates custody, trade matching, credit/intermediation and settlement among custodians, venues, prime brokers and institutional participants.	Unlike Anchorage's integrated custody platform, Atlas expressly unbundles market functions and coordinates evidence and settlement across specialized regulated actors. It is still network-specific, so it sits near the Q2–Q4 boundary rather than at the center of Q4.
Coinbase Bitcoin Yield Fund tokenized share class (ERC-3643 on Base)	Token-level eligibility enforcement against identity claims (ERC-3643, Apex as on-chain transfer agent).	Boundary case because the trusted-issuer registry is appointed by the issuer, not a shared trust list.

Exhibit 22: Scenario 3. Fragmented market examples

Example	What it does	Why it fits Q3
Sygna Bridge — live protocol/network	Enables members of its VASP alliance to exchange FATF Travel Rule originator and beneficiary information through encrypted messaging.	It performs a specialist compliance function, but trust and reach are tied to the Sygna network rather than automatically recognized across all VASPs and protocols.
TRISA Global Directory Service — live network	Issues network-specific identity certificates and provides VASP discovery and counterparty information for TRISA members.	TRISA creates meaningful shared trust inside its network, but the certificate and directory model remains one of several Travel Rule ecosystems rather than a universal market layer.
OpenVASP Travel Rule Protocol — live standard	Provides an open, peer-to-peer protocol for VASPs to exchange Travel Rule data without a central intermediary.	It unbundles the information-exchange activity, but counterparties still need compatible implementations and their own identity, due-diligence and risk arrangements.
VerifyVASP — live Travel Rule network	Provides encrypted peer-to-peer exchange of originator and beneficiary information, VASP discovery and related verification services for member institutions.	It creates trust inside its own member network, but recognition and interoperability still depend on counterparties using or connecting to the same scheme.

Example	What it does	Why it fits Q3
Global Travel Rule — live Travel Rule network	Provides API and manual workflows for encrypted Travel Rule data exchange, member connectivity and out-of-network handling.	It reduces bilateral integration for participating VASPs, but remains one network among several with its own membership and operating arrangements.
Overlapping agentic protocols — emerging ecosystem	AP2 addresses payment mandates; ACP covers checkout and delegated payment; Visa TAP identifies trusted agents; x401 requests identity proofs; and x402 enables HTTP-native payments.	These are useful, partly complementary building blocks, but there is not yet one mutually recognized framework binding agent identity, principal authority, payment credentials, liability and compliance across all networks.
Cloudflare Monetization Gateway — emerging	Enables websites, APIs and AI tools to require and verify stablecoin payments over HTTP before granting access.	The access-and-payment function is modular, but the gateway does not itself establish a shared framework for customer identity, agent mandate, liability or regulated compliance.
AOPP — abandoned protocol	Defined a wallet-signing flow through which a user could prove control of a withdrawal address to a VASP.	It addressed a narrow wallet-control proof, depended on bilateral implementation by exchanges and wallets, and did not provide a broader shared identity or reliance layer; adoption was withdrawn by major wallets.

Exhibit 23: Scenario 2. Two-tier market examples

Example	What it does	Why it fits Q2
SWIFT tokenized-deposit ledger — initial pilot	Provides a shared orchestration layer for bank-issued tokenized deposits, with participating banks using the network for tokenized cross-border payment pilots.	The infrastructure is common, but deposits remain on participating banks' ledgers; banks retain compliance and risk controls, and settlement uses regulated institutional systems.
BIS Project Agorá — prototype and real-value testing	Combines tokenized commercial-bank deposits and wholesale central-bank money on a programmable multi-currency platform for atomic cross-border settlement.	The settlement infrastructure is shared, but participation is limited to central banks and regulated financial institutions, which retain their customer and compliance responsibilities.
Pontes — launched with phased implementation	Links market DLT platforms with Eurosystem TARGET Services so wholesale tokenized-asset transactions can settle in central-bank money.	It provides a common settlement utility for eligible banks and market infrastructures, while access, onboarding and compliance remain within the regulated institutional tier.
Fnality Sterling Payment System — live	Provides a regulated DLT-based wholesale payment system backed one-for-one by funds held at the central bank and designed to interoperate with external applications.	It is shared settlement infrastructure, but access is through regulated financial institutions and the surrounding customer and compliance functions remain institution-based.
Partior — live network	Operates a permissioned shared ledger for 24/7 cross-border clearing, settlement, FX and transaction pre-validation.	Authorized financial institutions share a common settlement layer, while retaining their customer relationships, due diligence and regulated responsibilities.
HKMA Ensemble TX — real-value pilot	Enables banks and other participants to use tokenized deposits for real-value digital-asset transactions, initially settling interbank positions through Hong Kong's RTGS system.	It creates a common institutional rail, but regulated banks continue to issue the money, onboard participants and carry the compliance obligations.
Canton Network — live institutional network	Connects institutional applications through a shared synchronization layer while allowing participants to keep private sub-ledgers and permissioned data flows.	The network supplies shared interoperability and settlement coordination, but participant identity, permissions and compliance controls remain anchored in institutions and applications.

Example	What it does	Why it fits Q2
Regulated Liability Network — proof-of-concept	Explores a shared ledger on which tokenized regulated money and securities can support programmable, multi-asset and cross-network settlement.	It creates common infrastructure under existing legal and regulatory arrangements, while regulated institutions continue to issue liabilities, onboard customers and carry the obligations.
UPI — live retail shared rail	Provides an interoperable real-time payment system and standard APIs through which banks and payment applications send, clear and settle retail payments.	The baseline rail is shared at scale, but regulated banks and PSPs retain customer onboarding, authentication, fraud, compliance and recourse.
Visa Intelligent Commerce and Mastercard Agent Pay — rollout/live use cases	Add agent registration, tokenized payment credentials, user-intent controls and agent-recognition signals to existing payment networks.	Agents use shared global rails, but issuers, acquirers, PSPs and merchants continue to provide authentication, fraud controls, authorization, recourse and regulated accountability.
Adyen Agentic — limited availability	Provides modular feed, cart and payment APIs and translates between multiple agentic-commerce protocols while retaining fraud screening and payment processing.	There is a shared orchestration layer, but merchants remain dependent on an integrated PSP platform and retain the merchant-of-record relationship.
Notabene SafeGateway — live	Connects VASPs to several Travel Rule protocols, identifies counterparties, exchanges required information and supports screening.	It is a reusable shared utility, but it operates behind regulated VASPs, which remain responsible for CDD, risk assessment and the decision to transact.

Exhibit 24: Scenario 1. Integrated platform market examples

Example	What it does	Why it fits Q1
J.P. Morgan Kinexys Blockchain Deposit Accounts — live	Provides eight-currency blockchain deposit accounts, 24/7 movement, programmable payments and on-chain FX within J.P. Morgan.	Identity, KYC/AML, deposit account, programmability and settlement are anchored inside one regulated bank. Assurance is platform-specific rather than portable across providers.
Citi Token Services — live	Enables eligible Citi clients to make near-real-time, 24/7 liquidity transfers and trade-related payments through Citi accounts, channels and APIs.	The account relationship, onboarding, permissioning, liquidity and transaction controls remain inside Citi; the assurance is not portable outside the platform.
Coinbase Prime — live	Combines institutional custody, trading, financing, staking and on-chain operations through a single Prime relationship.	The client accesses multiple functions through one regulated platform, which performs onboarding, custody, permissions and risk controls internally.
Anchorage Digital institutional platform — live	Provides qualified custody together with trading, settlement, fiat services, staking and governance support.	The core offering consolidates regulated custody and related activities in one federally chartered platform. Anchorage Atlas CMS, discussed under Q4, represents a different and more modular model.
Fidelity Digital Assets — live	Provides institutional custody, asset transfer, trading execution and collateral-related services through an integrated digital-asset platform.	Keys, custody, trading access and controls are consolidated behind a single Fidelity relationship rather than supplied as independently portable trust services.
Circle Mint — live	Allows eligible institutions to mint, redeem, custody and transfer USDC, EURC and cirBTC through Circle accounts and APIs.	Onboarding, asset issuance, mint/redemption permissions, custody and account controls are centered on the licensed issuer's platform.

Appendix D
Hong Kong case study

This appendix supports the Hong Kong case in Chapter 4. It sets out the timeline of legal, identity, and regulatory milestones from 2000 to the present, followed by three visuals based on the HKChain technical report and research by Prof. James Zhibin Lei (Hong Kong University of Science and Technology (HKUST)): the stablecoin regulatory framework and its first licensees, an on-chain identity and compliance model, and the transaction flows enabled by the Stablecoins Ordinance.

D.1. Hong Kong developments detailed timeline

Date	Milestone	Contribution to trust and modularity
January–April 2000	Electronic Transactions Ordinance, Cap. 553. The Ordinance was gazetted in January 2000, and the key provisions recognizing electronic records and digital signatures commenced on 7 April 2000. It also established a framework for recognized certification authorities. (Legislative Council of Hong Kong)	Creates the foundational legal-trust layer: electronic evidence, signatures and certificates can be relied on across different digital services instead of every participant requiring paper documentation.
2017–29 December 2020	The Government announced a common electronic identity in the 2017 Policy Address and launched iAM Smart on 29 December 2020. It provides authentication, user-authorized form filling and, through iAM Smart+, legally backed digital signing. The Digital Policy Office provides APIs for adoption by public and commercial services. (iAM Smart)	Adds a reusable identity and authentication component. Service providers can integrate a common government-backed capability instead of building every identity and signature function independently.
24 May 2021	The HKMA confirmed that iAM Smart was an acceptable technology for banks' remote onboarding and could supply authentication results and verified Hong Kong identity-card data through APIs. Banks nevertheless remained responsible for applying risk-based CDD. (HKMA Document Repository)	Shows how shared identity infrastructure can reduce repeated document collection, while preserving the regulated institution's responsibility for the customer relationship.
January 2022–December 2023	The HKMA issued its stablecoin discussion paper in January 2022, published conclusions in January 2023 and, with the Financial Services and the Treasury Bureau, issued a detailed legislative proposal in December 2023. The proposed regime followed the principle of "same activity, same risk, same regulation" and prioritized fiat-referenced stablecoin issuance. (Hong Kong Monetary Authority)	Moves from general digital trust to activity-specific financial regulation: the issuance activity is regulated according to its risks rather than requiring one vertically integrated digital-asset platform.

Date	Milestone	Contribution to trust and modularity
March–July 2024	The HKMA launched its stablecoin-issuer sandbox on 12 March and selected the first participant groups on 18 July. Participants tested operational models, reserves, redemption, wallet and private-key controls, technology risks and AML/CFT arrangements within controlled limits. (Hong Kong Monetary Authority)	Allows regulators and specialist providers to test common outcomes without prescribing one blockchain or technology stack — the technical-assurance layer is standardized, while implementation can vary.
December 2024–June 2025	The Stablecoins Bill was gazetted on 6 December 2024, passed by the Legislative Council on 21 May 2025 and gazetted as the Stablecoins Ordinance on 30 May. The Government appointed 1 August 2025 as its commencement date. (Legislative Council of Hong Kong)	Converts the proposed assurance model into a statutory licensing regime, including enforceable requirements for reserves, redemption, risk management, AML/CFT, governance and supervision.
1 August 2025	The Stablecoins Ordinance, Cap. 656, and the final HKMA supervisory and AML/CFT guidelines came into force. Licensed issuers must meet capital, full-backing, reserve-segregation, redemption, disclosure, technology-risk and AML/CFT requirements. The AML/CFT framework includes customer and beneficial-owner identification, ongoing monitoring, wallet ownership or control checks, and screening of self-hosted wallets. (Hong Kong Monetary Authority)	Creates a standardized regulatory assurance package that wallets, custodians, distributors and payment providers can use as a common trust signal. It does not require one blockchain or mandate the use of iAM Smart.
30 September 2025–10 April 2026	The HKMA received 36 applications by the initial application deadline. On 10 April 2026 it granted the first licenses to Anchorpoint Financial Limited and The Hongkong and Shanghai Banking Corporation Limited. (Hong Kong Monetary Authority)	Moves the framework from legislation into implementation. License status becomes an independently supervised attribute rather than a self-declared issuer claim.
April 2026–current	The statutory HKMA Register of Licensees under the Stablecoins Ordinance currently lists two issuers: Anchorpoint, license FRS01, and HSBC, license FRS02, both effective from 10 April 2026. (Hong Kong Monetary Authority)	The public register acts as an authoritative trust list that different market participants can consult. It is not yet a prescribed machine-verifiable credential or common regulatory API.
October 2026	Anchorpoint began the phased rollout of HKDAP, which included eligible institutional clients and partners pursuing on-chain use cases. Starting from 24 August 2026, Standard Chartered had become the first authorised bank distributor of HKDAP. (Anchorpoint) Separately, HSBC launched RedCoin (RCHKD) to retail users through PayMe on 23 October 2026. Integration with the HSBC HK Mobile Banking App remains planned for later in 2026. (HSBC)	Provides practical evidence of modularity: the issuer and distributor can be separate regulated entities, connected by common license, reserve, compliance and disclosure requirements. The ecosystem remains at an early implementation stage.

Hong Kong regulated stablecoin issuance and digital identity in three key visuals

The following insights are drawn from the HKChain technical report and research findings shared by Professor James Zhibin Lei (HKUST). They are presented in Exhibits 25, 26, and 27.

First, Exhibit 25 outlines six core requirements of Hong Kong's stablecoin regulatory framework, which together establish safeguards for transparency, financial integrity, consumer protection, and market stability. It also identifies Hong Kong's first stablecoin licensees, granted licenses in 2026: Anchorpoint and HSBC.

- Anchorpoint adopts a B2B2C ecosystem model targeting institutional and corporate clients, leveraging distributors and open APIs.
- HSBC, in contrast, pursues a bank-led retail model, using its existing retail network to target mass-market users and payments.

Exhibit 25: Hong Kong Stablecoin Regulatory Framework

100% reserve backing High-quality liquid assets verified by independent auditors to ensure full collateralization.	**Real-name KYC** Mandatory Customer Due Diligence (CDD); strict prohibition of anonymous accounts.	**Zero-threshold travel rule** Applies to all transfers; enhanced data sharing for transactions ≥ HKD 8,000.
Transparency reporting Daily par-value statements and weekly public disclosures for full market visibility.	**At-par redemption** Guaranteed redemption at face value to maintain user trust and stability.	**AML/CFT controls** Robust transaction monitoring to prevent money laundering and illicit finance.

First stablecoin licensees granted on 10 April 2026

Licensee	Anchorpoint	HSBC
Model	B2B2C ecosystem	Bank-led retail
Go-to-market	Distributors and Open API; 1st phase HKDAP on 12 August 2026	Existing retail network
Focus	Institutional and corporate	Mass retail and payments

Sources: HKUST analysis, Professor James Zhibin Lei

Two critical components of Hong Kong's developing on-chain compliance framework are (a) the modular identity model and (b) the compliance gates (see Exhibit 26).

a) The top part shows the envisioned six-tier identity model, which defines what each type of user can do. From blacklisted addresses at L0 to licensed issuers at L5, every transaction's permission is pre-determined.

b) The bottom part shows seven compliance gates: pre-execution checks that every transaction must pass. They cover KYC, sanctions, travel rules, and more. Any failure results in a blocked transaction, which is logged on-chain for audit.

Together, these two elements create a bypass-resistant, privacy-preserving and fully auditable system designed to support robust regulatory compliance for stablecoin transactions.

Exhibit 26: Identity Framework and On-chain Compliance

01 | Six-tier identity model (chain-enforced)

A consensus-embedded hierarchy defining transaction permissions directly on the blockchain, ensuring regulatory alignment at the protocol level.

L0 — Blacklisted

Zero access: Cannot hold or transfer tokens; protocol-level block.

L1 — Unverified

Testnet-only access; restricted from mainnet transactions.

L2 — Retail basic

HKD 8,000 cap; simplified Travel Rule reporting.

L3 — Retail enhanced

Unlimited tx; full IVMS101 compliance.

L4 — Institutional

Entity-verified; full privileges for institutions.

L5 — Licensed issuer

Admin-level; mint/burn permissions.

Immutable enforcement

Identity levels are hard-coded into the chain, eliminating any possibility of regulatory bypass.

02 | Seven compliance gates (pre-execution)

AnteHandler checks that every transaction must pass before execution. Failures are logged as immutable on-chain events.

KYC Gate

Verifies both parties are KYC-verified.

Sanctions

Blocks addresses on global sanction lists.

Travel Rule

Validates IVMS101 data for transfers.

Threshold

Flags high-value tx for manual review.

Velocity

Detects suspicious frequency patterns.

Role Gate

Restricts actions to assigned roles.

Agent Policy

Enforces agent-level send limits.

Auditable records

All gate decisions (allow/block) are recorded as on-chain events, creating a tamper-proof audit trail.

Sources: HKUST analysis, Professor James Zhibin Lei

Exhibit 27 presents stablecoin transaction flows that can be enabled under the Hong Kong Stablecoin Ordinance, with a focus on identity verification, wallet ownership validation and AML compliance.

- During onboarding (minting), issuers must conduct full KYC/CDD checks and verify ownership of destination wallets, whether custodial or self-custodial, to ensure traceability.
- During off-boarding (redemption), users can redeem stablecoins from any wallet type, with issuers verifying ownership of the sending wallet before disbursing fiat funds to the user's verified bank account.

Exhibit 27: Hong Kong stablecoin: on/offboarding and cross-wallet transfer

01 | On-boarding (minting)

Issuers conduct full KYC/CDD for all users. Mandatory verification of destination wallet ownership (custodial/self-custodial) is required prior to minting to ensure traceability.

02 | Off-boarding (redemption)

Users can redeem from any wallet type. Issuer verifies ownership of the sending wallet and disburses fiat to the user's verified bank account, ensuring compliance with AML standards.

Transfer route	Primary compliance responsible party	Travel Rule (IVMS101) required
Self-custody → self-custody	Stablecoin issuer (on-chain protocol gates + post-monitoring)	No (no VASP gateway)
Self-custody → VASP-custody	Receiving VASP	Yes (receiving side)
VASP-custody → self-custody	Sending VASP	Yes (sending side)
VASP-custody → VASP-custody	Both sending + receiving VASP	Yes, bilateral data exchange

Sources: HKUST analysis, Professor James Zhibin Lei

Appendix E
Requirements

Potential functional and non-functional requirements

The requirements below derive from analytical work conducted during the SIMFONIA workshop in Zurich, as well as discussions with and reviews by members of the working group.

They are a first articulation intended for market testing. Requirement families are expected to be added, consolidated and re-scoped as they are tested against transaction flows in practice and against supervisory expectations.

The requirements are not specific to wallets. They apply wherever trust functions are performed across multiple parties rather than inside a single institution, whether because those functions have been unbundled from a bank or other regulated institution, or because the market developed without one. This covers wallet-based payments, agentic transactions, tokenized deposits and securities, stablecoin settlement, and the traditional systems with which these interact.

The requirements describe what an ecosystem must deliver collectively rather than what any individual system must contain. No single provider is expected to satisfy the full set. The relevant test is whether each requirement is met by an identifiable party, on terms on which others are able to rely.

Functional requirements describe what the trust infrastructure should enable. Non-functional requirements describe the design qualities needed for those functions to operate safely, efficiently and at scale. The requirements are not tied to one technology, wallet model, identity framework or regulatory regime. They should be supported across custodial, hybrid and self-hosted wallet models.

The requirements assume compliance with applicable data protection law and do not restate it. Data minimization and purpose limitation appear below as functional properties of the infrastructure, but the legal basis for processing, the rights of data subjects, and the conditions for cross-border transfer are governed by law and by the relevant supervisory authorities, not by the trust layer.

Requirements are numbered continuously across the appendix (see Exhibit 28 below for the overview).

Exhibit 28: Typology of requirements in one overview

E-I. Foundational requirements inside each family

E-II. Cross-cutting requirements across families

E-III. Sixteen families of requirements

1 Issuer, instrument and asset governance	**2** Safeguarding, custody and asset control	**3** Legal identity and jurisdictional anchoring	**4** Authority, mandate and delegation
5 Counterparty and participant due diligence	**6** Account, wallet, address and control attribution	**7** Transaction permissioning and policy enforcement	**8** Governance, and accountability of the trust layer
9 Participation and access	**10** Reliance, liability and dispute resolution	**11** Client, investor and user protection	**12** Market conduct and market integrity
13 Information exchange and data minimisation	**14** Recordkeeping, auditability and supervisory visibility	**15** Interoperability	**16** Operational resilience and security

E-I. Foundational requirements

The requirements in this appendix are not of equal weight. The following form the main subset without which the remainder cannot operate. They are stated in full in their respective families and are listed here to indicate sequence for anyone assessing or building against this set.

	Requirement
E-II.1	Relying-party autonomy: a verifiable claim does not determine whether a transaction is acceptable
E-II.2	Separation of evidence, policy, decision and enforcement
E-II.3	Evidence verifiable against an authoritative or recognized source
E-II.7	Revocation visible in published status information within a bounded and known interval
E-II.8	Relying party sets how recent evidence must be
E-III.15	Delegation chain verifiable as an object in its own right
E-III.16	Each link bounded by the authority granted by the link above it
E-III.43	Reliance conditions linked to evidence and to the assurance level relied upon
E-III.55	Allocation of loss where evidence proves incorrect, set out in advance
E-III.73	Record establishes what was relied upon and that it was valid at the point of authorization

The first two establish what the trust layer does not do, and without them the remainder describes a central utility rather than shared infrastructure. Requirements E-II.3, E-II.7 and E-II.8 are the minimum for evidence to be relied upon at transaction time. Requirements E-III.15 and E-III.16 are the minimum for authority to be relied upon where the acting party is not the entity itself. Requirements E-III.43, E-III.55 and E-III.73 are the minimum for reliance to survive a dispute.

E-II. Cross-cutting Requirements — applicable across all families

Three sets of requirements apply across every family: the design principles that establish the boundary of the trust layer, the functional requirements that recur in each family, and the non-functional qualities the infrastructure needs for those functions to operate at scale.

Because these apply throughout, they are not repeated in the individual families below. In particular, neutrality across wallet models and settlement environments, data minimization, and the machine-readability of exchanged information are stated here once and should be read into every family.

Design principles

These establish what the trust layer does not do, and apply irrespective of family.

1. The trust layer preserves relying-party autonomy. A verifiable claim does not determine whether a transaction is acceptable. Each relying party decides whether the evidence is sufficient for its own obligations, policies and risk appetite.
2. The trust layer separates evidence, policy, decision and enforcement. It supports the exchange and verification of evidence. It does not assess whether evidence is sufficient, apply a participant's policy, or enforce a transaction outcome, unless a participant has expressly assigned that function to it.

Cross-cutting functional requirements

3. Evidence should be capable of being presented and cryptographically verified against an authoritative or recognized source, without the trust infrastructure itself becoming the source of truth.
4. Evidence should be capable of carrying assurance metadata, including source, issuer, verification method, validity, timestamp and revocation status, without that metadata determining sufficiency.
5. Participants should be able to prove relevant attributes or conditions, and to demonstrate that a required check was performed and with what outcome at the time of authorization, without disclosing unnecessary underlying information, client files, internal policies or risk models.
6. Evidence should be capable of being linked to a transaction context, including transaction intent, authorization outcome and settlement reference.
7. A revocation should appear in the issuer's published status information within a bounded and known interval. Where settlement is final on submission, there is no cancellation behind the control point, so visibility before reliance is the only available protection.
8. A relying party should be able to set, for a given transaction type, how recent any evidence must be, distinguishing between re-checking the status of evidence already held and requiring a newly issued attestation.
9. Access to information should be role-based and purpose-bound. Participants, auditors, supervisors and other authorized parties should receive only the information or references required for their role, legal basis and transaction context.
10. An evidence request should carry the purpose for which the information is sought, and the holder should be able to establish that purpose before responding.
11. Information should be machine-actionable and, where operators, auditors, supervisors or accountable decision-makers need to interpret it, human-readable.
12. A relying party should be identifiable and accountable for what it requests. A holder should be able to establish who is asking, under what registration or recognition, and for what purpose, before responding.
13. An issuer should not learn where or when a credential it issued is presented, unless the fact being attested genuinely requires a real-time check with that issuer.

Cross-cutting non-functional requirements

14. The infrastructure should connect participants, evidence, references and validation traces, and should not become the central repository for underlying evidence, policies or decision records.
15. The infrastructure should be neutral across technologies, wallet models and settlement environments, supporting custodial, hybrid and self-hosted wallet models as well as traditional financial systems, public chains, private chains, provider ledgers and token platforms.
16. The marginal cost of a verification should be low enough to permit verification per transaction rather than once per relationship.
17. Components should be modular, so that individual systems can be replaced or upgraded without breaking the wider trust model.
18. Two presentations of the same credential to different relying parties, or to the same one on different occasions, should not be linkable by the issuer, by the infrastructure or by a third party observing both.
19. Verification should complete within the time available before a transaction is authorized, including in machine-initiated flows where that interval is sub-second.

E-III. Sixteen Families of Requirements

E1. Issuer, instrument and asset governance

The trust infrastructure should allow participants to connect a transaction to relevant information about the asset being transferred. It should not determine the legal classification, economic value or eligibility of the asset. It should link asset-related information from issuers, registries, platforms, custodians and other recognized sources to the relevant wallet, counterparty and transaction context.

Functional requirements

1. The trust infrastructure should allow participants to request, present and verify information about the issuer, instrument, asset type, token terms, eligible holders, transfer restrictions and redemption rights.
2. The trust infrastructure should allow asset-related information to be linked to transaction intent, wallet attribution, counterparty eligibility and authorization outcomes.
3. The trust infrastructure should allow references to asset lifecycle events, including issuance, redemption, suspension, maturity, corporate actions and changes in transferability, to be connected to the relevant transaction or holding.
4. The trust infrastructure should allow identifiers of instruments and other objects, and the registers that issue them, such as the ISIN, to be verified in the same way as identifiers of subjects (natural or legal entities).

Non-functional requirements

5. The infrastructure should remain neutral as to asset class and should support internationally recognized standards and formats for financial instruments, including stablecoins, tokenized deposits, tokenized securities and tokenized real-world assets.

E2. Safeguarding, custody and asset control

The trust infrastructure should allow participants to obtain verifiable information about how an asset is held, safeguarded or controlled. It should not custody assets, control wallets, freeze assets or determine legal ownership. It should connect custody, control and safeguarding information to the relevant wallet, asset, party and transaction context.

Functional requirements

6. The trust infrastructure should allow participants to request, present and verify information about the applicable custody or control model, including institutional custody, self-custody and smart-contract-based control.
7. The trust infrastructure should allow participants to identify which party is responsible for custody, safeguarding, wallet operation, asset control and recovery, and to establish where no such party exists.
8. The trust infrastructure should allow custody and control information to be linked to wallet attribution, ownership, authority and transaction context.

E3. Legal identity and jurisdictional anchoring

The trust infrastructure should allow participants to connect a transaction to verifiable information about legal identity and the relevant jurisdictions. A wallet address does not establish who the legal entity is, where it is established, or which regulatory context applies. The infrastructure should enable participants to bring that information into the transaction context without becoming the identity register or the legal authority for identity.

Functional requirements

9. The trust infrastructure should allow participants to request, present and verify legal entity information, including legal name, registration number, legal form, registered address and relevant identifiers.
10. The trust infrastructure should allow participants to present and verify jurisdictional and regulatory status information, including jurisdiction of incorporation, establishment, licensing, operation and service provision, linked to the relevant participant, role and transaction context.
11. The trust infrastructure should allow legal identity and jurisdictional information to be connected to transaction intent, wallet attribution and authorization outcomes.
12. The trust infrastructure should allow a change in a legal entity's status, including merger, split, renaming and dissolution, to be referenced, so that a relying party can establish which entity a past credential or mandate referred to and what succeeded it.

Non-functional requirements

13. The infrastructure should support cross-border use without assuming that one jurisdiction's identity or registration framework is sufficient for all purposes.

E4. Authority, mandate and delegation

The trust infrastructure should allow participants to connect a transaction to verifiable information about who may act for a legal entity. Technical signing capability does not establish legal or operational authority. The infrastructure should enable participants to bring authority, mandate and delegation evidence into the transaction context, without becoming the system that grants or administers those mandates.

Where the acting party is an automated agent, authority is rarely a single step. It runs from the entity to a role-holder to an agent, and potentially onward. Scope, limits and revocation status can change between two transactions, and no single participant holds that state. The requirements below therefore treat the mandate and the delegation chain as objects to be verified in their own right.

Functional requirements

14. The trust infrastructure should allow participants to request, present and verify information about who is acting on behalf of a legal entity, including natural persons, systems, service providers and automated agents, and should allow that information to be linked to recognized sources such as mandate systems, company records, board approvals, powers of attorney, regulated service providers and qualified trust service providers.
15. The trust infrastructure should support the presentation and verification of a delegation chain as an object in its own right, from the legal entity through any role-holder to the acting party, and onward where authority has been further delegated.
16. The trust infrastructure should allow each link in a delegation chain to be verified as bounded by the authority granted by the link above it.
17. The trust infrastructure should support the presentation and verification of a mandate as a structured instrument, identifying the actor, the scope and purpose of the mandate, any quantitative limits, its validity window, its issuing chain and its revocation reference.
18. The trust infrastructure should allow a revocation at any point in a delegation chain to be propagated to the links below it, separately from the validity of any individual link.
19. The trust infrastructure should allow the assurance level of a delegation chain to be presented and verified, including the nature of the source in which the chain is anchored.
20. The trust infrastructure should allow authority to be scoped to the relevant transaction context, including role, asset type, amount, counterparty, jurisdiction, approval threshold and validity period, and to be linked to transaction intent, wallet signing and authorization outcomes.
21. The trust infrastructure should allow the lifecycle of a credential or mandate to be referenced, covering issuance, renewal, expiry, reissuance, suspension and revocation, so that a relying party can establish which instrument was in force at a given point.

Non-functional requirements

22. The infrastructure should distinguish between legal authority, operational authority and technical signing capability.
23. The infrastructure should support verification of authority without requiring disclosure of internal governance arrangements beyond what the transaction requires.

E5. Counterparty and participant due diligence

The trust infrastructure should allow participants to exchange and verify due diligence information relevant to a transaction. It should not replace onboarding, compliance review or risk assessment by participants. It should help parties bring relevant due diligence evidence into the transaction context, so that each relying party can assess it against its own obligations, policies and risk appetite.

Functional requirements

24. The trust infrastructure should allow participants to request, present and verify due diligence information about counterparties and other relevant participants, including beneficial ownership, regulatory status, sanctions status, tax status, eligibility status and relevant risk indicators.
25. The trust infrastructure should allow due diligence information to be linked to the relevant participant, wallet, transaction intent and authorization outcome.
26. The trust infrastructure should support relationship-level information, such as onboarding or periodic review status, and transaction-level information, such as sanctions, wallet-risk or eligibility checks.

Non-functional requirements

27. The infrastructure should support due diligence exchange without requiring participants to share full underlying client files, and should allow due diligence information to be reused where this is legally, commercially and operationally appropriate.

E6. Account, wallet, address and control attribution

The trust infrastructure should allow participants to connect wallets, accounts, addresses, keys and smart contracts to the relevant parties and transaction roles. A settlement endpoint does not identify who owns, controls or is authorized to use it. The infrastructure should help parties bring wallet and control information into the transaction context, without holding keys, controlling wallets or determining ownership.

Functional requirements

28. The trust infrastructure should allow participants to present and verify information linking a wallet, address, account, key or smart contract to a legal entity, natural person, custodian, wallet provider or service provider.
29. The trust infrastructure should allow proof of wallet, address or key control to be connected to the relevant transaction intent.
30. The trust infrastructure should support attribution of transaction roles, including sender, receiver, beneficiary, controller, signer, approver, custodian and wallet provider.
31. The trust infrastructure should allow control information to be linked to the applicable custody or wallet model, including arrangements in which there is no service provider to rely on.
32. The trust infrastructure should treat the binding of a party to a wallet as a lifecycle rather than a one-time proof of control, allowing binding, rotation, delegation, recovery, suspension, compromise and revocation to be referenced, and allowing an existing credential to be rebound to a new key without re-establishing the underlying fact.

Non-functional requirements

33. The infrastructure should distinguish between legal ownership, beneficial ownership, technical control, operational control and authority to transact.
34. The infrastructure should support wallet attribution without holding keys, controlling wallets or acting as a custodian.

E7. Transaction permissioning and policy enforcement

The trust infrastructure should allow participants to bring policy-relevant information into the transaction flow before, during or after settlement. It should not decide whether a transaction is permitted. It should connect transaction intent, evidence requests, policy conditions, authorization outcomes and settlement references, so that each relevant party can apply its own policies and controls.

Functional requirements

35. The trust infrastructure should support the creation of a transaction intent capturing the relevant transaction context, including parties, wallets, asset, amount, role and settlement reference.
36. The trust infrastructure should allow participants to request, present and receive policy-relevant information before transaction execution, and should support staged disclosure in which detailed policy conditions are shared only with identified or authorized parties.
37. The trust infrastructure should allow authorization outcomes from participants, custodians, policy engines or other assigned systems to be linked to the transaction intent.
38. The trust infrastructure should allow the mandate reference to be carried on the transaction intent where the initiating party acts under delegated authority.
39. The trust infrastructure should allow a relying party to check the conformance of the intended action to the purpose of the mandate. An acting party may hold a valid delegation chain and still act outside the purpose for which the mandate was granted, and no identity, authentication or signing check will detect this.
40. The trust infrastructure should allow information needed for enforcement or exception handling to be routed to the relevant wallet, custodian, smart contract, settlement system or receiving provider.

Non-functional requirements

41. The infrastructure should support both pre-settlement and post-settlement control models, with straight-through processing where possible and escalation where needed.
42. The infrastructure should remain neutral as to which participant or system applies the policy, makes the decision or performs enforcement.

E8. Governance and accountability of the trust layer

The trust infrastructure should make clear which actors perform which trust functions, and on what conditions others may rely on the information exchanged. It should not replace the legal, contractual or regulatory responsibilities of participants. It should connect roles, responsibilities, reliance conditions and governance rules to the relevant evidence and transaction context.

Functional requirements

43. The trust infrastructure should allow reliance conditions to be linked to evidence, including permitted use, validity, liability limitations and applicable governance rules, and to the assurance level actually relied upon rather than the assurance level nominally available.
44. The trust infrastructure should allow participants to present and verify information about trust-layer roles, including credential issuers, verifiers, wallet providers, custodians, policy engines, relying parties, auditors and market infrastructures.
45. The trust infrastructure should allow the identifiable participant at the head of a delegation chain to be established, so that accountability can be located where the acting party is software.
46. The trust infrastructure should allow the admission, recognition, suspension and withdrawal of participants in a trust-layer role to be referenced against the governing scheme or authority.

Non-functional requirements

47. Accountability should remain with identifiable participants and should not be obscured by automation, smart contracts or outsourced service providers.
48. No single party should be able to condition access to the recognition on which others depend, whether by commercial terms or by exclusion.
49. Each body that sets rules in the modular trust layer, such as a scheme or trust list operator, should document and disclose its governance, with clear lines of responsibility, a stated procedure for changing its rules, management of conflicts of interest, and representation of the interests of direct and indirect participants. Each party performing a trust function should disclose its responsibilities and how it manages conflicts of interest. Where schemes recognize each other, the terms of that recognition should be disclosed in the same way.

E9 Participation and access

The trust infrastructure should allow participants to identify and involve the relevant parties for a transaction, in the role in which they are expected to act. It should not itself decide who may access a market or approve a transaction. It should connect participants to verifiable information about identity, role, status and access conditions, so that the relevant parties can decide whether participation is acceptable for their purposes.

Functional requirements

50. The trust infrastructure should allow participants to request, present and verify information about participant category and role, including transacting organizations, financial institutions, digital asset service providers, wallet service providers, custodians, credential issuers, verifiers, risk-service providers, policy engines, auditors and market infrastructures.
51. The trust infrastructure should support direct participation, participation through a regulated intermediary, and participation through a recognized service provider.
52. The trust infrastructure should allow participants to present information relevant to access conditions, including regulatory status, recognized role, technical connectivity, scheme membership and service-provider status.
53. The trust infrastructure should allow changes in participant status to be referenced, including changes in role, participation model, suspension, termination and loss of recognition, as notified by the relevant source.

Non-functional requirements

54. The infrastructure should support transaction-specific participation and access assessments without becoming the access decision-maker.

E10. Reliance, liability and dispute resolution

Reliance on another party's evidence is only workable where the consequences of that evidence being wrong are allocated in advance. At present a relying party generally bears the full consequence, which makes bilateral contracting the only safe route and limits the market to the number of counterparty pairs willing to negotiate terms. The requirements below concern what the trust layer must carry for liability to be allocated by scheme rulebook rather than determined after the event.

The trust layer does not itself allocate liability, adjudicate disputes or determine fault. It carries the reliance terms and produces the evidence on which an allocation can be made.

Functional requirements

55. The reliance terms attached to a piece of evidence should state how loss is allocated where that evidence proves incorrect, incomplete or out of date, and should be available to a relying party before it relies.
56. The trust infrastructure should allow each party's contribution to an authorization to be distinguished in the record, separating the fact asserted by the issuer, the verification performed by the verifier, and the decision taken by the relying party.
57. The trust infrastructure should produce the evidence needed to establish whether a relying party acted in accordance with the applicable reliance terms, including which checks were performed, against which source, and at what point relative to authorization.
58. The trust infrastructure should allow a dispute to be raised against a specific authorization, evidence presentation or verification, and should provide the references needed by the party responsible for handling it.
59. The trust infrastructure should allow the applicable dispute route to be established from the evidence, including the governing scheme, the responsible party and any limitation period.

Non-functional requirements

60. Reliance terms should be capable of being determined at transaction time rather than only on inspection of a contract, so that a relying party can establish its position before relying rather than after a loss.
61. Where evidence passes through an intermediary, the record should establish which party carried which obligation, so that intermediation does not obscure the allocation of loss.
62. Reliance terms and scheme rules should have a clear and enforceable legal basis in every jurisdiction relevant to the transaction, and the governing scheme should identify conflicts of law between those jurisdictions and state how they are resolved.

E11. Client, investor and user protection

The trust infrastructure should help participants connect transactions to verifiable information about rights, restrictions and responsible parties. It should not provide investor protection, handle complaints or determine liability. It should allow relevant protection information to be brought into the transaction context, so that participants and users can establish which rights, obligations and recourse mechanisms apply.

Functional requirements

63. The trust infrastructure should allow participants to request, present and verify information about responsible parties, including custodians, wallet providers, issuers, execution providers and settlement providers.
64. The trust infrastructure should allow information on user rights, investor eligibility, redemption rights, transfer restrictions, applicable terms, fees, risks and recourse mechanisms to be linked to the relevant asset or transaction.
65. The trust infrastructure should provide the references needed to investigate errors, fraud, unauthorized transactions, failed transfers and disputes.

Non-functional requirements

66. The infrastructure should support different protection models, including arrangements in which no service provider carries responsibility for the user's position.

E12. Market conduct and market integrity

The trust infrastructure should support market integrity by helping participants connect market activity to the relevant parties, wallets, assets and transaction context. It should not determine whether conduct is abusive, manipulative or fraudulent. It should provide the verifiable links and references that allow authorized parties to perform surveillance, investigation, reporting or escalation.

Functional requirements

67. The trust infrastructure should support verifiable links between market activity and the participants, wallets, agents, platforms and service providers involved, for the purposes of surveillance, investigation or reporting.
68. The trust infrastructure should allow market-integrity information to be routed to authorized parties, market infrastructures or supervisors.

Non-functional requirements

69. The infrastructure should support traceability without requiring public disclosure of identities, positions, strategies or internal risk models.

E13. Information exchange and data minimization

The trust infrastructure should allow participants to exchange the information needed to assess, authorize and evidence a transaction. In wallet-based and agentic markets the information flow may be separate from the value flow. The infrastructure should connect evidence requests, responses and references to the relevant transaction, without becoming the central store for the information exchanged.

Functional requirements

70. The trust infrastructure should support structured evidence requests and responses between transaction participants, covering identity, authority, wallet control, due diligence, asset eligibility, transaction context and policy conditions.
71. The trust infrastructure should allow exchanged information or references to be linked to transaction intent, authorization outcome and settlement reference.

Non-functional requirements

72. Information exchange should support both bilateral and multi-party transaction workflows, and should be configurable to reflect the roles, legal basis and information needs of the participants involved.

E14. Recordkeeping, auditability and supervisory visibility

The trust infrastructure should support recordkeeping without becoming the central repository for transaction evidence. Its role is to provide the references and validation traces needed to connect transaction intent, evidence exchange, authorization outcome and settlement reference. The underlying records should remain with the participants.

Reliance depends on whether the evidence was current, valid and unrevoked at the point at which the transaction was authorized. That is a property of the record, not of the evidence. The requirements below therefore address the state of the evidence at the moment of reliance, and not only its state at the moment of checking.

Functional requirements

73. The trust infrastructure should allow a record to establish what was relied upon, including the mandate reference and the assurance level of the evidence, that the evidence was valid at the point of authorization rather than at the point at which it was checked, and how recent it was at that point.
74. The trust infrastructure should provide the references needed for participants to create and reconcile their own transaction trust records across evidence exchange, internal books and records, and on-chain or settlement-system activity.
75. The trust infrastructure should maintain a minimal audit trail of information flows through the infrastructure, using references, codes, hashes or pointers rather than retaining the underlying evidence.
76. The trust infrastructure should support controlled access to audit-trail information for audit, reconciliation, dispute handling and supervisory visibility.
77. The trust infrastructure should allow an authorization record to be proven to have existed in that exact form at the time of authorization, and that proof to be checkable by a party that trusts none of the participants, using a commitment that binds to the record without revealing it.
78. Authorization records should be sequenced per participant, so that a missing record is visible and the absence of a check can be established rather than assumed.
79. Audit and supervisory verification should be possible from commitments and proofs, without granting read access to the underlying records or to the pattern of relationships between participants.

Non-functional requirements

80. The audit trail should be proportionate to the infrastructure's linking function, and durable for the period over which the underlying transactions may be disputed or examined.
81. Recordkeeping should remain decentralized, with participants responsible for retaining their own evidence and decision records.
82. Evidence and authorization records should remain verifiable for as long as the transaction may be examined, including after keys are rotated, algorithms are replaced or the issuer ceases to exist.

E15. Interoperability

The trust infrastructure should allow participants to exchange and verify information across different wallets, custodians, chains, credential frameworks and financial systems. It should not impose one technical architecture or settlement environment. It should provide the common interfaces, schemas and semantics needed to connect participants and transaction-related evidence across infrastructures.

Functional requirements

83. The trust infrastructure should support common schemas and semantic definitions for participant roles, identity, authority, wallet control, asset information, transaction context and authorization outcomes, published as a versioned interoperability profile.
84. The trust infrastructure should support integration with existing financial messaging, compliance, ERP, custody, reporting and settlement systems.
85. Evidence should be presentable over the credential presentation protocols converging in the market, including OpenID4VP, the W3C Digital Credentials API and HTTP-native challenge flows, while the infrastructure remains neutral as to which is used.

Non-functional requirements

86. The infrastructure should avoid dependence on a single wallet, chain, custodian, credential issuer, messaging protocol or identity framework.

E16. Operational resilience and security

The trust infrastructure should be secure and resilient enough to support transaction-critical evidence exchange, verification and linking. It should not operate the underlying wallets, credentials, policy engines, custody systems or settlement infrastructures. Its resilience requirements therefore concern the continuity, integrity and recoverability of the linking and verification functions it performs.

Functional requirements

87. The trust infrastructure should support continuity of its core linking functions, including transaction intent, evidence exchange, authorization outcome and settlement reference.
88. The trust infrastructure should allow participants to verify the availability, validity or status of relevant information with the appropriate source or issuer.
89. The trust infrastructure should provide fall-back paths where evidence exchange, verification or transaction linking is unavailable, delayed or inconclusive, and should define that degraded-mode behavior in advance so participants know what happens when a check cannot complete.

Non-functional requirements

90. Core linking and verification functions should be recoverable, and should avoid single points of failure for evidence exchange, transaction linking and audit-trail continuity.
91. Failures, delays and incomplete verification should be visible to the relevant participants and recorded in the audit trail, so that a transaction is not treated as fully evidenced where trust-layer checks were unavailable or inconclusive.

Areas for further development regarding requirements

Three main areas for further development are identified but not resolved in this overview.

1. **Assurance thresholds.** This appendix states that assurance levels, freshness bounds and revocation intervals must be explicit and that a named party must set them. It does not propose values. Those are properly a matter for scheme rulebooks in the relevant jurisdiction and asset class.
2. **Allocation of verification cost and value.** Requirement E-II.16 sets a threshold for the marginal cost of verification. Who bears that cost, and who captures the value created by shared verification, is a question of market structure rather than a requirement on the trust layer, and is not answered here.
3. **Extent of the agentic dimension.** Requirements addressing delegated authority, mandate purpose, evidence freshness and the location of accountability have been placed in the families to which they belong, in E4, E7, E8 and E14. The requirement language in those families should be treated as indicative pending further technical validation.

Oliver Wyman, a Marsh (NYSE: MRSH) business, is a management consulting firm driven by deep industry insight, bold innovation, and a collaborative approach that cuts through complexity to help organizations navigate their most defining transformative moments. Marsh is a global leader in risk, reinsurance and capital, people and investments, and management consulting, advising clients in 130 countries. With annual revenue of $27 billion and more than 95,000 colleagues, Marsh helps build the confidence to thrive through the power of perspective.

For more information, visit oliverwyman.com, or follow us on LinkedIn and X.

Americas	Europe	Asia Pacific	India, Middle East & Africa
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700	+971 (0) 4 425 7000

AUTHORS

Ivan Mortimer-Schutts
Ivan.Mortimer@gleif.org

Pieter Verhagen
Pieter.Verhagen@oliverwyman.com

Douwe Lycklama
Douwe.Lycklama@oliverwyman.com

Yekaterina Travkina
Yekaterina.Travkina@oliverwyman.com

About the Global Legal Entity Identifier Foundation (GLEIF)

The Global Legal Entity Identifier Foundation (GLEIF) was established by the Financial Stability Board (FSB) in June 2014 as a non-for-profit organization to support the implementation and use of the Legal Entity Identifier (LEI) and its digital counterpart, the verifiable LEI (vLEI). GLEIF is headquartered in Basel, Switzerland.

GLEIF's mission is to enable trust and transparency through open, global organizational identity. GLEIF supports the Global LEI System as a public good, using open standards and freely accessible reference data to connect organizational identity across borders and systems. GLEIF is overseen by the Regulatory Oversight Committee, which is made up of representatives of public authorities from across the globe.

Diversity and inclusion underpin GLEIF's values. This is reflected in its workforce of approximately 60 staff from over 20 nations, its operational excellence, and its commitment to open, global participation in the Global LEI System.

For more information, visit the GLEIF website at https://www.gleif.org/en.

Copyright 2026 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.